

Board Policy Book



Finance Policies

Budget Policy

I. Budget Policy – Strategic Purpose

The purpose of this policy is to guide the Sourcewell budget development and organizational planning discussions in a way that aligns with Sourcewell’s Vision, Mission, and Values.

Through the guidance of Sourcewell’s organizational planning, departmental budgets, goals, and initiatives shall align.

II. Scope

The Sourcewell Board adopts estimated revenue and expense budgets for all Enterprise Funds. The Budget Policy also covers the scope of Sourcewell’s Net Position management strategies.

III. Budget Period and Basis of Budgeting

All budgets within the scope above shall be adopted annually on the accrual basis of accounting. Actual financial results are reported in the annual Financial Statements in accordance with generally accepted accounting principles (GAAP) using the accrual basis of accounting.

IV. Balanced Budget

Financial planning practices will be designed to recognize the best practices of structurally balanced budgets. Therefore, Sourcewell promotes the adoption of a structurally balanced budget. A budget shall be considered structurally balanced when recurring revenues equal or exceed recurring expenses.

However, Net Position may be spent down strategically, as recommended by the Executive Director, Sr. Leadership Team, and approved by the Sourcewell Board.

Sourcewell promotes long-term financial planning and balanced budget best practices by focusing on “non-operating or non-recurring” expenses as the best areas for the utilization of Net Position. The following list highlights examples of financially strategic and/or prudent ways that Sourcewell can manage these reserve resources:

- A. Region 5 partnerships to reinvest in the communities we serve;
- B. Organizational capital improvements.
- C. Productivity, technology, and service enhancement projects (one-time projects);
- D. Pre-funding or buying down of long-term liabilities or debt.
- E. Litigation;
- F. Other one-time purposes deemed to be fiscally prudent for Sourcewell.

V. Long-Term Strategy and Financial Planning

Sourcewell recognizes the importance of long-term strategic planning, as evidenced by the organizational planning

Sourcewell will integrate internal financial practices into Sourcewell’s organizational planning. Budgetary and financial resources shall be managed in a way that promotes growth in services across North America. Resources will also be re-invested into Region 5 through “value-added” services and partnerships.

Sourcewell recognizes that prudent financial planning considers the multi-year implications of organizational objectives and business decisions. Sourcewell shall maintain a long-term financial focus in its financial planning that is mindful of the long-term “value-added” service growth objectives of Sourcewell. This long-term focused philosophy shall be evident in the management practices of Net Position.

VI. Examination of Spending Patterns

Sourcewell seeks to maximize the value the public receives through its spending. Accordingly, staff should develop budget tools and methods to measure outcomes and maximize value.

VII. Priority of Services

Sourcewell desires to maintain and potentially grow current service levels for all services; however, if necessary, Sourcewell will reduce or eliminate low-priority services before essential core services. Priority will be recommended by the Executive Director and Sr. Leadership Team after analysis and consideration of financial information, social benefit, state or federal requirements, or other factors contributing to the importance of a program or service and approved by the Sourcewell Board.

VIII. Funding of Liabilities

The budget will provide sufficient funding to avoid accumulating excessive liabilities over the long term.

IX. Budget-Balancing Strategies

Sourcewell will implement a structurally balanced budget as described in Note IV. Temporary shortages, or operating deficits, can occur, but they shall not be tolerated as existing trends. Sourcewell will avoid budgetary and accounting procedures which balance the current budget at the expense of future budgets.

X. Budget Process

Sourcewell is committed to timely certification of the budget and overall comprehensive financial planning. A financial planning calendar will be developed by the Finance staff annually to coincide with **organizational planning**.

XI. Budgetary Monitoring

Department heads are responsible for monitoring their monthly budget information. Finance will maintain a system for monitoring Sourcewell's budget performance. This system will provide the Sourcewell Board with monthly budget updates.

XII. Level of Budgetary Authority/Control

The original budget is adopted through the passage of a Board resolution. The Executive Director can authorize the transfer of budgeted amounts within Sourcewell. Revisions that alter the total expenses of Sourcewell must be approved by the Board.

XIII. Budget Amendments

Amendments to the budget increasing total budgeted expenses within Sourcewell require approval of the Sourcewell Board. Generally, a budget amendment will occur due to the following: implementation of a new program increases in services provided affecting revenues or expenses, requesting additional staff, or requesting the purchase or construction of capital items.

A. BUDGET AMENDMENT PREPARATION

Budget amendment requests are to be initially prepared by the department requesting the change.

Since the level of budgetary authority/control is at the organizational level, individual departments shall communicate their budgetary amendment requests to Finance. Additionally, **Sourcewell will utilize a budget amendment materiality threshold of greater than \$100,000.**

Finance will work with the Executive Director and Senior Leadership Team in determining if the budget amendment request can be absorbed by an Executive Director-approved reallocation, prior to making a Board request for increased funding.

Lastly, all budget amendments that are deemed to require Board approval shall be reviewed and approved by the Senior Leadership Team for accuracy, objectivity, completeness, and format before submission to the Sourcewell Board.

B. COMPONENTS OF A BUDGET AMENDMENT

The following two components are required in each formal budget amendment:

(1) Budget Amendment Request Heading and Description

This component includes a summary heading and a description of the purpose for the budget amendment.

Budget amendments should be factual, informative, and concise.

(2) Fiscal Commitments

This component forecasts revenues and expenses for a minimum of three years or the length of the activity or service, whichever is shorter. During a partial year, forecasts should include the portion of the year remaining and two full subsequent years. Finance is available to assist departments with the preparation of the fiscal section.

Ongoing and current (one-time) revenues/expenses should be clearly differentiated in the budget amendment request to better understand the long-range commitments.

Budget Policy Adoption

Sourcewell's Budget Policy shall be adopted by resolution of the Sourcewell Board. The policy shall be reviewed on a regular basis by the Senior Leadership Team, and any modifications made thereto must be approved by the Sourcewell Board.

Capital Asset Management Policy

Purpose

The purpose of this document is to set forth policies to maintain accurate records of assets whose value and useful life meet the definition of capital assets. This policy focuses on compliance with Generally Accepted Accounting Principles (GAAP) to ensure accurate reporting and valuation of capital assets within Sourcewell’s external financial statements.

Scope

The Capital Asset Management Policy applies to all capitalized assets of Sourcewell and specifically addresses the external financial reporting aspects of capital assets. The scope of this policy does not address financial planning, budgetary project management, non-capital asset inventory tracking, or insurance tracking considerations of assets.

Throughout this policy, the term “capital asset” is used to describe both tangible and intangible assets, as well as right-of-use assets, unless otherwise indicated.

Capitalization Threshold

Capital assets are classified as property purchased or developed by Sourcewell that has a value greater than or equal to \$15,000 and has an estimated useful life of at least three years.

Right-of-use (ROU) assets recognized under GASB Statement No. 87 (leases) and GASB Statement No. 96 (subscription-based information technology agreements, or SBITAs) have no set minimum capitalization threshold. Sourcewell will consider the materiality and length of the underlying contracts when recognizing ROU assets in accordance with Statement Nos. 87 and 96.

Depreciation, Amortization, and Estimated Useful Life

Capital assets will be depreciated or amortized using the straight-line method over an asset’s estimated useful life. The estimated useful life of capital assets will be determined using reasonable assumptions, based on current information. In general, Sourcewell will use the following broad categories of estimated useful life, although each asset will be considered individually, and useful life may vary. Finance will work with the appropriate department head to identify a suitable useful life in ambiguous circumstances.

<u>Asset</u>	<u>Useful Life (Years)</u>
Building	20-40
Building Improvements	15-20
Land Improvements	15-20
IT Software and Equipment*	3-7
Furniture, Fixtures, and Equipment	5-15

*Including internally generated intangible assets (i.e., developed software).

The useful life of an ROU asset is based on the length of the agreement and whether the agreement includes a right to purchase the underlying asset and may differ from the chart above.

Periodic Review and Updates

Sourcewell will perform an annual inventory that addresses the physical condition of its tangible capital assets and the current state of its intangible assets, by the department by asset class.

- An updated asset list and depreciation schedule will be provided by the Finance department to each department head.
- It is each department’s responsibility to review capital assets on their respective lists, record any changes or corrections, note any capital assets that have been impaired/disposed of or may be missing, and identify any new assets that were not included in the database.

Disposal of Assets

Assets that have reached the end of their serviceable life and/or are no longer of use by the organization will be disposed of in an efficient and environmentally responsible manner.

- Assets that will be disposed of must be offered to voting members of Sourcewell at no cost, using existing processes, before any further disposition is made.

- Departments shall update their asset list to reflect the disposal status of assets in their respective areas of responsibility.
- Departments shall follow all applicable local, state, and federal laws when disposing of assets.
- Departments shall use environmentally sound practices, suppliers, and services when disposing of assets.

Capital Asset Management Policy Adoption

Sourcewell's Capital Asset Management Policy shall be adopted by the resolution of Sourcewell's Board of Directors. The policy shall be reviewed on a periodic basis and any modifications made thereto must be approved by Sourcewell's Board of Directors.

Long-Term Financial Planning Policy

I. Purpose:

The purpose of this policy is to ensure Sourcewell's on-going financial sustainability beyond a single fiscal year budget cycle in light of the organization's long-term mission, vision, and strategic objectives.

II. Scope:

This policy is applicable organization-wide.

III. Definitions and Acronyms:

Business Plan: An operational plan that describes how a given department will accomplish a mission.

Capital Improvement Plan (CIP): A plan that describes the capital projects and associated funding sources Sourcewell intends to undertake in the current year plus three additional future years, including the acquisition or construction of capital facilities and assets.

Long-Term Financial Plan (LTFP): An investment plan or strategy with a term of usually longer than one year.

Program: A set of activities, operations, or organizational units designed and directed to accomplish specific service outcomes or objectives for a defined customer.

IV. Policy:

A. Commitment to Long-Term Financial Planning

Sourcewell will maintain long-term fiscal solvency by identifying significant future expenses, liabilities, capital needs and resources that are not included or recognized in the annual budget.

The Long-Term Financial Plan (LTFP) process evaluates known internal and external issues impacting Sourcewell's financial condition. Such issues are identified, presented, and mitigated when and where possible. The process begins by identifying critical areas which have, or are expected to have, an impact on the financial condition of Sourcewell over the next three years. Once the issues are identified, specific goals and objectives are developed for each structural deficiency. The LTFP is a constantly changing and moving document which will be routinely updated and presented on a rolling basis. The LTFP will be completed during the organizational planning process, and is intended to help Sourcewell achieve the following:

1. Ensure Sourcewell can attain and maintain financial sustainability.
2. Ensure Sourcewell has sufficient long-term information to guide financial decisions.
3. Ensure Sourcewell has sufficient resources to provide programs and services for members.
4. Ensure potential risks to on-going operations are identified in the long-term financial planning process and communicated on a regular basis.
5. Identify changes in expenses or revenue structures needed to deliver services or to meet the strategic goals and objectives; and

6. Recognize that Sourcewell may need to adapt after consideration of outside forces and changing economic conditions.

B. Scope of the Plan

1. Time Horizon – The LTFP will forecast revenues, expenses, and financial position at least three years into the future or longer where specific issues call for a longer time horizon.
2. Comprehensive Analysis - The LTFP will provide meaningful analysis of key trends and conditions, including, but not limited to, the following:
 - a) *Analysis of the affordability of current services, projects, and obligations:*
 - (1) An analysis of Sourcewell’s environment to anticipate changes that could impact Sourcewell’s services or financial objectives.
 - (2) Revenue and expense projections, including the financial sustainability of current service levels over a multi-year period.
 - (3) The affordability of maintaining and replacing Sourcewell’s current capital assets (e.g., buildings, infrastructure, equipment, technology).
 - (4) The ability to maintain reserves within the target ranges.
 - (5) The impact of non-current liabilities on Sourcewell’s financial position.
 - b) *Analysis of the affordability of anticipated service expansions or investments in new assets.*
 - (1) The operating costs of any new initiatives, projects, or expansion of services where funding has been identified through alternative sources. Administrative services and other indirect costs shall be included to the extent needed proportionately with the expansion of other services.
 - (2) The affordability of Sourcewell’s long-term Capital Improvements Plan (CIP), including operating and maintenance costs for new assets.
 - (3) The affordability of other business plans that call for significant financial investment by Sourcewell.
 - c) *Synthesis of the above to present Sourcewell’s financial position:*
 - (1) A clear presentation of the resources needed to accomplish the capital improvements identified in Sourcewell’s CIP and to maintain existing capital assets.
 - (2) A clear presentation of the resources needed to maintain existing services at their present level in addition to the expansion of services as may have been identified through the analysis described above.
 - (3) Identification of any imbalances between Sourcewell’s current direction and the conditions needed for continued financial health.

3. Solution Oriented - The LTFP will identify issues that may challenge the continued financial health of Sourcewell, and the plan will identify possible solutions to those challenges. Planning decisions shall be made primarily from a long-term perspective, and structural balance is the overarching goal of the planning process.
- C. Relationship between Financial and Strategic Planning – Sourcewell’s annual budget process involves incorporating the goals, initiatives, and strategies identified by Sourcewell’s three-year strategic plan. Strategic planning begins with determining Sourcewell’s fiscal capacity based upon long-term financial forecasts of recurring available revenues.
- D. Continuous Improvement – Sourcewell staff will regularly look for and implement opportunities to improve the quality of the forecasting, analysis, and strategy development that is part of the planning process. These improvements will primarily be identified through the comparison of projected performance with actual results.
- E. Structural Balance – Long-term structural balance is the goal of long-term financial planning. Should the long-term forecasting and analysis show that Sourcewell is not structurally balanced over the next three-year projection period; staff would then make recommendations on how the plan can be brought into balance.

V. Long-Term Financial Planning Policy Adoption

Sourcewell’s Long-Term Financial Planning Policy shall be adopted by resolution of Sourcewell’s Board of Directors. The policy shall be reviewed on a periodic basis and any modifications made thereto must be approved by Sourcewell’s Board of Directors.

Organizational Reserve Policy

I. Purpose

This policy establishes the minimum amount Sourcewell will strive to maintain in its organizational reserve, how reserves will be funded, and the conditions under which reserves may be used.

II. Scope

This policy is applicable to all funds within Sourcewell's external financial reporting structure, excluding the Better Health Collective which has a separate policy for reserve management.

III. Purpose of Reserves and Definitions

Sourcewell desires to maintain a prudent level of financial resources to guard against service disruption in the event of unexpected temporary revenue shortfalls or unpredicted one-time expenses. Reserves are accumulated and maintained to provide stability, capital investments, growth, and flexibility to respond to unexpected adversity and/or business opportunities.

Capital Improvement Plan (CIP): A plan that describes the capital projects and associated funding sources Sourcewell intends to undertake in the current year plus three additional future years, including the acquisition or construction of capital facilities and assets.

Reserve: Reserve refers broadly to working capital and the resources available to provide operational stability, funding for the CIP, one-time strategic reinvestments, and to respond to unplanned events or business growth opportunities. For purposes of this policy, reserve refers to working capital which is defined as current assets plus long-term investments less current liabilities. Working capital indicates the relatively liquid portion of total enterprise fund capital, which constitutes a margin or buffer for meeting obligations.

IV. Policy

A. Reserve Target Range

Sourcewell's targeted range of reserves is equivalent to six to twelve months of regular, ongoing operating expenses. Sourcewell will measure its compliance with this policy as of June 30th each year, or as soon as practical after final year-end account information becomes available.

The following risks and drivers support the six to twelve months reserve target range:

1. Sourcewell is a self-supporting entity with no taxing authority or debt issuance authority.
2. Diversification risk – A large portion of Sourcewell's operating revenue and profit is dependent on a single business model which increases overall organization risk.
3. Demand for services – Sourcewell has supported a growing demand for regional programs, services, and one-time reserve utilization considerations to reinvest in member communities.
4. Business growth mindset – Sourcewell has significant interest in securing flexibility for future opportunities and organizational funding diversification. These opportunities may require significant up-front investment that cannot be supported by operating revenues.

Reserves can include both truly unrestricted resources and resources that have internal limitations placed upon them (e.g., board-designated) and/or that may be committed for future spending. These amounts may appear as unrestricted on the Statement of Net Position but may be unavailable in the future to serve as a buffer or tool to help manage financial risk.

B. Funding the Reserve

Funding of reserve targets will generally come from excess revenues over expenses. Departmental metrics and budget monitoring are the primary drivers in guiding the incremental reserve growth needs as it relates to organizational growth forecasts.

C. Authority Over Reserves

The Executive Director/CEO will make reserve utilization recommendations to the Board of Directors.

D. Use, Replenishment, and Sustainability of Reserves

If reserve usage results in a balance below the target range minimum of six months, a plan to restore reserve levels will be developed and included in the formulation of the three-year forecast. This plan will be presented during the annual budget process.

Reserves that fall within the bottom half of the target range (six to nine months of regular, ongoing operating expenses) should not be applied to recurring annual operating expenses.

Reserve ranges should be monitored and forecasted at least annually. Actual or forecasted levels in the six to nine-month range should be monitored more frequently to ensure reserve levels are not falling lower than the minimum.

E. Healthy Reserves

If reserves exceed nine months of regular, ongoing operating expenses at the end of each fiscal year, reserves may be used in the following ways:

1. Appropriated to fund major capital asset projects in the CIP.
2. One-time expenses that do not increase recurring operating costs that cannot be funded through current revenues.
3. Fund long-term liabilities, including but not limited to lease obligations, pension, compensated absences, and other post-employment benefits. Priority will be given to those items that relieve financial operating pressure in future periods.
4. Start-up expenses for new Solution Innovation opportunities.

V. Quality Assurance and Policy Adoption

It is the responsibility of the Director of Finance/CFO to ensure the presence of procedures that provide sufficient guidance to affected Sourcewell personnel to fulfill the intent of this policy.

The Organizational Reserve Policy will be adopted by resolution of the Sourcewell Board of Directors. The policy will be reviewed on a regular basis by the Senior Leadership Team and any modifications made must be approved by the Sourcewell Board of Directors.

Investment Policy

INVESTMENT POLICY TABLE OF CONTENTS

<u>SECTION DESCRIPTION</u>	<u>Page</u>
I. Purpose	2
II. Scope	2
III. Objectives	2
A. Safety	2
B. Liquidity	2
C. Yield	2
IV. Standards of Care	2
A. Authority to Invest	2
B. Prudence	3
V. Investment Portfolio	3
A. Authorized Investments	3
B. Diversification	3
C. Maturities	3
VI. Safekeeping and Custody	4
A. Eligible Institutions	4
B. Investment Advisors	4
C. Collateral	4
D. Safekeeping	4
E. Internal Control	4
VII. Reporting	5
A. Frequency and Format	5
B. Performance Targets	5
VIII. Interest Allocations	5
IX. Investment Policy Adoption	5

I. Purpose

This policy has been developed to serve as a reference point for the management of assets and the investment of Sourcewell funds.

II. Scope

This Investment Policy applies to all financial assets of Sourcewell. All cash and investments are pooled together to achieve economies of scale. These funds are accounted for in the annual financial statements and include all Sourcewell funds. Additionally, Sourcewell will apply these objectives and standards of care to investments made on behalf of other organizations of a fiduciary nature, such as the Better Health Collective. In this policy "Sourcewell" will refer both to funds of Sourcewell, as well as funds held and invested by Sourcewell on behalf of others, unless stated otherwise.

III. Objectives

It is the policy of Sourcewell to invest funds in a manner which provides for the following in order of importance: Safety, Liquidity, and Yield, that conforms to all federal, state, and local regulations. All investments purchased by Sourcewell are expected to be held until maturity. Sourcewell will invest in securities that match Sourcewell's operational, short-term, and longer-term core reserve needs.

A. Safety

Investments of Sourcewell shall be undertaken in a manner that seeks to ensure the preservation of principal in the overall portfolio. The objective will be to mitigate credit risk and interest rate risk.

B. Liquidity

Sourcewell's investment portfolio will remain sufficiently liquid to enable Sourcewell to meet all operating requirements as reasonably anticipated. The portfolio will be structured so that the liquid component of the portfolio (a minimum of five percent of total investments) will be invested only in short-term securities maturing in less than thirty days. Furthermore, a portion of the portfolio may be placed in money market mutual funds or local government investment pools which offer same day liquidity for short-term funds.

C. Yield

Sourcewell's investment portfolio shall be designed with the objective of attaining a market rate of return. The core of investments is limited to low-risk securities in anticipation of earning a fair return relative to the risk being assumed. Securities shall generally be held until maturity with the following exceptions:

1. A security with declining credit may be sold early to minimize loss of principal.
2. A security swap would improve the quality, yield, or target duration in the portfolio.
3. Liquidity needs of the portfolio require that the security be sold.

IV. Standards of Care

The investment program shall be operated in conformance with federal, state, and other legal requirements. Authority to manage Sourcewell's investment program is derived from Minn. Stat. § 118A, Deposit and Investment of Local Public Funds.

A. Authority to Invest

Responsibility for the investment program is hereby delegated from the Sourcewell Board to the Director of Finance/CFO. Authority to conduct actual investment transactions may be delegated to designees within Finance or a third-party Investment Manager, who shall act in accordance with procedures as established with this investment policy.

No person may engage in an investment transaction except as provided under the terms of this policy and the procedures established by the Director of Finance/CFO. The Director of Finance/CFO shall be responsible for all investment transactions and shall establish a system of controls to regulate the activities of subordinates.

- B. Prudence
Investments shall be made with judgment and care under circumstances existing at the time the investment is made. The standard to be used by investment officials shall be the “prudent person” standard and shall be applied in the context of managing an overall portfolio. The prudent person standard requires that a fiduciary exercise discretion and average intelligence in making investments that would be generally acceptable as sound. Investment officers acting in accordance with written procedures and the investment policy and exercising due diligence shall be relieved of personal liability for an individual security’s credit risk or market price changes, provided deviations from expectations are reported in a timely fashion and appropriate action is taken to control adverse situations.

V. Investment Portfolio

- A. Authorized Investments
Sourcewell will invest funds based on the investment objectives as defined in section III of this policy, and in accordance with Minn. Stat. § 118A.

Sourcewell is also authorized under Minn. Stat. § 118A to enter into Securities Lending Agreements. Securities lending transactions may be entered into with entities meeting the qualifications and the collateral for such transactions shall be restricted to the securities described in Minn. Stat. § 118A.

- B. Diversification
Sourcewell will substantially reduce the risk of loss resulting from the over-concentration of assets in a specific maturity, issuer, institution, or class of securities.

Diversification strategies will be implemented with the following constraints:

ISSUER TYPE	MAXIMUM % OF TOTAL PORTFOLIO ²
a. Savings/demand deposits ¹	25%
b. Certificates of Deposit	75%
c. U.S. Treasury Obligations	100%
d. U.S. Agency Securities	100%
e. Per Issuer:	50%
f. Municipal Securities	100%
g. Per Issuer:	5%
h. Mortgage-Backed Securities	10%

¹The savings/demand deposits held by Sourcewell will fluctuate because of operational cash flow needs.

²Due to fluctuations in the value of the portfolio, maximum percentages for a particular issuer or investment type may be exceeded at a point in time after the purchase or maturity of a particular security. Securities need not be liquidated to realign the portfolio; however, consideration should be given to this matter when future purchases are made.

Interest rate risk is the risk that changes in market interest rates will adversely affect the fair value of an investment. To minimize Sourcewell’s exposure to interest rate risk, Sourcewell will:

1. Invest in both shorter-term and longer-term investments; and
2. Evenly time cash flows from maturities; and
3. Monitor the expected mark-to-market adjustment if interest rates increase by 100-200 Basis Points.

- C. Maturities
Sourcewell shall structure the maturity of investments as follows:
1. A minimum of five percent of the overall cash and investment portfolio will mature in under 30 days,
 2. Total weighted average maturity of total funds will not exceed 7 years, and
 3. Maturities will be diversified to avoid undue concentration of assets in a specific sector.

VI. Safekeeping and Custody

A. Eligible Institutions

Deposit shall be made in a qualified public depository as established by state laws.

B. Investment Advisors

Sourcwell may enter into agreements with third-party investment advisory firms when their services are deemed to be beneficial to Sourcwell. The advisor must comply with this Investment Policy and may have authority to transact investments on behalf of Sourcwell. The advisor may act on a discretionary basis if they are hired to provide transactional services on behalf of Sourcwell.

C. Collateral

In accordance with Minn. Stat. § 118A, the total amount of the collateral computed at its market value shall be at least ten percent more than the amount on deposit at the close of the financial institution's banking day, except that where the collateral is irrevocable standby letters of credit issued by Federal Home Loan Banks, the amount of collateral shall be at least equal to the amount on deposit at the close of the financial institution's banking day. The financial institution may furnish both a surety bond and collateral aggregating the required amount.

Collateralization will be required on the following types of investments:

1. Certificates of Deposit
2. Demand Deposits

Collateral is limited to securities allowable pursuant to Minn. Stat. § 118A.03.

For cash deposits on hand, collateralization shall be in the form of specific securities with an active secondary market for Sourcwell held by an independent third party. The only exceptions are Federal Depository Insurance Corporation (FDIC), Securities Investor Protection Corporation (SIPC) and pre-approved insurance coverage.

D. Safekeeping

Securities purchased shall be held in a segregated account for Sourcwell's benefit at a third-party trustee as safekeeping agent in accordance with Minn. Stat. § 118A.06. The investment dealer or bank in which the security is purchased shall issue a confirmation ticket to Sourcwell listing the specific instrument, issuer, coupon, maturity, CUSIP number, purchase or sale price, transaction date, and other pertinent information. The financial service provider which executes the transaction on Sourcwell's behalf shall deliver all securities on a delivery versus payment method (DVP) to the designated third party.

Sourcwell's ownership of all securities should be evidenced by written acknowledgments identifying the securities by:

1. The names of issuers
2. The maturity dates
3. The interest rates
4. Any serial numbers or other distinguishing marks

E. Internal Controls

Sourcwell's Finance department is responsible for establishing and maintaining an internal control structure designed to ensure that the assets of Sourcwell are protected from loss, theft, or misuse. The internal control structure shall be designed to provide reasonable assurance that these objectives are met. The concept of reasonable assurance recognizes that (1) the cost of a control should not exceed the benefits likely to be derived; and (2) the valuation of costs and benefits requires estimates and judgments.

VII. Reporting

A. Frequency and Format

Finance is charged with the responsibility of preparing a periodic investment report, including a management summary that provides an analysis of the status of the current investment portfolio.

B. Performance Targets

The investment portfolio will be designed to obtain a market average rate of return during budgetary and economic cycles, considering Sourcewell's investment risk constraints and cash flow needs. The investment portfolio will be structured to meet specific criteria addressing safety, liquidity, and yield.

Sourcewell's investment strategy is conservative. Industry benchmarks will be utilized to determine whether market yields are being achieved.

VIII. Interest Allocations

Sourcewell shall allocate monthly any investment interest earned that month to the Cooperative Purchasing Fund and the Better Health Collective Fund. Each fund will receive an allocation based on its proportionate share of total Sourcewell cash and investments.

IX. Investment Policy Adoption

Sourcewell's Investment Policy shall be adopted by resolution of Sourcewell's Board of Directors. The policy shall be reviewed on a periodic basis and any modifications made thereto must be approved by Sourcewell's Board of Directors.



General Policies

Appreciation Awards

Each year at the Annual Employee Recognition Event, Appreciation Awards will be presented. Years of Service awards will be given to all full-time employees for every five (5) years of service. Additional awards and recognition may be given to employees at the discretion of the Executive Director/CEO.

Each year at the Annual Representative Assembly Meeting, departed Board of Director members will be presented an Appreciation Award, regardless of the length of service.

The Board of Directors may consider other awards and means of recognition as deemed necessary.

Drug, Cannabis, Alcohol, and Tobacco-Free Workplace and Testing Policy

I. Purpose

Sourcewell is committed to maintaining a safe work environment for its employees. As part of this commitment, Sourcewell maintains a drug, cannabis, alcohol, and tobacco-free workplace.

The purpose of this policy is to define:

- The specific acts prohibited by this policy.
- The circumstances under which Sourcewell may discipline or discharge an employee for violating the policy.
- The circumstances under which Sourcewell may request or require an employee to undergo drug, alcohol, or cannabis testing.

II. Scope

This policy applies to all employees and independent contractors while on Sourcewell property, in or operating vehicles, equipment, or machinery owned, leased, or rented by Sourcewell, and while conducting Sourcewell business. For ease of reading, employees and independent contractors will be collectively identified as “employees” herein.

III. Definitions

“Alcohol” means beer, wine, spirits, and medications that contain alcohol.

“Cannabis,” for purposes of this policy, means cannabis flower and cannabis consumer products, including edibles, which contain cannabis concentrate or have been infused with cannabinoids; medical cannabis flower; and medical cannabinoid products.

“Cannabis Testing” means the analysis of a body component sample to measure the presence or absence of cannabis, lower-potency hemp edibles, hemp-derived consumer products, or cannabis metabolites.

“Drug” means a controlled substance listed in Schedules I through V of Minnesota Statutes, § 152.02, and includes prescription drugs and over-the-counter medication. “Drug” does not include Cannabis or Hemp except for individuals working in the positions outlined in the “Drug and Alcohol Testing Policy” below.

“Drug and Alcohol Testing” means an analysis of a body component sample to measure the presence or absence of drugs, alcohol, or their metabolites. Drug or Alcohol Testing does not include Cannabis Testing except as stated in the “Drug and Alcohol Testing Policy” below.

“Edible” means a product eaten or consumed as a beverage that contains Cannabis in combination with food ingredients, including products that resemble nonalcoholic beverages, candy, and baked goods.

“Hemp,” for purposes of this policy, means consumer products and lower-potency edibles that contain or consist of hemp plant parts, the extracts or resins of a hemp plant or plant parts, or artificially derived cannabinoids in combination with other ingredients. “Hemp” does not include products that contain Cannabis.

“Impaired” or “Impairment” means an employee lacks the usual clarity of intellect and self-control they would typically possess.

“Lawful Consumable Product” means a product whose use or enjoyment is lawful, including food, alcoholic or nonalcoholic beverages, tobacco, Cannabis, and Hemp.

“Paraphernalia” means equipment, products, or materials used primarily to ingest, inhale, or otherwise introduce Cannabis into the body.

“Tobacco” means a product that contains tobacco or nicotine, including cigarettes, pipes, cigars, snuff, chewing tobacco, or e-cigarettes.

IV. Policy

A. Tobacco-Free Workplace

Sourcewell employees are prohibited from using Tobacco in any enclosed Sourcewell building or while in or operating vehicles, equipment, or machinery owned, leased, or rented by Sourcewell.

B. Alcohol-Free Workplace

Sourcewell employees are prohibited from using, possessing, being impaired by, selling, or transferring Alcohol on Sourcewell property and while operating vehicles, equipment, or machinery owned, leased, or rented by Sourcewell.

C. Drug and Cannabis-Free Workplace

Sourcewell employees are prohibited from using, possessing, being impaired by, selling, or transferring Drugs or Cannabis on Sourcewell property while operating Sourcewell vehicles, equipment, and machinery owned, leased, or rented by Sourcewell and while conducting Sourcewell business. This prohibition includes Lawful Consumable Products that have an intoxicating effect or impair the ability of an employee to work safely and effectively. Sourcewell employees are also prohibited from using, possessing, selling, or transferring Drug and Cannabis Paraphernalia on Sourcewell property while in or operating vehicles, equipment, or machinery owned, leased, or rented by Sourcewell and while conducting Sourcewell business.

Use of prescription medication or over-the-counter drugs during working hours is not a violation of this policy unless using such medication or drugs results or may result in the employee's impairment during work hours.

D. Drug-related Convictions

Any Sourcewell employee convicted of a state or federal misdemeanor or felony crime involving a controlled substance as defined in applicable state or federal law must inform Sourcewell within five (5) days of the conviction. If applicable, Sourcewell will notify the appropriate federal authority within the time prescribed by federal law or applicable contract.

E. Compliance

Sourcewell may discipline an employee for violating this policy, up to and including discharge. Sourcewell may not, however, take an adverse personnel action against an employee for engaging in the use of Lawful Consumable Products off Sourcewell property during nonworking hours unless:

1. As a result of consuming the Lawful Consumable Products, the employee lacks the usual clarity of intellect and self-control of self that they otherwise would have at work; and
2. Drug or Alcohol Testing conducted in accordance with the Testing Policy below verifies the presence of Drugs, Cannabis, Alcohol.

Drug and Alcohol Testing Policy¹

Sourcewell may require an employee to undergo Drug and Alcohol Testing when reasonable suspicion exists to believe the employee:

- Is impaired by or under the influence of Drugs, Cannabis, or Alcohol during working hours; or
- Has violated this policy; or
- Has sustained a personal injury or caused another Sourcewell employee to sustain an injury; or
- Has caused a work-related accident or was operating a vehicle, equipment, or machinery owned, leased, or rented by Sourcewell involved in a work-related accident.

Reasonable suspicion may be based upon observable facts regarding appearance, behavior, speech, breath, or odor. It may also stem from indicators such as possession, proximity to, or use of Drugs, Cannabis, or Alcohol, as well as the possession or the presence of containers or paraphernalia. Additionally, a poor safety record, frequent absenteeism, impaired job performance, or any other circumstances that would lead an employer to suspect a violation of this policy.

I. Cannabis Testing

Sourcewell may not require an employee to undergo testing solely for the purpose of determining the presence or absence of Lawful Consumable Products, including Cannabis, unless the employee works in:

- A safety-sensitive position, which includes any position in which impairment caused by Drug, Cannabis, or Alcohol use would threaten the health or safety of any person; or
- A position requiring face-to-face care, training, education, supervision, counseling, or consultation to children or vulnerable adults; or
- A position requiring a commercial driver's license; or
- A position funded by a federal grant; or
- Any other position for which state or federal law requires Cannabis Testing.

II. Right of Refusal

Employees have the right to refuse to submit to Drug, Cannabis, and Alcohol Testing. However, refusal may result in adverse personnel action up to and including termination. Intentional acts or omissions that prevent completion of the testing process, including the substitution, alteration, or attempt to substitute or alter a testing sample, constitutes refusal to submit to testing. Refusal to undergo blood testing on religious grounds will not constitute refusal to testing unless the employee also refuses to undergo testing of a urine sample.

III. Cost of Required Testing

Sourcewell will pay for the Drug, Cannabis, and Alcohol Testing requested or required of all employees. Sourcewell is not responsible for costs associated with Confirmatory Retests.

IV. Review and Notification of Test Results

Within three (3) working days after receiving testing results from the laboratory, Sourcewell will provide the employee with written notice of: (1) the test results; (2) the right to explain a positive test, including whether the employee is or has recently taken prescription or over the counter medication; (3) the employee's right to request a confirmatory retest, if applicable; and (4) any limitations on Sourcewell's ability to discipline or discharge the employee based on the test results.

Pursuant to Minn. Stat. § 181.953, subd. 10, an employee may access information contained in their personnel file relating to positive test results, the testing process, and any information gathered as part of that process.

¹ Sourcewell must conduct all testing in compliance with Minnesota Statutes, §§ 181.953 and 181.954.

IV. Policy

A. Tobacco-Free Workplace

Sourcewell employees are prohibited from using Tobacco in any enclosed Sourcewell building or while in or operating vehicles, equipment, or machinery owned, leased, or rented by Sourcewell.

B. Alcohol-Free Workplace

Sourcewell employees are prohibited from using, possessing, being impaired by, selling, or transferring Alcohol on Sourcewell property and while operating vehicles, equipment, or machinery owned, leased, or rented by Sourcewell.

C. Drug and Cannabis-Free Workplace

Sourcewell employees are prohibited from using, possessing, being impaired by, selling, or transferring Drugs or Cannabis on Sourcewell property while operating Sourcewell vehicles, equipment, and machinery owned, leased, or rented by Sourcewell and while conducting Sourcewell business. This prohibition includes Lawful Consumable Products that have an intoxicating effect or impair the ability of an employee to work safely and effectively. Sourcewell employees are also prohibited from using, possessing, selling, or transferring Drug and Cannabis Paraphernalia on Sourcewell property while in or operating vehicles, equipment, or machinery owned, leased, or rented by Sourcewell and while conducting Sourcewell business.

Use of prescription medication or over-the-counter drugs during working hours is not a violation of this policy unless using such medication or drugs results or may result in the employee's impairment during work hours.

D. Drug-related Convictions

Any Sourcewell employee convicted of a state or federal misdemeanor or felony crime involving a controlled substance as defined in applicable state or federal law must inform Sourcewell within five (5) days of the conviction. If applicable, Sourcewell will notify the appropriate federal authority within the time prescribed by federal law or applicable contract.

E. Compliance

Sourcewell may discipline an employee for violating this policy, up to and including discharge. Sourcewell may not, however, take an adverse personnel action against an employee for engaging in the use of Lawful Consumable Products off Sourcewell property during nonworking hours unless:

1. As a result of consuming the Lawful Consumable Products, the employee lacks the usual clarity of intellect and self-control of self that they otherwise would have at work; and
2. Drug or Alcohol Testing conducted in accordance with the Testing Policy below verifies the presence of Drugs, Cannabis, Alcohol.

Environmental Health and Safety

Purpose:

The purpose of this policy is to provide a healthy and safe environment for staff and the public by establishing and complying with health and safety standards. These standards will be based on federal, state, and local laws.

Policy:

The Director of Administration or their designee will be responsible for the establishment of a written set of Health and Safety Standards. The Director of Administration will be responsible for ensuring compliance with these standards through:

A. Training.

- a. Identify the staff groups who need to be informed about these standards.
- b. Develop and maintain a system of keeping the members of these staff groups informed about these standards and changes to these standards.

B. Reinforcing the roles and responsibilities of leaders.

- a. Building/Site Responsibilities
 - i. Directors, managers, and supervisors are responsible for their staff adhering to the health and safety program within their departments and ensuring that staff participates in the safety-training program.
- b. Human Resources Department Responsibilities
 - i. The Manager of Human Resources is responsible for coordinating the workers' compensation insurance policy and accident claim reporting with the insurance carrier.
 - ii. Human Resources is responsible for processing the First Report of Injury for submittal to the workers' compensation insurance carrier.
 - iii. Human Resources is responsible for ensuring all new staff receive Health and Safety training related to their position.
 1. Large group, small group, and individualized instruction for staff identified as exposed to a safety hazard will be offered.
 - iv. Human Resources is responsible for facilitating annual AWAIR training.
 1. The training curriculum shall follow the Occupational Health and Safety Administration guidelines, and staff shall receive their training during their normal work hours.
 2. Staff training records shall be maintained for a period of three years.
 3. Records shall be provided for review by regulatory inspectors and the public upon request.
- c. Director of Administration Responsibilities
 - i. The Director of Administration will develop and manage the implementation of the Health and Safety Program.
 - ii. The Director of Administration will establish and lead, or may designate another to lead, a Safety Committee. The committee will promote safety. The committee will be comprised of staff representing at least three (3) staff groups. The committee will also be responsible for:
 1. Facilitating action on health and safety concerns.
 2. Recommending health and safety program manual and procedure improvements.
 3. Reviewing accident reports to identify trends and recommend steps for accident reduction.
 4. Facilitating communications on health and safety issues.
 5. Supporting safety initiatives.
 - iii. Exposure Control Officer.
 1. The Building and Grounds Superintendent is the designated Exposure Control Officer and is responsible for facilitating SHARPS waste disposal and bloodborne pathogens.
 - iv. CPR / AED training will be offered to staff on a regular basis.

- v. The Director of Administration will establish and lead, or may designate another to lead, an Incident Management Team (IMT). The IMT will be comprised of certified first responders and facilities staff. The IMT will meet regularly to plan and conduct emergency drills (e.g., fire, tornado, violent intruder drills, etc.).

C. Infection Control

- a. Sourcewell will operate according to the standards promoted by the Occupational Health and Safety Administration for the prevention of bloodborne infections.
- b. All staff will be trained with current information regarding bloodborne pathogen exposure and procedures for handling blood and bodily fluids. Staff whose positions require additional training relevant to their positions and responsibilities will receive this training on an annual basis.
- c. All staff will consistently follow infection control procedures to prevent bloodborne pathogen exposure at all times. Sourcewell will supply personal protective equipment for the staff to meet infection control standards.
- d. In the event of a staff member's communicable disease exposure, staff will be directed to their private physician. The staff will complete an Exposure to Bloodborne Infectious Disease report and forward it to the Human Resources Department.

Exercise Facility Policy

Purpose:

Sourcewell provides an on-site exercise facility at its headquarters free of charge for employees, who are encouraged to take advantage of the facility to maintain a healthy lifestyle.

Policy:

The exercise facility is open Monday through Friday for use by employees during established hours. The hours of operation will be posted on or near the facility's doors and updated as necessary. A Buddy system must be utilized during non-office hours. Except for pre-approved programs*, all time spent using the exercise facility shall be considered non-work time, and employees shall have no claim for payment of this time. Non-employees are not permitted in the exercise facility.

Use of the exercise facility is considered a privilege. Employees not complying with policy and procedure may be asked to leave, be restricted, and/or banned from the facility. Employees are expected to:

- Utilize exercise equipment with care and in a safe and responsible manner.
- Wear appropriate clothing, including a shirt and shorts or pants that cover the legs to at least mid-thigh.
- Wear appropriate clean athletic shoes in all fitness areas; bare feet, sandals, or street shoes are not permitted.
- Be courteous to others by limiting the length of workouts, observing posted time limits, etc., when others are waiting.
- Return portable fitness equipment/items to appropriate locations after use.
- Be sensitive to other employees' privacy in all locker rooms or changing facilities, and, always treat each other with common courtesy, respect, and professionalism.
- Refrain from taking pictures or videos in any portion of the exercise facility to maintain other users' right to privacy.
- Abide by all terms of the Sourcewell Employee Handbook and Board Policies while at the exercise facility, including prohibitions against sexual harassment, harassment, and violence. Sexualized comments or actions are strictly prohibited.

* Sourcewell may, at its discretion, provide and/or approve fitness learning opportunities within the exercise facility. These will be considered pre-approved programs. All staff will be invited to participate, and the program(s) will clearly be identified as "pre-approved."

Facilities Use Policy

Sourcewell is committed to making the Sourcewell facilities and equipment available to the communities we serve. The purpose of this policy is to define the use of Sourcewell's Public & Semi-Private Facilities.

Definitions

Region 5 Sourcewell Members: For the purpose of this policy, Region 5 Sourcewell Members means all eligible school districts, cities, counties, and nonprofits of/or within the counties of Cass, Crow Wing, Morrison, Todd, and Wadena.

Regular business hours mean 8:00 a.m. – 4:30 p.m., Monday through Friday.

Sourcewell Semi-Private Facilities means the areas marked as “Semi-Private” on the Public Use Map attached hereto as **Appendix A**.

Facilities Use and Permit Procedure:

1. Any individual or entity (“Applicant”) may apply to use Sourcewell Semi-Private Facilities by submitting a Facility Use Request (“Request”) at least fourteen (14) days prior to the date of expected use.
2. Upon receipt of a Facility Use Request, designated Central Services staff shall grant or deny the Request based on the following criteria:
 - a. Decisions on incomplete Requests will be deferred until all necessary information has been provided by the Applicant.
 - b. Requests that comply with this Policy will be granted provided the use will not conflict with Sourcewell activities, events, and day-to-day operations.
 - c. Requests for the following uses will be denied:
 - i. Uses that conflict with or violates Sourcewell policy
 - ii. Uses that may be dangerous or harmful to Sourcewell facilities, grounds, equipment, staff, or visitors
 - iii. Uses that does not serve a public purpose
 - iv. Capital and endowment campaigns
 - v. Fundraising campaigns and individual benefit events
 - vi. Political and religious activities
 - d. Requests may also be denied if the Applicant has a history of failing to comply with this Facilities Use Policy.
3. When a Request for Facility Use is granted, designated Central Services staff shall:
 - a. Work with the Applicant to schedule their event in accordance with Sourcewell’s master calendar of activities;¹ and
 - b. Issue to the Applicant a Facilities Use Agreement detailing:

- c. The date(s) and time(s) during which the User may use the Sourcewell facilities;
 - d. Any fees due for use of the facilities and terms of payment determined in accordance with the Class and Rental Fee Schedule attached as **Appendix B**; and
 - e. The policies and procedures applicable to the User and their use of the facilities
4. The User shall sign the Agreement to express their acknowledgment and understanding of their obligations related to their use of the Sourcewell facilities.

Administrative Responsibility

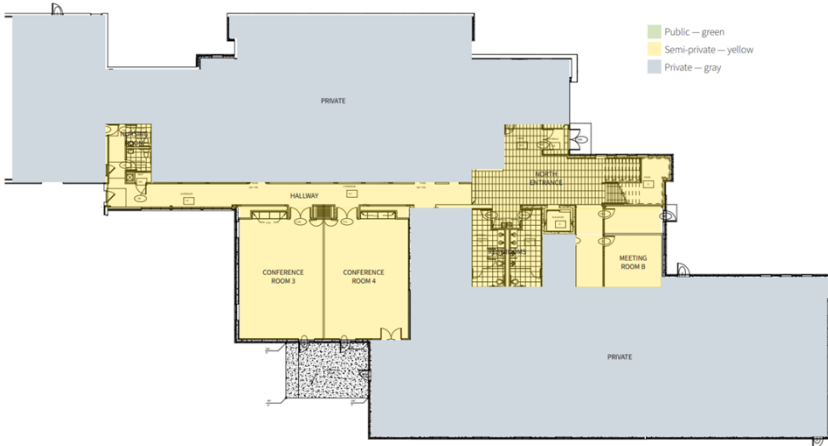
1. Sourcewell Administration reserves the right to deny any Application or terminate any Facilities Use Agreement, without liability, for any violation of this Facilities Use Policy or breach of the Facilities Use Agreement.
2. Sourcewell Central Services shall be responsible for fulfilling the following obligations with respect to this Facilities Use Policy:
 - a. Maintaining a master calendar of activities occurring at Sourcewell on a yearly, quarterly, weekly, and daily basis.
 - b. Assigning Sourcewell staff to be present and monitor events scheduled outside of regular business hours.
 - c. Preparing the facilities to suit the use(s) described in the Facilities Use Agreement.
 - d. Postponing or canceling events due to inclement weather or site limitations, such as water, heat, or utilities malfunction.

In the event of postponement or cancellation, there shall be no claim or right to damages or compensation on account of any loss, damage, or expenses whatsoever.

Appendix A: Public Use Map

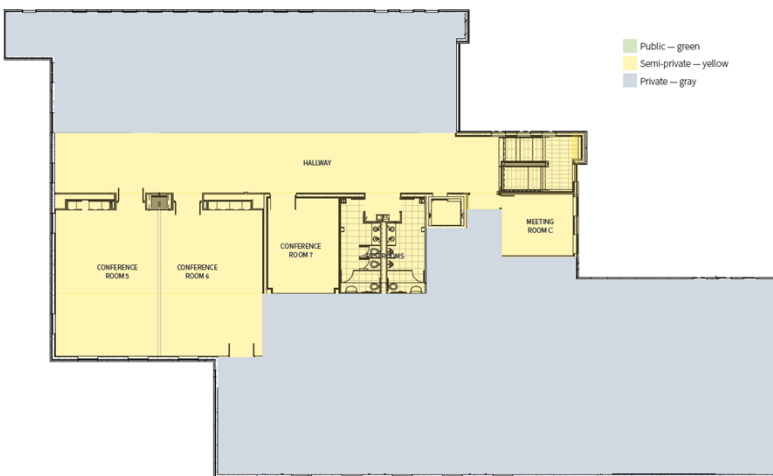
Public Use Map

First floor — South



Public Use Map

Second floor



Appendix B: Class and Rental Schedule

User fees and obligations are based on the User's class as follows:

CLASS A: Region 5 Sourcewell Members

- Facilities Use Agreement
- Custodial fee if event is held outside of regular business hours

CLASS B: Nonmember political subdivision (state, county, city, and local governmental entities), school districts, and youth, civic, service, charitable, and educational organizations

- Facilities Use Agreement
- Custodial fee
- Refundable deposit*

CLASS C: Commercial or for-profit organization

- Facilities Use Agreement
- Custodial fee
- Rental charge
- Refundable deposit *

*Refundable deposit shall be returned to the User after the event is complete provided that, in the sole discretion of Sourcewell Central Services staff, no damages have occurred.

Facilities Fee Schedule

Custodial Fee	\$50.00 per hour
Rental Fee	\$25.00 per hour
Technology Fee	\$50.00 per hour
Refundable deposit fee	\$250.00

Procurement Card

Purpose:

The purpose of this policy is to communicate eligibility, usage, and payment of expenditure requirements of the organizational credit card (Procurement card aka P-card).

Policy

1. Generally, Sourcewell will issue all employees a P-card during their initial onboarding process in Workday. During onboarding, cardholders are required to acknowledge the "Sourcewell Agreement to Accept the U.S. Bank One Card" indicating they accept these terms. Individuals who do not adhere to these policies and procedures risk revocation of their P-card privileges and/or disciplinary action.
2. Employees shall use their P-card to charge eligible business-related expenses. Personal purchases of any type are strictly prohibited. The P-card may NOT be used to obtain cash advances, bank checks, traveler's checks, or electronic cash transfers.
3. Initial limits are established by Finance. Limits may be increased by Finance upon request by the employee's supervisor.
4. Each employee is responsible for all charges made to their assigned card, with the exception of fraudulent charges outside the employee's control while exercising due diligence of the use of the P-card. Employees shall report fraudulent credit card charges immediately to the P-card company, and shall be available to Finance and the P-card company for resolution. Employees are also responsible for contacting the P-card company for lost P-cards.
5. Misuses of the P-card may result in suspension and/or withdrawal of P-card privileges.
6. Employee is responsible for reimbursing Sourcewell for unauthorized use charges of the P-card. Employees must coordinate with Finance to reimburse Sourcewell either through separate remittance or a deduction from the next available employee expense reimbursement.
7. Employees must submit detailed receipts for all transactions:
 - a. A detailed receipt is one which indicates at a minimum the date of the charge, the vendor/supplier, the item or service procured, and the amount of the charge. In the case of meals, receipts should detail the food and non-alcoholic beverages purchased, and should not be the signed credit card slip with only the total.
 - b. If a receipt has been lost, the Affidavit of Lost Receipt must be submitted in lieu of receipt.
 - i. Utilization of the Affidavit of Lost Receipt three or more times per fiscal year may result in a ninety-day (90) suspension of P-card on the third use. If lost receipts continue after the P-card is reinstated, permanent loss of P-card may occur.
8. Sourcewell may, at its own discretion, withdraw the employee's assigned P-card at any time and the employee agrees to surrender the P-card immediately upon request.

Cancellations and Refunds

Cancellations requested with more than 72 hours' notice before the start date will receive a refund of the registration fee minus any applicable credit card processing fees. Refunds will not be issued for no-shows or cancellations made within 72 hours of the event. Sourcewell reserves the right to postpone, reschedule or cancel at any time. In the unlikely event that we must cancel, a full refund will be issued.

On-demand courses

No refunds will be issued for on-demand courses once access to the content has been granted.

Removal of Existing Board Policies

Purpose:

To establish a system for removal of existing policies deemed outdated, no longer necessary, or ineffective for the administration of Sourcewell activities.

Policy:

When deemed necessary, the Sourcewell Board of Directors may remove policies from existing policies currently in effect.

The following process will be employed when removing existing policy:

1. Any policy being recommended for removal will be placed on the Agenda of a regularly scheduled board meeting, and the policy will be included as an enclosure.
2. At the scheduled board meeting, the Executive Director/CEO will provide the board rationale for removing the recommended policy. The board will be asked to review the current policy recommended for removal but will not take action until the next board meeting.
3. At the next scheduled board meeting, the Executive Director/CEO will ask for board action to remove the policy.
4. By a simple majority vote of the board, the recommended policy will be removed.

Travel Policy

I. Purpose:

It is Sourcewell's intent to ensure the safety of employees while providing them with a reasonable level of comfort and service while traveling on business and establish a system for travel that ensures the maximum use of financial resources.

II. Policy:

Sourcewell recognizes that employees, Board members, and nonemployees periodically travel on authorized business on behalf of Sourcewell. All travel shall be preapproved by immediate supervisors. For nonemployee travel, additional preapproval of a director is required.

Sourcewell leverages an online travel request software system that enables employees to request and book all travel (in-state and out-of-state) and receive approval from their immediate supervisor.

For nonemployee travel, the Sourcewell event specialists will work with the department to ensure travel arrangements are completed.

Sourcewell has implemented the following parameters within the travel request system:

A. Air travel

- Economy/coach class airfare
- Comparison of available flight times and airlines to receive the best value
- No airline first-class upgrades
- No use of rewards/miles/credits for upgrades

Airline frequent flyer mileage: Minn. Stat. 15.435 requires all frequent flyer miles earned by employees while on work-related travel to be credited to Sourcewell. Sourcewell employees and other officials using Sourcewell funds traveling on Sourcewell business and using commercial airlines that award frequent flyer miles cannot claim these frequent flyer miles as their own. Any benefits received belong to Sourcewell.

B. Lodging

- Reservations for **business travel only** (additional hotel nights due to personal travel, before or after the business event, must be arranged and paid for by the employee separately from business use and booked outside the travel request software system that Sourcewell utilizes)
- Hotel classes are limited
- Standard rooms

C. Rental vehicle

- Reservations for **business travel only** (additional use for personal travel must be arranged and paid for by the employee separately from business use and booked outside the travel request software system that Sourcewell utilizes)
- Up to mid-size car allowed
- GPS device or Bluetooth option allowed
- Selection of satellite radio not allowed

Any exceptions to this policy must be approved by the Executive Director/CEO.

WELLNESS POLICY

PURPOSE

The Sourcewell Board of Directors approves this Wellness Policy for all Sourcewell employees (collectively, “Employees”). The purpose of this policy is to promote good mental health and physical well-being for Sourcewell’s employees. This Wellness Policy describes Sourcewell’s efforts to promote mental health and physical well-being for its employees. The Sourcewell Executive Director may recommend periodic changes or additions to this policy.

The Board delegates to the Executive Director, in consultation with the Wellness Committee, the authority to determine what wellness benefits and other offerings to implement each year and to expend allocated funds to implement the agreed-upon benefits and offerings.

Wellness Offerings:

Wellness Incentives

Sourcewell employees receive employee health benefits through the Better Health Collective, the government joint risk pool sponsored by Sourcewell. The Better Health Collective strives to offer affordable employee health benefits. Employees can contribute to these efforts and earn cash incentives by engaging in wellness challenges, which can be viewed on the wellness portal administered by HealthSource Solutions. Cash incentives include, but are not limited to, On the Spot and wellness contest incentives. Employees can also use the wellness portal to track any wellness incentives earned.

Sourcewell employees will receive wellness incentives they earn and those earned by their spouse, if applicable, through payroll in July and January each year. Employees who receive wellness incentives intended for their spouse are responsible for passing the funds on to the appropriate recipient.

If an Employee is terminated, Sourcewell will pay those earned wellness incentives and those earned by their spouse to the employee, if applicable, within a reasonable time after the date of the Employee’s termination.

Employee Assistance Programs

The Employee Assistance Program offered through HealthPartners provides resources to employees to help them manage stress, be more productive at work, and live healthier every day. When employees need everyday support, the HealthPartners Employee Assistance Program (EAP) is your free and confidential partner to help with whatever life throws your way, 24/7. Think of your EAP as that life coach you always wanted and never knew you had until now. Whatever you're struggling with — whether it be mental health, financial concerns, childcare, elder care, navigating challenging relationships, your career, and more — they are there no matter what with tailored, free and confidential support for you and your household. Employees can participate in unlimited phone calls and up to three (3) counseling sessions each year.

Omada

Omada provides cognitive behavioral therapy to assist with weight loss, diabetes, and hypertension. Employees are encouraged to take a free assessment to determine if they are eligible to participate in Omada. If so, the Employee may enroll in the multi-week program free of charge.

HealthPartners Disease and Case Management Programs

HealthPartners disease and case management programs provide optimal care and reduce costs for Employees with specific health conditions, including, but not limited to, pregnancy, cancer, and medication therapy management. HealthPartners will identify and contact eligible Employees.

Other Wellness Benefits

Sourcewell also offers the following benefits:

- Flu Shots
- Biometric Screenings
- Onsite exercise facilities
- Healthy snacks onsite
- Lunch & Learn programs and meals
- Wellness t-shirts
- Other Professional Development opportunities
- Wellbeats, a free online exercise platform
- HealthSource Solutions, a monthly wellness newsletter

Wellness Events

Sourcewell may sponsor and pay all or a portion of costs for wellness activities for Employees and Employees' families. Examples of wellness activities include but are not limited to, ice skating, golf, curling, flag football, and frisbee golf; arts and crafts opportunities; visits to an apple orchard, planetarium, or other local attraction; or participation in the Sourcewell 5K; and Adopt-a-Highway cleanup events.

Compensation

Cash or cash equivalent payments or incentives are compensation and will be treated appropriately for tax purposes.



Legal Policies

Sourcewell Data Practices Policy, Data Inventory, and Records Retention Schedule

I Data Practices Policy for the Public

A. Your Right to See Public Data

The Government Data Practices Act (Minnesota Statutes, Chapter 13) presumes that all government data are public unless a state or federal law says the data are not public. Government data means all recorded information a government entity has, including paper, email, digital, flash drives, CDs, DVDs, photographs, etc.

The law also says that Sourcewell must keep all government data in a way that makes it easy for you to access public data. You have the right to look at (inspect), free of charge, all public data Sourcewell keeps. You also have the right to get copies of public data. The Data Practices Act allows Sourcewell to charge for copies. You have the right to look at data, free of charge, before deciding to request copies.

B. How to Request Public Data

You can ask to look at (inspect) data at the Sourcewell offices or ask for copies of public data that Sourcewell keeps by submitting a written data request to:

Chad Coquette, Responsible Authority
Sourcewell
202 – 12th Street NE
PO Box 219
Staples, MN 56479

Pursuant to Minnesota Statutes, section 13.02, subd. 6, Sourcewell's Responsible Authority has designated its Senior Leadership Team to oversee the government data maintained by each of their department(s). Pursuant to Minnesota Statutes, section 13.05, subd. 13, the Responsible Authority has also appointed these individuals to serve as the Data Practices Compliance Official for their respective department(s). See [Appendix A](#) for a list of the Designees and the department(s) for which each is responsible.

You may use the Data Request Form – Requesting Public Data found below.

If you do not use the Data request Form, your request should:

- Say that you are making a request for public data under the Government Data Practices Act;
- Include whether you would like to inspect the data, have copies of the data, or both; and
- Provide a clear description of the data you would like to inspect or have copied.

You are not required to identify yourself or explain the reason for your data request. However, you may need to provide Sourcewell with some personal information for practical reasons (for example: if you want Sourcewell to mail copies to you, you need to provide Sourcewell staff with an address or P.O Box). If Sourcewell staff do not understand your request and have no way to contact you, Sourcewell cannot respond to your request.

C. How We Will Respond to Your Data Request

Upon receiving your request, Sourcewell staff will review it.

- Sourcewell may ask you to clarify what data you are requesting.
- If Sourcewell does not have the data, staff will notify you in writing as soon as reasonably possible.
- If Sourcewell has the data but is not allowed to give it to you, staff will tell you as soon as reasonably possible and identify the law that prevents Sourcewell from providing the data.

- If Sourcewell has the data, and the data are public, staff will respond to your request appropriately and promptly, within a reasonable amount of time by doing one of the following:
 - Arrange a date, time, and place for you to inspect the data at the Sourcewell offices; or
 - Invite you to pick up your copies, or Sourcewell will mail or email them to you.

You may be required to prepay for your copies. (See (F) below regarding copy costs.) Sourcewell will provide electronic copies (such as email or CD-ROM) upon request, if it keeps the data in that format and can reasonably make a copy. Response time may be impacted by the size and/or complexity of your request, and by the number of requests you make in each period.

Following our response, if you do not make arrangements within ten (10) business days to inspect the data or pay for the copies, we will conclude that you no longer want the data and will consider your request closed.

If you do not understand some of the data (technical terminology, abbreviations, or acronyms), please tell the person who provided the data to you. Sourcewell will give you an explanation if you ask.

The Data Practices Act does not require Sourcewell to create or collect new data in response to a data request, or to provide data in a specific form or arrangement if Sourcewell does not keep the data in that form or arrangement. For example, if the data you request are on paper only, Sourcewell is not required to create electronic documents to respond to your request. If Sourcewell agrees to create data in response to your request, Sourcewell will work with you on the details of your request, including cost and response time.

Sourcewell is also not required to respond to questions that are not about your data requests or other requests for government data.

D. Requests for Summary Data

Summary data are statistical records or reports created by removing identifying information about individuals from entirely private or confidential data.

Sourcewell will prepare summary data if you make your request in writing and pre-pay for the cost of creating the data.

You may use the Data Request Form – Requesting Public Data below to request summary data. Sourcewell will respond to your request within ten (10) business days with the data or details of when the data will be ready and how much Sourcewell will charge you.

E. Data Practices Contacts

Responsible Authority

Chad Coauette, Chief Executive Officer

Sourcewell

202 – 12th Street NE

PO Box 219

Staples, MN 5647

877-585-9706

service@sourcewell-mn.gov

See **Appendix A** for a list of Designees appointed by the Responsible Authority and the department(s) for which each is responsible.

F. Copy Costs – When You Request Public Data

Minnesota Statutes, section 13.03, subdivision 3(c) allows Sourcewell to charge for copies. The Responsible Authority or their Designee may waive such charges in their discretion.

*You must pay for the copies before we will give them to you.
If possible, and upon request, we will provide you with an estimation of the total cost of supplying copies.*

For 100 or Fewer Paper Copies – 25 cents per page

One hundred or fewer pages of black and white, letter or legal-size paper copies cost 25¢ for a one-sided copy or 50¢ for a two-sided copy. Sourcewell will charge for copies when the total cost is over \$1.

Most Other Types of Copies – Actual Cost

The charge for most other types of copies, when a charge is not set by statute or rule, is the actual cost of searching for and retrieving the data and making the copies or electronically sending the data.

In determining the actual cost of making copies, Sourcewell includes employee time, the cost of the materials onto which staff are copying the data (paper, CD, DVD, etc.), and mailing costs (if any). If your request is for copies of data that Sourcewell cannot copy itself, such as photographs, it will charge you the actual cost Sourcewell must pay an outside vendor for the copies.

If, based on your request, Sourcewell finds it necessary for a higher-paid employee to search for and retrieve the data, Sourcewell will calculate search and retrieval charges at the higher salary/wage.

G. Data Having Commercial Value - Enhanced Remote Access

Pursuant to Minnesota Statutes, section 13.03, subdivision 3(d), when you request copies of public data that has commercial value or data that was developed with a significant expenditure of public funds, Sourcewell may charge a reasonable fee for the information in addition to the costs of making and certifying the copies.

Pursuant to Minnesota Statutes, section 13.03, subdivision 3(e), If you request copies of public data in a format that is different from the format or program in which the data are maintained by Sourcewell, Sourcewell may require you to pay the actual cost of providing the data in the format you request.

H. Data Request Form – Requesting Public Data

Request date:

The data I am requesting:

Describe the data you are requesting as specifically as possible.

I am requesting access to data in the following way:

- Inspection
- Copies
- Both inspection and copies

Note: Inspection is free, but we charge for copies when the cost is over \$1.

Contact information (optional)*

Name: _____

Phone Number: _____

Email Address: _____

Address: _____

Sourcewell will respond to your request as soon as reasonably possible.

* You do not have to provide any contact information. However, if you want Sourcewell to mail/email you copies of data, Sourcewell will need some type of contact information. Sourcewell will also need contact information if staff do not understand your request. Sourcewell will not work on your request until staff can clarify it with you.

II. Data Practices Policy for Data Subjects

A. What is a “Data Subject”?

When government has information recorded in any form (paper, hard drive, voicemail, video, email, etc.), that information is called “government data” under the Government Data Practices Act (Minnesota Statutes, Chapter 13). When Sourcewell can identify you in government data, you are the “data subject” of that data. The Data Practices Act gives you, as a data subject, certain rights. This policy explains your rights as a data subject and tells you how to request data about you, your minor child, or someone for whom you are the legal guardian.

B. When Sourcewell has Data About You

Sourcewell has data on many people, such as grant applications, education reporting, professional development materials, and public procurement records. Sourcewell can collect and keep data about you only when it has a legal purpose to have the data. Sourcewell must also keep all government data in a way that makes it easy for you to access data about you.

Government data about an individual have one of three “classifications.” These classifications determine who is legally allowed to see the data. Data about you are classified by state law as public, private, or confidential.

1. Public Data

The Data Practices Act presumes that all government data are public unless a state or federal law says that the data are not public. Sourcewell must give public data to anyone who asks. It does not matter who is asking for the data or why the person wants the data. The following are examples of public data about you that Sourcewell might have: your name and contact information if you have participated in professional development activities or submitted a requisition for purchase through Sourcewell.

2. Private data

Sourcewell cannot give private data to the general public. It can share your private data with you, with someone who has your permission, with Sourcewell staff whose job requires or permits them to see the data, and with others as permitted by law or court order. The following are examples of private data about you that Sourcewell might have information regarding your participation in programs or services provided by Sourcewell through a contract with your county or school district.

3. Confidential Data

Confidential data have the most protection. Neither the public nor you can access confidential data even when the confidential data are about you. Sourcewell can share confidential data about you with Sourcewell staff who have a work assignment to see the data, and to others as permitted by law or court order. The following is an example of confidential data about you: information about your involvement in sexual harassment or discrimination claim involving Sourcewell.

C. Your Rights Under the Government Data Practices Act

As a data subject, you have the following rights.

1. Access to Your Data

You have the right to look at (inspect), free of charge, public and private data that Sourcewell keeps about you. You also have the right to get copies of public and private data about you. The Data Practices Act allows Sourcewell to charge for copies. You have the right to look at data, free of charge, before deciding to request copies.

Also, if you ask, Sourcewell staff will tell you whether Sourcewell keeps data about you and whether the data are public, private, or confidential.

As a parent, you have the right to look at and get copies of public and private data about your minor children (under the age of 18). As a legally appointed guardian, you have the right to look at and get copies of public and private data about an individual for whom you are appointed guardian.

Minors have the right to ask us not to give data about them to their parent or guardian. If you are a minor, we will tell you that you have this right. We will ask you to put your request in writing and to include the reasons that we should deny your parents access to the data. We will make the final decision about your request based on your best interests.

2. When We Collect Data from You

When Sourcewell asks you to provide data about yourself that are not public, it must give you a notice called a Tennesen warning. The notice controls what Sourcewell can do with the data that it collects from you. Usually, Sourcewell can use and release the data only in the ways described in the notice. Sourcewell will ask for your written permission if it needs to use or release private data about you in a different way, or if you ask Sourcewell to release the data to another person. This permission is called informed consent.

If you want us to release data to another person, you may use the consent form we provide.

3. Protecting Your Data

The Data Practices Act requires Sourcewell to protect your data. Sourcewell has established appropriate safeguards to ensure that your data are safe.

In the unfortunate event that Sourcewell determines a security breach has occurred and an unauthorized person has gained access to your data, Sourcewell will notify you as required by law.

4. When Your Data are Inaccurate or Incomplete

You have the right to challenge the accuracy and/or completeness of public and private data about you. You also have the right to appeal Sourcewell's decision. If you are a minor, your parent or guardian has the right to challenge data about you.

D. How to Make a Request for Your Data

You can ask to look at (inspect) data at the Sourcewell offices or ask for copies of data that Sourcewell has about you, your minor child, or an individual for whom you have been appointed legal guardian.

You may make your request in writing by mail, fax, or email to the attention of Chad Coquette, using the Data Request Form.

Sourcewell recommends using the sample **Data Request Form – Data Subjects** below. If you do not choose to use the Data Request Form, your request should:

- Say that you are making a request as a data subject, for data about you (or your child, or person for whom you are the legal guardian), under the Government Data Practices Act (Minnesota Statutes, Chapter 13);
- Include whether you would like to inspect the data, have copies of the data, or both;
- Provide a clear description of the data you would like to inspect or have copied; and
- Provide proof that you are the data subject or data subject's parent/legal guardian.

Sourcewell requires proof of your identity before staff can respond to your request for data. If you are requesting data about your minor child, you must show proof that you are the minor's parent. If you are a legal guardian, you must show legal documentation of your guardianship. Please see the Standards for Verifying Identity below. If you do not provide proof that you are the data subject, Sourcewell cannot respond to your request.

E. How Sourcewell Responds to a Data Request

Upon receiving your request, Sourcewell will review it.

- Staff may ask you to clarify what data you are requesting.
- Staff will ask you to confirm your identity as the data subject.
- If Sourcewell does not have the data, staff will notify you within ten (10) business days.
- If Sourcewell has the data, but the data are confidential or not public data about someone else, staff will notify you within ten (10) business days and identify the law that prevents Sourcewell from providing the data.
- If Sourcewell has the data, and the data are public or private data about you, staff will respond to your request within ten (10) business days by doing one of the following:
 - Arrange a date, time, and place to inspect data in Sourcewell offices, for free; or
 - Provide you with the data within ten (10) business days. You may choose to pick up your copies, or Sourcewell will mail or fax them to you. Sourcewell will provide electronic copies (such as email or CD-ROM) upon request if it keeps the data in electronic format
- Staff will notify you that you must prepay for your copies, if applicable.
- Following our response, if you do not make arrangements within ten (10) days to inspect the data or pay for the copies, Sourcewell will conclude that you no longer want the data and will consider your request closed.
- After Sourcewell has provided you with your requested data, Sourcewell does not have to show you the same data again for six (6) months unless there is a dispute about the data or Sourcewell collects or creates new data about you.

If you do not understand some of the data (technical terminology, abbreviations, or acronyms), please tell the person who provided the data to you. Sourcewell will give you an explanation if you ask.

The Data Practices Act does not require Sourcewell to create or collect new data in response to a data request, or to provide data in a specific form or arrangement if Sourcewell does not keep the data in that form or arrangement. For example, if the data you request are on paper only, Sourcewell is not required to create electronic documents to respond to your request. If Sourcewell agrees to create data in response to your request, staff will work with you on the details of your request, including cost and response time.

In addition, Sourcewell is not required to respond to questions that are not about your data requests, or that are not requests for government data.

F. Data Practices Contacts

Responsible Authority

Chad Coauette, Chief Executive Officer

Sourcewell

202 – 12th Street NE

PO Box 219

Staples, MN 5647

877-585-9706

service@sourcewell-mn.gov

See **Appendix A** for a list of Designees appointed by the Responsible Authority and the department(s) for which each is responsible.

G. Copy Costs – Data Subjects

Minnesota Statutes, section 13.04, subdivision 3 allows Sourcewell to charge for copies. If Sourcewell intends to charge you for your copies, staff will notify you in advance.

*You must pay for the copies before staff will give them to you.
Sourcewell does not charge for copies if the cost is less than \$1.*

Actual Cost of Making the Copies

Sourcewell may charge the actual cost of making copies for data about you. In determining the actual cost, Sourcewell includes the employee time to create and send the copies, the cost of the materials onto which staff are copying the data (paper, CD, DVD, etc.), and mailing costs such as postage (if any).

If your request is for copies of data that Sourcewell cannot copy ourselves, such as photographs, Sourcewell will charge you the actual cost we must pay an outside vendor for the copies.

H. Data Having Commercial Value - Enhanced Remote Access

Pursuant to Minnesota Statutes, section 13.03, subdivision 3(d), when you request copies of public data that has commercial value or data that was developed with a significant expenditure of public funds, Sourcewell may charge a reasonable fee for the information in addition to the costs of making and certifying the copies.

Pursuant to Minnesota Statutes, section 13.03, subdivision 3(e), If you request copies of public data in a format that is different from the format or program in which the data are maintained by Sourcewell, Sourcewell may require you to pay the actual cost of providing the data in the format you request.

I. Data Request Form – Data Subject

Request date:

Contact information:

Data Subject Name: _____

Parent/Guardian Name (if applicable): _____

phone number/email address: _____

To request data as a data subject, you must show a valid state ID, such as a driver's license; military ID; or passport as proof of identity.

The data I am requesting:

Describe the data you are requesting as specifically as possible.

I am requesting access to data in the following way:

- Inspection
- Copies
- Both inspection and copies

Note: Inspection is free but, Sourcewell will charge for copies when the cost is over \$1.

Sourcewell will respond to your request within ten (10) business days

To Be Completed by Staff Member Responding to Data Request:

Identity Confirmed:

Date:

Staff Name:

J. Standards For Verifying Identity

The following constitute proof of identity:

- An adult individual must provide a valid photo ID, such as
 - a driver's license
 - a state-issued ID
 - a tribal ID
 - a military ID
 - a passport
 - the foreign equivalent of any of the above
- A minor individual must provide a valid photo ID, such as
 - a driver's license
 - a state-issued ID (including a school/student ID)
 - a tribal ID
 - a military ID
 - a passport
 - the foreign equivalent of any of the above
- The parent or guardian of a minor must provide a valid photo ID and either
 - a certified copy of the minor's birth certificate or
 - a certified copy of documents that establish the parent or guardian's relationship to the child, such as
 - a court order relating to divorce, separation, custody, foster care
 - a foster care contract
 - an affidavit of parentage
- The legal guardian for an individual must provide a valid photo ID and a certified copy of appropriate documentation of formal or informal appointment as guardian, such as
 - court order(s)
 - valid power of attorney

Note: Individuals who do not inspect data or pick up copies of data in person may be required to provide either notarized or certified copies of the documents that are required or an affidavit of ID.

III. Data Practices and Records Retention Policy

A. Minnesota Government Data Practices Act and Minnesota Records Management Act

The Minnesota Government Data Practices Act at Minnesota Statutes, Chapter 13, regulates the collection, creation, storage, maintenance, dissemination, and access to government data in government entities. It establishes a presumption that government data are public and reasonably accessible for inspection and copying unless the data are classified as not public by state or federal law, or temporary classification.

1. Data Inventory

Minnesota Statutes, section 13.025, requires the Responsible Authority for each government entity to prepare an inventory containing the Responsible Authority's name, title address, and a description of each category of record, file, or process relating to private or confidential data maintained by the entity.

The inventory must be posted in a conspicuous place at the entity's office or on its website.

2. Data Index

Under Minnesota Rules 1205.1500, the Responsible Authority is also required to prepare an index describing all data collected, stored, used, or disseminated by the entity and identifying the law authorizing the functions for which data are collected.

The index must be available to the general public, upon request, and it must be updated when new or different data collection or use is authorized.

3. Records Retention Schedule

Minnesota Statutes, section 138.17, subd. 7, requires the head of each government entity to establish and maintain an active, continuing program for the economical and efficient management of the records in its custody. This includes preparing an inventory of the records in the entity's custody and establishing a period for the retention or disposal of each series of records. Each entity must also maintain a list of records it has disposed. In accordance with Minnesota Statutes, section 325L.12, Sourcewell may retain electronic records of any data subject to this retention policy.

B. Policy

The Data Practices and Records Retention Policy and the Sourcewell Data Inventory and Records Retention Schedule serve as Sourcewell's compliance with these requirements.

Sourcewell's current Data Inventory and Records Retention Schedule is attached as Appendix B. The retention period listed represents the minimum period records will be retained. Sourcewell may, in its discretion, maintain a particular record for longer than the listed retention period.

Appendix A: Designees and their Department

Jeremy Schwartz	Administration, Human Resources, and Building Facilities	Sourcewell 202 – 12 th Street NE PO Box 219 Staples, MN 56479 218-894-5488 Jeremy.schwartz@sourcewell-mn.gov
	Operations and Procurement, Information and Technology	
Robb Reid	Enterprise Solutions, Cooperative Purchasing, Government Accounts, and Category Development	Sourcewell 202 – 12 th Street NE PO Box 219 Staples, MN 56479 218-541-5246 Robb.reid@sourcewell-mn.gov
TBD	Legal and Government Relations	Sourcewell 202 – 12 th Street NE PO Box 219 Staples, MN 56479
Travis Bautz	Marketing	Sourcewell 202 – 12 th Street NE PO Box 219 Staples, MN 56479 218-895-4194 Travis.bautz@sourcewell-mn.gov
Paul Drange	Regional Programs and Education Solutions	Sourcewell 202 – 12 th Street NE PO Box 219 Staples, MN 56479 218-895-4134 Paul.drange@sourcewell-mn.gov
Mike Carlson	Finance	Sourcewell 202 – 12 th Street NE PO Box 219 Staples, MN 56479 218-895-4158 Mike.carlson@sourcewell-mn.gov

Appendix B: Sourcewell Data Inventory and Records Retention Schedule

Administration, Human Resources and Building Facilities – Jeremy Schwartz, Designee					
Item	Title	Description	Retention Period	Archival	Classification
1	Affidavits of Publication	Public hearings, budget publications, debt offerings	1 year after audit	No	Public
2	Annual Reports	Report specified by §123A.21	Permanent	Yes	Public
3	Authority to Dispose of Records	Requests to dispose under Minn. Stat. §§ 13.32; 13.39; 13.43.	6 years	No	Public/Private
4	Board Minutes	Meetings of Sourcewell Board of Directors	Permanent	Yes	Public
5	Board Policies	All policies adopted by the Sourcewell Board of Directors.	3 years	No	Public
6	Building Maintenance & Repair Records	Work orders for building maintenance, repairs, and damage.	1 year	No	Public
7	Committee Minutes	Meetings of official committees designated by the Board.	Permanent	Yes	Public
8	Election Records	Ballots, Notices, Notifications, Publications	For the duration of the (elected or appointed) term of office	No	Public
9	Facilities Records	Specs, blueprints, deeds, titles, and inspection reports.	Permanent	No	Public

10	Fixed Asset Records	Inventories and depreciation schedules.	Life of Item	No	Public
11	Leases Landlord/Tenant	Leases, licenses, and access agreements.	6 years	No	Public
12	Joint Powers Agreements	Agreements between Sourcewell and other entities.	Permanent	No	Public
13	Minutes-Tape Recordings	Board Minutes only	Until transcribed	No	Public
14	OSHA-Citations of Penalty	Notifications of Violations	Until violation has been corrected	No	Private/Public Minn. Stat. § 13.43
15	OSHA-Employee Accident Reports	OSHA Report Numbers 200 and 101	5 years after incident	No	Private/Public Minn. Stat. § 13.43
16	OSHA-Employee Exposure Records	Records of exposure to toxins/harmful physical agents.	30 years	No	Private/Public Minn. Stat. § 13.43
17	Safety Committee	Meeting Agendas and Minutes.	3 Years	No	Public
18	Training Records-Right to Know	MSDS	3 years	No	Public
19	Hazardous Waste Disposal	Disposal Manifest	Permanent	No	Public
20	AHERA	Abatement Files and Management Plans	Permanent	No	Public
21	Human Resources	Employee Medical Records	30 years after separation.	No	Private Minn. Stat. § 13.384; § 13.43

22	Human Resources	Request for Leave/Leave of Absence Reports	6 years after separation.	No	Public/Private Minn. Stat. § 13.43
23	Human Resources	Sexual Harassment Discrimination Claim Records	Until final disposition of charge	No	Public/Private Minn. Stat. § 13.43; § 13.39
24	Human Resources	First Report of Injury	Permanent in worker's comp file; 20 years for others	No	Private Minn. Stat. § 13.43; § 176.231
25	Applicant Records – Not Hired	Applications, resume, cover letter, interview documentation and notes, inquiries, rejection letter, and related records.	2 years	No	Private Minn. Stat. § 13.43
26	Applicant Records - Hired	Applications, resume, cover letter, supporting documents, interview documentation, inquiries, and offer letter.	6 years after termination	No	Minn. Stat. § 13.43
27	Human Resources	Arbitration Decisions	Permanent	No	Public/Private Minn. Stat. § 13.43
28	Human Resources	EEOC/MNCRIS Reports/Summary Data	3 years	No	Public 29 C.F.R. 1602.39
29	Human Resources	Grievance Files	Permanent	No	Public/Private Minn. Stat. § 13.43
30	Human Resources	Insurance Group Master Policies and Agreements	6 years	No	Public
31	Human Resources	Insurance Census Premium Reports	6 years	No	Public/Private Minn. Stat. § 13.43
32	Human Resources	STARS Report-Annual Report to State	1 year or until superseded	No	Public
33	Human Resources	Insurance Enrollment cards	Until superseded	No	Public/Private Minn. Stat. § 13.43

34	Human Resources	Insurance Records: Employees on Leave of Absence, FMLA, Long-Term Disability, Retired, Surviving Spouse, Terminated	2 years after termination	No	Public/Private Minn. Stat. § 13.43
35	Human Resources	Labor Contracts	Available in current state	Yes	Public
36	Human Resources	Long Term Disability Claims/Awards	10 years after resolution.	No	Public/Private Minn. Stat. § 13.43
37	Human Resources	Job Descriptions	Superseded	No	Public
38	Human Resources	Mediation Records	Permanent	No	Public
39	Human Resources	Negotiation Records	2 years	No	Public/Private Minn. Stat. Ch. 13D
40	Human Resources	Pay Equity Reports	Permanent	No	Public
41	Human Resources	Employee's Response Letter to Human Resources File	Same as document	No	Public/Private Minn. Stat. § 13.43
42	Human Resources	Seniority lists	1 year after separation.	No	Public 29 CFR 1627.3(b)
43	Human Resources	Recruitment records.	2 years	No	Public/Private Minn. Stat. § 13.43
44	Human Resources	Claims Summary and other information from the carrier.	6 years after separation	No	Public/Private Minn. Stat. § 13.43
45	Budget/Budget Records	Budget proposals, approved budget, includes supporting data and monthly department budget report	2 years	No	Public Minn. Stat. § 13.03

46	Electronic Calendars	Outlook	Available in current state and back 10 years	No	Public, unless an exception applies
47	Contracts/Agreements	Contracts/agreements and supporting documentation, including official publications, RFPs, responses, etc.	10 years after expiration	No	Public
48	Correspondence	Routine correspondence and memoranda.	3 years	No	Varies with subject of correspondence
49	Grant Applications – Successful	Application, correspondence, and supporting documents.	3 years	No	Public
50	Grant Applications – Unsuccessful	Applications, correspondence, and supporting documents.	1 year	No	Public
51	Expense Records	Documentation of departmental expenses, purchase orders, invoices, claims forms, etc.	6 years	No	Public
52	Meeting Minutes	Minutes recording actions taken in meetings necessary for the management of the department and its activities.	6 years	Yes	Public
53	Procedures	Procedures	Until superseded	No	Public

Enterprise Solutions, Supplier Development, Client Relations and Category Development – Robb Reid, Designee

Item	Title	Description	Retention Period	Archival	Classification
1	Budget/Budget Records	Budget proposals, approved budget, includes supporting data and monthly department budget report	2 years	No	Public Minn. Stat. § 13.03
2	Electronic Calendars	Outlook	Available in current state and back 10 years	No	Public, unless an exception applies

3	Contracts/Agreements	Contracts/agreements and supporting documentation, including official publications, RFPs, responses, etc.	10 years after expiration	No	Public
4	Correspondence	Routine correspondence and memoranda.	3 years	No	Varies with subject of correspondence
5	Grant Applications – Successful	Application, correspondence, and supporting documents.	3 years	No	Public
6	Grant Applications – Unsuccessful	Applications, correspondence, and supporting documents.	1 year	No	Public
7	Expense Records	Documentation of departmental expenses, purchase orders, invoices, claims forms, etc.	6 years	No	Public
8	Joint Powers Agreements	Contracts with other government units.	Permanent	Yes	Public
9	Meeting Minutes	Minutes recording actions taken in meetings necessary for the management of the department and its activities.	6 years	Yes	Public
10	Procedures	Procedures	Until superseded	No	Public

Finance – Mike Carlson, Designee

Item	Title	Description	Retention Period	Archival	Classification
1	Real Estate	Abstracts, deeds, title papers, and mortgages.	Permanent	No	Public
2	Year-End Reports	Year End-Revenue/Expense Reports (Summary and Detailed)	Permanent	No	Public

3	Year-End Reports	Year End-UFARS Revenue/Expense Reports to State	Permanent	No	Public
4	Year-End Reports	Year-End Special Funded Projects Report	Permanent	No	Public
5	Year-End Reports	Year-End Clerk's and Treasurer's Reports	Permanent	No	Public
6	Year-End Reports	Year-End Journals, Check Register, Budget Publications, Balance Sheets, and Budgets	Permanent	No	Public
7	Audits	Audit Reports	Permanent	No	Public
8	Investments	Bond Issues – Official Statements	Permanent	No	Public
9	Investments	Tax Sheltered Annuity Contracts	Permanent	No	Private/Public Minn. Stat. § 13.43;
10	Investments	Tax Sheltered Annuity Authorizations – 457 and 403(b) Plans	Permanent	No	Private/Public Minn. Stat. § 13.43
11	Year-End	Year-End Accounts Receivable Receipts, Invoices, Remittances	6 years	No	Public
12	Banking	Bank Statements and Reconciliation	6 years	No	Private/Public Minn. Stat. § 13.43
13	Taxes	County Auditor Statements and Reports	6 years	No	Public
14	Accounts Payable	Checks, disbursements, freight bills/claims, invoices, credit memos, claims/vouchers, 1099 forms, and inventory records	6 years	No	Private/Public Minn. Stat. § 13.43

15	Payroll	Cafeteria Plan Records	6 years	No	Private/Public Minn. Stat. § 13.43
16	Payroll	Payroll Register	6 years 29 C.F.R. 1627.3(a)	No	Private/Public Minn. Stat. § 13.43
17	Payroll	PERA Eligibility Sheets and Reports	6 years	No	Private/Public Minn. Stat. § 13.43
18	Payroll	Prior Years' Quarterly FICA	6 years	No	Private/Public Minn. Stat. § 13.43
19	Payroll	Salary Deduction	6 years	No	Private/Public Minn. Stat. § 13.43
20	Payroll	Stop Payment Orders and Bonds	6 years	No	Private/Public Minn. Stat. § 13.43
21	Payroll	Tax Reports	6 years	No	Private/Public Minn. Stat. § 13.43
22	Payroll	Time Sheets	6 years	No	Public
23	Payroll	TRA/PERA-Retirement Remittance Reports	6 years	No	Private/Public Minn. Stat. § 13.43
24	Payroll	W-2 Statements and W-4 Statements	6 years	No	Private/Public Minn. Stat. § 13.43
25	Purchasing	Acknowledgements/Orders/ Shipping Notices	6 years	No	Public
26	Purchasing	Bills of Lading	6 years	No	Public

27	Purchasing	Requisitions for Purchase	6 years	No	Public
28	Purchasing	Purchase Orders	6 years	No	Public
29	Purchasing	W-9 Form	6 years	No	Public
30	Purchasing	Statement of Pledged Securities	6 years	No	Public
31	Finance	Dues deduction authorizations.	3 years	No	Private/Public Minn. Stat. § 13.43
32	Finance	Garnishments	3 years	No	Private/Public Minn. Stat. § 13.43
33	Finance	Quarterly Report of Local Government Wages	3 years	No	Public
34	Finance	Leases/Agreements	3 years	No	Public
35	Finance	Replacement requests – lost/missing checks.	2 years	No	Private/Public Minn. Stat. § 13.43
36	Finance	Voluntary Withholding Requests	2 years	No	Private/Public Minn. Stat. § 13.43
37	Budget/Budget Records	Budget proposals, approved budget, includes supporting data and monthly department budget report	2 years	No	Public Minn. Stat. § 13.03
38	Electronic Calendars	Outlook	Available in current state and back 10 years		Public, unless an exception applies

39	Contracts/Agreements	Contracts/agreements and supporting documentation, including official publications, RFPs, responses, etc.	10 years after expiration	No	Public
40	Correspondence	Routine correspondence and memoranda.	3 years	No	Varies with subject of correspondence
41	Grant Applications – Successful	Application, correspondence, and supporting documents.	3 years	No	Public
42	Grant Applications – Unsuccessful	Applications, correspondence, and supporting documents.	1 year	No	Public
43	Expense Records	Documentation of departmental expenses, purchase orders, invoices, claims forms, etc.	6 years	No	Public
44	Joint Powers Agreements	Contracts with other government units.	Permanent	Yes	Public
45	Meeting Minutes	Minutes recording actions taken in meetings necessary for the management of the department and its activities.	6 years	Yes	Public
46	Procedures	Procedures	Until superseded	No	Public

Legal and Government Relations – TBD, Designee

Item	Title	Description	Retention Period	Archival	Classification
1	Legal Case Files /Attorney Work Product	Case Management System	Permanent	No	Minn. Stat. § 13.393
2	Civil Investigative Data	Case Management System	For duration of applicable statute of limitations	No	Private/Public Minn. Stat. § 13.39

3	Government Relation Case Files	Case Management System	6 years	No	Public/ Private Minn. Stat. §§ 13.03, 13.393
4	Electronic Calendars	Outlook	Available in current state and back 10 years	No	Public, unless an exception applies
5	Professional Services Contracts	Outside Counsel, Lobbyists, etc.	1 year after expiration	No	Public
6	Legislative File	Records on pending legislation of interest.	Until obsolete.	No	Public

Marketing – Travis Bautz, Designee

Item	Title	Description	Retention Period	Archival	Classification
1	Budget/Budget Records	Budget proposals, approved budget, includes supporting data and monthly department budget report	2 years	No	Public Minn. Stat. § 13.03
2	Electronic Calendars	Outlook	Available in current state and back 10 years	No	Public, unless an exception applies
3	Contracts/Agreements	Contracts/agreements and supporting documentation, including official publications, RFPs, responses, etc.	10 years after expiration	No	Public
4	Correspondence	Routine correspondence and memoranda.	3 years	No	Varies with subject of correspondence
5	Grant Applications – Successful	Application, correspondence, and supporting documents.	3 years	No	Public

6	Grant Applications – Unsuccessful	Applications, correspondence, and supporting documents.	1 year	No	Public
7	Expense Records	Documentation of departmental expenses, purchase orders, invoices, claims forms, etc.	6 years	No	Public
8	Joint Powers Agreements	Contracts with other government units.	Permanent	Yes	Public
9	Meeting Minutes	Minutes recording actions taken in meetings necessary for the management of the department and its activities.	6 years	Yes	Public
10	Special Events & Programs	Brochures, marketing materials, agendas, registration forms	2 years	No	Public
11	Marketing	Program guides, ads, promos, brochures, etc.	3 years	No	Public
12	Procedures	Procedures	Until superseded	No	Public

Operations and Procurement; Information and Technology – Jeremy Schwartz, Designee

Item	Title	Description	Retention Period	Archival	Classification
1	Budget/Budget Records	Budget proposals, approved budget, includes supporting data and monthly department budget report	2 years	No	Public Minn. Stat. § 13.03
2	Electronic Calendars	Outlook	Available in current state and back 10 years	No	Public, unless an exception applies

3	Contracts/Agreements	Contracts/agreements and supporting documentation, including official publications, RFPs, responses, etc.	10 years after expiration	No	Public
4	Correspondence	Routine correspondence and memoranda.	3 years	No	Varies with subject of correspondence
5	Grant Applications – Successful	Application, correspondence, and supporting documents.	3 years	No	Public
6	Grant Applications – Unsuccessful	Applications, correspondence, and supporting documents.	1 year	No	Public
7	Expense Records	Documentation of departmental expenses, purchase orders, invoices, claims forms, etc.	6 years	No	Public
8	Joint Powers Agreements	Contracts with other government units.	Permanent	Yes	Public
9	Meeting Minutes	Minutes recording actions taken in meetings necessary for the management of the department and its activities.	6 years	Yes	Public
10	Procedures	Procedures	Until superseded	No	Public

Regional Programs – Paul Drange, Designee

Item	Title	Description	Retention Period	Archival	Classification
1	Community Impact Funds/Community Match Funds	Applications, review standards, awards, and agreements.	6 years	No	Public
2	Intern/Mentorships	Applications, agreements, and invoices.	6 years	No	Private/Public Minn. Stat. §§ 13.32; 13.43

3	Professional Development/Training	Agreements, training materials, and attendee records.	6 years	No	Private/Public Minn. Stat. §§ 13.32; 13.43
4	Shared Services Programs	Contracts, reports, and policies and procedures.	6 years	No	Public
5	AVID	Permissions, activity logs, evaluations.	6 years	No	Public
6	CCR Programs	Contracts, strategic plans, and school data.	6 years	No	Public/Private Minn. Stat. § 13.32
7	In School Support	Strategic plans, activity logs, trend data, metrics, and school visit protocols.	6 years	No	Public
8	Low Incidence	Applications, reporting, event planning information.	6 years	No	Public
9	Metier	Permissions, activity logs, evaluations, Metier logo, and contracts.	6 years	No	Public
10	Minnesota Department of Education	All reports required by MDE.	6 years	No	Public/Private Minn. Stat. § 13.32
11	Networks	Participation lists, CEU/BOSA records, and evaluations.	7 years	No	Public
12	Professional Development	Session recordings, participation logs, contracts, course descriptions, CEU/BOSA hours, evaluations, and # of participants for virtual training.	7 years	No	Public
13	Regional Programs	MASA Board Minutes, MDE data, and special project files.	6 years	No	Public
14	Student Academic Programs	Contracts/agreements, conference invoices, school participation, handbooks, Codes of Conduct, rules, metrics, score sheets, questions, and champion information.	6 years	No	Public/Private Minn. Stat. § 13.32

15	Student Online Courses	Registration information, crop class information, grades, mentor lists, licenses, contracts, exam reviews, and evaluations.	6 years	No	Public/Private Minn. Stat. § 13.32
16	Budget/Budget Records	Budget proposals, approved budget, includes supporting data and monthly department budget report	2 years	No	Public Minn. Stat. § 13.03
17	Electronic Calendars	Outlook	Available in current state and back 10 years	No	Public, unless an exception applies
18	Contracts/Agreements	Contracts/agreements and supporting documentation, including official publications, RFPs, responses, etc.	10 years after expiration	No	Public
19	Correspondence	Routine correspondence and memoranda.	3 years	No	Varies with subject of correspondence
20	Grant Applications – Successful	Application, correspondence, and supporting documents.	3 years	No	Public
21	Grant Applications – Unsuccessful	Applications, correspondence, and supporting documents.	1 year	No	Public
22	Expense Records	Documentation of departmental expenses, purchase orders, invoices, claims forms, etc.	6 years	No	Public
23	Joint Powers Agreements	Contracts with other government units.	Permanent	Yes	Public
24	Meeting Minutes	Minutes recording actions taken in meetings necessary for the management of the department and its activities.	6 years	Yes	Public
25	Procedures	Procedures	Until superseded	No	Public

Records Common to all Departments

Item	Title	Description	Retention Period	Archival	Classification
1	Emails, Audio Video/Instant Messages	Emails and Instant Messages.	6 months unless properly archived.	No	Public
2	Security Video Recordings	Audio/Video recordings of indoor and outdoor managed spaces.	60 days unless properly archived.		Private/Public Minn. Stat. §§ 13.32; 13.43
3	Microsoft Teams Video Recordings	Audio/video records of online, in-person, or hybrid meetings.	45 days unless properly archived	No	Private/Public Minn. Stat. §§ 13.32; 13.43
4	Other Video Recordings	Audio/video records of other events, activities, video productions (e.g. Monthly Executive Message), and non-Team meeting platforms.	May be deleted immediately upon fulfillment of its business purpose with a retention period of potentially 0 days.	No	Private/Public Minn. Stat. §§ 13.32; 13.43

Gift Policy

Purpose

The purpose of this policy is to assist Sourcewell employees in avoiding the appearance of impropriety or conflict of interest with respect to the giving and receiving of gifts.

Definitions

“Gift” means anything that is given or received without the giver receiving consideration of equal or greater value in return. Gifts may be in the form of money, real or personal property, a loan, a forbearance or forgiveness of indebtedness, a promise of future employment, tangible items of value, or intangible items of value, including, but not limited to, awards of cash, cash equivalents, gift cards, gift coupons, or gift certificates, vacations, meals, drinks, lodging, tickets to theater or sporting events, or other similar items.

Policy

- Within the scope of employment, Sourcewell employees are prohibited from soliciting or accepting Gifts from any external individual or entity.
- Sourcewell employees are prohibited from offering or giving Gifts to any individual or entity using Sourcewell funds.
- Sourcewell employees may not solicit, accept, or give a Gift to any employee in a supervisory or leadership position within the workplace.

Procedures:

- Sourcewell employees must refuse to accept any Gift offered by an External Individual or Entity.
- If a Sourcewell employee receives a Gift despite refusing or without having an opportunity to refuse, the employee must:
 - Immediately return the Gift; or
 - Immediately submit the Gift to Sourcewell’s Director of Administration, who will work with Sourcewell Legal to determine the appropriate disposition of the Gift.
- Sourcewell’s Director of Administration has full discretion regarding the disposition of perishable items that cannot be returned.
- In general, plants or flowers and perishable food items will be displayed in a central location where they may be enjoyed by the entire staff.

Exceptions

- Attendance at networking events and accepting items of nominal value (\$5 or less) obtained by an employee while participating as a registered attendee at a conference, training event, seminar, or trade show.
- Food and refreshments shared in the office.
- Recognition of life events unrelated to workplace relationships (examples: marriage, illness, family events).

Violations

Any employees who violates this Policy may be subject to progressive discipline, which may include reprimand, suspension, and/or termination or discharge.

Legal References

Minn. Stat. § 10A.07 (Conflicts of Interest)

Minn. Stat. § 10A.071 (Prohibition of Gifts)

Minn. Stat. § 471.895 (Certain Gifts by Interested Persons Prohibited)

I.R.S. Publication 463 (2020)

I.R.S. Publication 535 (2020)

I.R.S. Publication 15-B (2021)

HIPAA Hybrid Entity Policy

I. Introduction and Policy Statement

The Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), is a federal law intended to strengthen the privacy and security of individuals' health information.

HIPAA applies to Covered Entities, which are limited to health plans, health plan clearinghouses, and health care providers that transmit health information electronically in certain types of transactions. It also applies to Business Associates, which are persons or entities that perform specific functions on behalf of a Covered Entity.

A legal entity that conducts both covered and non-covered functions may designate itself as a hybrid entity for HIPAA compliance purposes.

Sourcewell has designated itself as a hybrid entity. This policy addresses the organizational requirements for hybrid entities and documents Sourcewell's intent to comply with the HIPAA and the HITECH Act applicable to this designation.

II. Designation of Health Care Components

Pursuant to 45 CFR § 164.105(a)(2)(iii)(C), Sourcewell must designate any department as a health care component if:

- The department would meet the definition of "covered entity" or "business associate" if it were a separate legal entity; or
- The department performs covered functions.
 - A. Sourcewell Insurance and Risk Management Solutions
Sourcewell's Insurance and Risk Management Solutions department operates a group health plan for public agencies and provides employee benefit programs to public and nonprofit organizations. As such, the department meets the definition of "covered entity" and has been designated by Sourcewell as a health care component for HIPAA compliance purposes.
 - B. Human Resources
Sourcewell maintains employee health records through its Human Resources department. In its capacity as an employer. However, employee health records are expressly excluded from the definition of protected health information (PHI). Therefore, Sourcewell has not designated this department as a health care component.
 - C. Regional Solutions
Sourcewell's Regional Solutions department provides contracted services to county Human Service Agencies, including, but not limited to, mental health and chemical dependency transition support; adult and child foster care licensing; and daycare licensing. These services require department employees to access and use PHI, but the department does not provide covered services or meet the definition of covered entity or business associate. Therefore, Sourcewell has not designated Regional Solutions as a health care component.

III. Required Safeguards

- A. Health Care Components
It is Sourcewell's policy to ensure that it complies with the HIPAA requirements applicable to hybrid entities. Specifically:

1. Its health care components do not disclose PHI to other departments in a manner that would be prohibited under the HIPAA Privacy Rule¹ if the health care component and other department were separate legal entities;
 2. Its health care components protect electronic PHI from other Sourcewell departments as would be required under the HIPAA Security Rule² if the health care component and other department were separate legal entities; and
 3. If a Sourcewell employee performs duties for a health care component and non-health care component, the employee does not use or disclose PHI created or received in the course of (or incident to) his/her work for the health care component in a way that is prohibited under the HIPAA Privacy Rule.
- B. Related Requirements
Sourcewell also complies with HIPAA provisions regarding compliance and enforcement (45 CFR Part 160, Subpart C) and the implementation of compliance policies and procedures (45 CFR §§ 164.316(a) and 164.530(i)).
- C. Recordkeeping
In compliance with 45 CFR § 164.105(c), Sourcewell retains its health care component designations for at least six (6) years from the date of each was last in effect.

IV. Privacy and Security Officer

Sourcewell has appointed Ryan Donovan, Manager of Insurance and Risk Management, as the Privacy and Security Officer for its health care components. For any questions regarding Sourcewell's compliance with HIPAA and its implementing regulations, please contact the Privacy and Security Officer.

V. Consequences of Failing to Follow Hybrid Entity Policy

All Sourcewell departments must adopt procedures necessary to ensure compliance with HIPAA, its implementing regulations, and this policy.

Any individual who fails to comply with this policy may be subject to sanctions up to and including disciplinary action, suspension, dismissal, or legal action.

¹ 45 CFR Part 164, Subpart E.

² *Id.* at Subpart C.

Rebate Policy for Region 5 Members

The purpose of this policy is to provide an administrative fee rebate to Region 5 Sourcewell Qualifying Members based on administrative fees earned by Sourcewell from purchases made by Qualifying Members from Sourcewell-awarded suppliers. Qualifying Members receiving a rebate are encouraged to use the proceeds to purchase Sourcewell services, or to make purchases from Sourcewell cooperative contracts, but may use the rebate for any lawful purpose.

Definitions

Qualifying Members: Administrative fee rebates are only available to Qualifying Members. A Qualifying Member is a Sourcewell Voting Member or voting-eligible member located within Region 5, as defined in Minnesota Statutes Section 123A.21, subdivision 3, and the Sourcewell Bylaws effective April 11, 2019.

Policy

Sourcewell will track the purchases made by each Qualifying Member. Shortly after the close of the Sourcewell fiscal year, if sufficient funds are available and as determined by the Sourcewell Board of Directors, Sourcewell will rebate to each Qualifying Member a percentage of the administrative fees earned by Sourcewell based on the eligible purchases made by that specific Qualifying Member. Eligible purchases are defined as any purchase made through Sourcewell cooperative contracts. Rebates will be dispersed to Qualifying Members in the form of a check after the conclusion of each Sourcewell fiscal year.

The rebate program may be discontinued or modified at any time and for any reason by the Sourcewell Board of Directors. The Sourcewell Board of Directors has no obligation to provide advanced notice of modification or cancellation to Qualifying Members participating in this program.

Calculation of Rebate Amount

The rebate for each Qualifying Member will be calculated at 1% of each Qualifying Member's purchases made through Sourcewell cooperative contracts in the preceding fiscal year.

Administration and Procedure

The Board of Directors authorizes its Chief Executive Officer to prepare and administer appropriate procedures designed to meet the purpose of this Board Policy.



PROCUREMENT POLICY

Approved by the Sourcewell Board of Directors
Effective July 1, 2022

I. PURPOSE

To ensure that Sourcewell's internal procurements and contracts are created pursuant to, a process that enhances access, competition, and fairness; and results in optimal balance of overall benefits to Sourcewell.

Sourcewell's acquisition and contract process is designed to stand the test of public scrutiny in matters of good judgment and integrity, open competition, and fairness in the spending of public funds.

II. SCOPE

This policy applies to all acquisitions made, and contracts entered by Sourcewell for its own use. As defined in this Policy a contract is an agreement for the sale or purchase of supplies, materials, equipment, or the rental thereof, or the construction, alteration, repair, or maintenance of real or personal property. Questions about the scope and application of this policy will be determined by the General Counsel.

III. PROCUREMENT OBJECTIVES

A. Compliance

Sourcewell procurements must comply with all applicable laws of the State of Minnesota and United States federal laws.

B. Fair and Open Competition

When competition is required by law and this policy solicitations should be written so that they are able to be met by more than one supplier, notice of the opportunity is posted so that it receives broad publication, and all responsible suppliers are permitted to compete in the solicitation process.

C. Conflicts of Interest

1. Individual Conflicts of Interest.

No employee of or individual associated with Sourcewell may participate in the development, selection, award, or administration of a contract or master agreement if they have a real or potential conflict of interest. Conflicts of interest arise when the employee, any member of their immediate family, or an organization which employs or is about to employ, or an

organization with which any of the parties indicated herein are affiliated, has a financial or other interest in or receives a tangible personal benefit from a potential supplier. Employees of Sourcewell may not solicit or accept gifts, gratuities, or favors creating a tangible personal benefit from any current or potential supplier.

2. Organizational Conflicts of Interest.

Sourcewell will take affirmative action to identify, avoid, or mitigate organizational conflicts of interest in all procurement transactions. An organizational conflict of interest is created when a current or prospective supplier is unable to render impartial service to Sourcewell due to the supplier's:

- a. Creation of evaluation criteria during performance of a prior contract which potentially influences future competitive opportunities to its favor;
- b. Access to nonpublic and material information that may provide for a competitive advantage in a later procurement competition;
- c. Impaired objectivity in providing advice to Sourcewell.

3. Procedures for Mitigating Conflicts of Interest

Employees must disclose any actual or potential conflict of interest immediately upon discovery to the Chief Procurement Officer or the General Counsel. Failure to provide notice may subject an employee to discipline. Employees participating in the response evaluation process must sign the Evaluation Committee Member Agreement.

Upon notification or discovery of any an actual or potential conflict of interest, the General Counsel will review the circumstances and determine whether a legal conflict of interest exists. A legal conflict of interest includes any violation of applicable statues, rules, regulations, and the requirements of this Program. Upon a determination a legal conflict exists, the General Counsel will advise the Executive Director, Chief Procurement Officer, or Board of Directors as may be appropriate on remedial and mitigation actions.

If no legal conflict of interest is determined to exist, but the appearance of a potential conflict of interest exists, the CPO, in consultation with appropriate Senior Leaders, must then review the circumstances and exercise common sense, good judgment, and sound discretion in determining an appropriate means for resolving. Employees may be subject to discipline for conduct creating a conflict of interest or the reasonable perception of a conflict of interest or failure to follow these requirements.

4. Silent Period

To avoid the appearance of any actual or potential conflict of interest, all discussions with currently awarded or prospective suppliers specifically relating to any upcoming solicitation which the supplier is likely to respond will stop 14 days prior to the issuance of any solicitation (Silent Period). During this Silent Period, all questions relating to the solicitation must be directed to Sourcewell's Procurement Department until the solicitation is officially completed resulting in issuance of award(s) or upon cancellation of the competitive process by the CPO.

This section does not prohibit discussions with industry partners and suppliers which are not relating specifically to any open solicitation, including ongoing administration of an existing and current contract. During this Silent Period and any open solicitation period, Sourcewell employees will make affirmative efforts to limit or avoid contact with prospective suppliers which may create the appearance of any actual or potential conflict of interest. All travel activity relating or potentially relating to a prospective supplier during this time must be approved by the employee's Director.

IV. PROCUREMENT AUTHORITY

A. Statutory Authority

1. Sourcewell is governed by Minnesota Statutes § 123A.21 and the Sourcewell Bylaws.
2. The sale or purchase of supplies, materials, equipment, or the rental thereof, or the construction, alteration, repair, or maintenance of real or personal property are governed by Minnesota Statutes § 471.345.
3. Article XI, Section 4 designates the Sourcewell Board of Directors as the contracting authority for Sourcewell. The Board may delegate this function in accordance with Minnesota law.
4. Sourcewell's Procurement Policy and any amendments must be approved by Board of Directors.

V. GENERAL REQUIREMENTS

A. Solicitation Form and Management, and Templates

When competition is required or utilized, solicitations will be issued as a Request for Proposals (RFP), Invitation for Bids (IFB), Request for Information (RFI), Request for Quote (RFQ), or other method as approved by the Chief Procurement Officer. The CPO may exercise lawful discretion in determining the selection method, scope, evaluation criteria, award standards, and any other elements which are compliant with applicable legal standards and intended to achieve the desired solicitation-specific results to serve the needs of Sourcewell.

To ensure compliance, this Policy, all solicitation forms, templates, and all other legal documents related to this Policy will be subject to review, at least annually, by the CPO (or designee) in consultation with the General Counsel (or designee) and the Director of Enterprise Services (or designee).

B. Public Notice

Public notice of contracting opportunities will be posted for a minimum of 30 days on the Sourcewell website and other locations as may be required by law.

C. Receipt of Responses

Sourcewell will not evaluate any proposal, bid, or any other form of response to a solicitation that was not received by the due date and time specified in the solicitation document.

D. Evaluation

All proposals that are received timely will be evaluated for compliance with the evaluation criteria that have been defined in the solicitation.

E. Awards

1. Contract awards may only be made to responsible suppliers as defined by Minnesota law and any applicable federal requirements.
2. Sourcwell will not award a contract to a supplier that has been debarred, suspended, or otherwise excluded from or ineligible for participation by the State of Minnesota.

VI. PROCUREMENT CONTRACTS

Procurement of contracts to be used by Sourcwell must follow the requirements of Minnesota's Uniform Municipal Contracting Law, Minnesota Statutes § 471.345.

Before making any purchase or creating a new contract, Sourcwell should look first to the State of Minnesota Cooperative Purchasing Venture and its own Cooperative Purchasing Program contracts to fulfill its needs.

After a determination that the solutions available through Sourcwell's Cooperative Purchasing Program do not meet its needs, Sourcwell may enter contract(s) to meet its needs for products and services following the process outlined below.

A. Procurement of Supplies, Materials, Equipment, or the Rental thereof, or the Construction, Alteration, Repair or Maintenance of Real or Personal Property

1. Acquisitions of \$25,000 or less.

If the amount of the resulting contract, including all foreseeable amendments, is estimated to be \$25,000 or less, in Sourcwell's discretion, the contract may be made either upon quotation or direct negotiation in the open market. If the contract is based upon quotation, it should be based on at least two quotations. The quotations must be kept on file for a period of at least one year after their receipt.

2. Acquisitions exceeding \$25,000 but not \$175,000.

If the amount of the resulting contract, including all foreseeable amendments, is estimated to exceed \$25,000 but not to exceed \$175,000, the contract may be made through:

a. Quotation or direct negotiation in the open market. If the contract is based upon quotation, it should be based on at least two quotations. The quotations must be kept on file for a period of at least one year after their receipt.

b. Informal Competition. Sourcwell may utilize any solicitation method as authorized by the CPO and consistent with this policy. All solicitation documents must be kept on file for a period of at least one year after receipt thereof.

c. Formal Competition. Upon consultation with the CPO and election by the purchasing division, a full competitive process may be utilized consisting of publicly posted notice of the solicitation, use of a formal solicitation document, and a complete and thorough evaluation process.

3. Acquisitions exceeding \$175,000.

For all resulting contracts with an estimated value, including all foreseeable amendment, exceeding \$175,000, Sourcwell will follow the full competitive process consisting of publicly posted notice of the solicitation, use of a formal solicitation document, and a complete and thorough evaluation process.

4. Construction Best Value Alternative.

Sourcwell may award a contract for construction, alteration, repair, or maintenance work to the supplier or contractor offering the best value under a request for proposals as described in Minnesota Statutes Section 16C.28, subdivision 1, paragraph (a), clause (2), and paragraph (c). Solicitation documents must state the relative weight of price and other selection criteria. The award must be made to the supplier(s) or contractor(s) offering the best value applying the weighted selection criteria.

B. Professional and Technical Services Contracts

Professional and technical services are intellectual in character, including consultation, analysis, evaluation, predication, planning, programming, recommendations, and often result in production of a report or completion of a task. Sourcwell may establish contracts for professional and technical services without formal competition. The CPO may be consulted on professional and technical service contracts where use of an informal or formal competitive solicitation processes is desired or where the process may be advantageous to Sourcwell.

C. Software and Technology Contracts

Sourcwell's Information Technology (IT) division will be consulted prior to any potential purchase of software and technology to evaluate need, compatibility, and ongoing support obligations to Sourcwell.

D. Contracts using United States Federal Funding

In the event Sourcwell uses federal funding for either direct or pass-through federal dollars, it will comply with the applicable procurement requirements set forth in 2 C.F.R. 200.317 – 200.326, along with Sourcwell's procurement policies. In the event of a conflict between the federal requirements and Sourcwell's requirements, the most restrictive requirement will prevail.

VII.EXCEPTIONS

A. Cooperative Purchasing (Minnesota Statutes Section 471.345, subdivision 15)

Sourcwell may contract for the purchase of supplies, materials, or equipment by utilizing

contracts that are available through the State of Minnesota's Cooperative Purchasing Venture (CPV) or another cooperative purchasing program. In the event Sourcwell uses another entity's cooperative purchasing contracts, documentation of that entity's solicitation process must be contained within the procurement file.

B. Single Source

A single source acquisition occurs when, after a search, only one supplier is determined to be reasonably available for the required product, service, or construction item. Single source contracts should only be awarded when Sourcwell has performed sufficient research to ensure the supplier meets the single source criteria. The request for single source procurement, along with sufficient justification, will be presented to the Chief Procurement Officer who will make the final determination of whether a contract meets single source requirements.

C. Emergencies

A valid emergency is one where the required product or service is immediately needed for continued operation of Sourcwell. The request for emergency procurement, along with sufficient justification, will be presented to the Chief Procurement Officer who will make the final determination of whether a contract meets the requirements for being classified as an emergency.

VIII. DATA PRACTICES AND RECORDS RETENTION

All data created and maintained by Sourcwell is subject to the Minnesota Data Practices Act (Minnesota Statutes Chapter 13) and Sourcwell's Records Retention Policy.

IX. APPROVAL

The Sourcwell Board of Director has approved this Policy effective July 1, 2022.

DocuSigned by:

By _____
Authorized Signature – Signed
By Greg Zylka
Name – Printed
Title Sourcwell Board of Directors Chair
Date Effective July 1 , 2022

DocuSigned by:

By _____
Authorized Signature – Signed
By Sara Nagel
Name – Printed
Title Sourcwell Board of Directors Clerk
Date Effective July 1, 2022



PROCUREMENT CODE OF ETHICS

Approved by the Sourcewell Board of Directors

Effective November 21, 2023

Procurement is a public trust, and as such, procurement staff must abide by the highest ideals of honor and integrity in all dealings in order to merit respect and inspire the confidence of the organization and the participating entities we serve.

All Sourcewell employees involved with the procurement process are responsible for impartially assuring fair and open competitive access to procurement opportunities to all responsible suppliers and contractors. Employees must conduct themselves by:

- Diligently following all Minnesota laws and regulations and any applicable United States federal requirements;
- Following Sourcewell’s Procurement Policy and Sourcewell Cooperative Purchasing Program requirements;
- Striving to practice the highest degree of business ethics, professional courtesy, and competence in all transactions; and
- Avoiding any actual or perceived unethical behavior and practices or any activity that may influence or appear to influence procurement decisions (such as soliciting gifts, favors, money, etc.).

The Sourcewell Board of Directors authorizes and directs Sourcewell’s Chief Procurement Officer to issue and be the responsible authority for this Procurement Code of Ethics.

The Sourcewell Board of Directors has approved this Procurement Code of Ethics, effective November 21, 2023.

DocuSigned by:
 X Greg Zylka
 6BD483769B484F1...
 Greg Zylka
 Chair, Sourcewell Board of Directors

Date: 11/22/2023 | 12:36 PM CST

ATTEST:

DocuSigned by:
 X Linda Arts
 0EF5785E1EAD4CF...
 Linda Arts
 Clerk to the Board of Directors

Date: 11/22/2023 | 4:01 PM CST

Sourcewell Cooperative Purchasing Program

Approved by the Sourcewell Board of Directors

Updated July 1, 2022

Authority:

Minn. Stat. § 123A.21

Minn. Stat. § 471.59

Sourcewell Bylaws

Related Policies:

Rebate Policy for Region 5 Members

Records Retention

Data Practices

Program Description:

The Sourcewell Board of Directors authorizes a Cooperative Purchasing Program acting pursuant to the Sourcewell Bylaws, and consistent with specific authority of Minn. Stat. § 123A.21, Subd. 7(23).

The Program establishes Sourcewell's authority to offer cooperative purchasing master agreements for use by eligible participating entities. This Program includes all current Sourcewell cooperative purchasing contracts, and the term "master agreement" includes these contracts. Each Participating Entity, as defined herein, may access master agreements in accordance with the laws and requirements of its respective jurisdiction.

Sourcewell Board of Directors retains the right to amend any element of this Program or to create supplemental programs related to cooperative purchasing as duly permitted within its authority.

Program Purpose:

Sourcewell's Cooperative Purchasing Program is designed to provide participating entities with access to competitively awarded cooperative purchasing solutions. To facilitate the Program, Sourcewell awards cooperative purchasing master agreements following a competitive procurement process intended to meet compliance standards in accordance with Minnesota law and the requirements contained herein. Benefits of the Program include:

- Competitively solicited and awarded agreements
- Administrative time and money efficiencies
- Cost savings based on volume purchasing

Program Eligibility:

Sourcewell's Cooperative Purchasing Program is available to participating entities. A Participating Entity is any government unit, including a state, city, county, town, school district, political subdivision of any state, federally recognized Indian tribe, any agency of the United States, any instrumentality of a governmental unit, any other entity as defined in Minn. Stat. § 471.59, subd. 1(b), and any entity as defined in Art. VI of the Sourcewell Bylaws.

Awarded suppliers may expressly agree to extend master agreement terms to additional categories of entities, including nonprofits or public agencies in foreign jurisdictions. Extension of Sourcewell master agreement eligibility will be determined by each respective supplier within its respective solicitation response prior to award, or upon execution of an amendment after award. Additionally, Sourcewell may also enter partnership agreements to further expand availability of master agreements.

Program Registration:

Each Participating Entity will complete a Participation Agreement detailing the terms and conditions of Program participation and master agreement use. Entities will register with Sourcewell to create an account and to receive a Client Number. Registration will include acceptance of the terms of use as evidenced in a form approved by the Sourcewell Board of Directors. Alternatively, an entity may request to enter a joint powers, interlocal, or similar agreement with Sourcewell to establish access to the Program.

Sourcewell will maintain and continue to recognize any eligible entity that has joined, utilized, or accessed Sourcewell programs prior to July 1, 2022. Each such entity will retain its status and access to Sourcewell programs. After July 1, 2022, entities will be encouraged to re-register with Sourcewell.

Program Duties:

A. Chief Procurement Officer (CPO) Authorization

Pursuant to the Sourcewell Bylaws, the Board of Directors designates a Chief Procurement Officer to administer components of Sourcewell's Cooperative Purchasing Program. The Chief Procurement Officer is authorized to award all competitively solicited cooperative purchasing master agreements. The Board delegates to the Chief Procurement Officer the authority to execute all cooperative purchasing master agreements, and amendments thereto, on behalf of Sourcewell. The Board will subsequently ratify cooperative purchasing master agreement awards.

B. Director of Enterprise Solutions (DES)

After award, the Director of Enterprise Solutions develops Sourcewell's cooperative purchasing program. This includes direction of Sourcewell's Category Development, Supplier Development, and Client Relations divisions and coordination with Sourcewell's central services functions.

Functions include participating agency and supplier awareness training activities, promotional and educational activities relating to the Program, market analysis, category development, day to day support of master agreements, customer service, and related functions focused on training, educating, and facilitation of Program use between Sourcewell, awarded suppliers, and Participating Entities.

Program Requirements:

I. PURPOSE

Sourcewell's Cooperative Purchasing Program is conducted in a manner that ensures cooperative purchasing master agreements are awarded pursuant to a competitive public procurement process consistent with the legal principles of open access, competition, fairness, and transparency.

II. SCOPE

These requirements apply to Sourcewell's Cooperative Purchasing Program master agreements awarded by Sourcewell on behalf of, and intended for use by, eligible Participating Entities.

III. PROCUREMENT OBJECTIVES

A. Compliance

Sourcewell cooperative purchasing procurements must comply with all applicable State of Minnesota and United States federal laws.

B. Fair and Open Competition

As a Minnesota local government unit and service cooperative, Sourcewell requires fair and open competition in its master agreement process. Solicitations will be written so that they are able to be met by more than one supplier, notice of the opportunity is posted so that it receives broad publication, and all responsible suppliers are permitted to compete in the solicitation process. Sourcewell will provide equal opportunity to access information to promote competition.

C. Awards

Awards will be made to the proposers whose proposal conforms to all conditions and requirements of a solicitation, and consistent with the award criteria defined in the solicitation. Proposal evaluation will be based on scoring criteria defined in the solicitation and the Sourcewell Evaluator Scoring Guide.

Social and economic preferences will be implemented to the extent practicable and when required by Minnesota law. Participating entities accessing master agreements are subject to their own specific legal requirements.

D. Conflicts of Interest

1. Individual Conflicts of Interest.

No employee of or individual associated with Sourcewell may participate in the development, selection, award, or administration of a contract or master agreement if they have a real or potential conflict of interest. Conflicts of interest arise when the employee, any member of their immediate family, or an organization which employs or is about to employ, or an organization with which any of the parties indicated herein are affiliated, has a financial or other interest in or receives a tangible personal benefit from a potential supplier. Employees of Sourcewell may not solicit or accept gifts, gratuities, or favors creating a tangible personal benefit from any current or potential supplier.

2. Organizational Conflicts of Interest.

Sourcewell will take affirmative action to identify, avoid, or mitigate organizational conflicts of interest in all procurement transactions. An organizational conflict of interest is created when a current or prospective supplier is unable to render impartial service to Sourcewell due to the supplier's:

- a. Creation of evaluation criteria during performance of a prior contract which potentially influences future competitive opportunities to its favor;
- b. Access to nonpublic and material information that may provide for a competitive advantage in a later procurement competition;
- c. Impaired objectivity in providing advice to Sourcewell.

3. Procedures for Mitigating Conflicts of Interest

Employees must disclose any actual or potential conflict of interest immediately upon discovery to the Chief Procurement Officer or the General Counsel. Failure to provide notice may subject an employee to discipline. Employees participating in the response evaluation process must sign the Evaluation Committee Member Agreement.

Upon notification or discovery of any an actual or potential conflict of interest, the General Counsel will review the circumstances and determine whether a legal conflict of interest exists. A legal conflict of interest includes any violation of applicable statues, rules, regulations, and the requirements of this Program. Upon a determination a legal conflict exists, the General Counsel will advise the Executive Director, Chief Procurement Officer, or Board of Directors as may be appropriate on remedial and mitigation actions.

If no legal conflict of interest is determined to exist, but the appearance of a potential conflict of interest exists, the CPO, in consultation with appropriate Senior Leaders, must then review the circumstances and exercise common sense, good judgment, and sound discretion in determining an appropriate means for resolving. Employees may be subject to discipline for conduct creating a conflict of interest or the reasonable perception of a conflict of interest or failure to follow these requirements.

4. Silent Period

To avoid the appearance of any actual or potential conflict of interest, all discussions with currently awarded or prospective suppliers specifically relating to any upcoming solicitation which the supplier is likely to respond will stop 14 days prior to the issuance of any solicitation (Silent Period). During this Silent Period, all questions relating to the solicitation must be directed to Sourcewell's Procurement Department until the solicitation is officially completed resulting in issuance of award(s) or upon cancellation of competitive process by the CPO.

This section does not prohibit discussions with industry partners and suppliers which are not relating specifically to any open solicitation, including ongoing administration of an existing and current contract. During this Silent Period and any open solicitation period, Sourcewell employees will make affirmative efforts to limit or avoid contact with prospective suppliers which may create the appearance of any actual or potential conflict of interest. All travel activity relating or potentially relating to a prospective supplier during this time must be approved by the employee's Director.

IV. AUTHORITY

A. Statutory Authority

1. Sourcewell is expressly authorized to provide a cooperative purchasing program pursuant Minnesota Statutes § 123A.21, Subdivision 7 (23) and the Sourcewell Bylaws.

2. Sourcewell is governed by Minnesota Statutes § 471.345 when awarding contracts.

B. Chief Procurement Officer Authority

As delegated by the Sourcewell Bylaws (Article XV, Section 2) the Chief Procurement Officer is authorized to award all competitively solicited cooperative purchasing master agreements, without limitation. The Sourcewell Board will subsequently ratify of all cooperative purchasing awards made by the CPO.

V. GENERAL REQUIREMENTS

A. Solicitations

Solicitations will be issued as a Request for Proposals (RFP), Invitation for Bids (IFB), or other method approved by the Chief Procurement Officer. The CPO may exercise lawful discretion in determining the selection method, scope, evaluation criteria, award standards, and any other elements which are compliant with applicable legal standards and intended to achieve the desired solicitation-specific results to serve the needs of Sourcewell and its participating entities.

To ensure compliance, all solicitation forms, templates, master agreements, Participation Agreements, and all other legal documents related to the cooperative purchasing program

will be subject to review, at least annually, by the CPO (or designee) in consultation with the General Counsel (or designee) and the Director of Enterprise Services (or designee).

B. Public Notice

Public notice of all cooperative purchasing master agreement solicitations will be posted for a minimum of 30 days on the Sourcewell website. Additional notification of solicitations may occur through alternative media locations as determined to be reasonable or necessary by the Chief Procurement Officer.

C. Receipt of Responses

Sourcewell will not evaluate any proposal, bid, or any other form of response to a solicitation, that was not received by the due date and time specified in the solicitation document.

D. Evaluation

All proposals that are received timely will be evaluated for responsiveness and compliance with the evaluation criteria that have been clearly defined in the solicitation.

VI. COOPERATIVE PURCHASING PROCUREMENT REQUIREMENTS**A. Board Approval**

The Board must approve all categories of products and services prior to posting public notice of a solicitation.

B. Awards**1. Responsible Suppliers**

Master agreement awards may only be made to responsible suppliers as defined by Minnesota law, federal requirements, and the specific solicitation.

2. Multiple Awards

Sourcewell intends to award one or more master agreements to responsive and responsible suppliers to meet the needs of Sourcewell participating entities. Factors to be considered in determining the number of awards in any category may include the following:

- a. The number and geographic location of suppliers necessary to offer a comprehensive selection of products for use by participating entities.
- b. The number and geographic locations of suppliers, and their sales and service network, to assure availability of product supply and coverage to meet participating entities' anticipated needs.
- c. The attributes of suppliers' products and services that are necessary to assist Sourcewell participating entities with achieving environmental, sustainability, supplier diversity, and technological goals and objectives.

3. Debarment Status Updates

All cooperative purchasing master agreements must contain a provision requiring the supplier to notify Sourcewell if its status changes regarding debarment and suspension in any jurisdiction.

4. Term

The Board of Directors will establish the maximum term of any cooperative purchasing master agreement upon request of the CPO when approving the opening of a solicitation. The CPO may exercise lawful discretion in defining any combination of term and extensions not exceeding the maximum term established by the Board. The Board may approve, upon written request of the CPO, an extension of any existing master agreement beyond the established maximum term only in exceptional situations and to be determined on a case-by-case basis.

5. Ratification

Upon completion of the procurement process and award, and as soon as practicable, the Chief Procurement Officer will present a resolution to the Board for ratification of awards.

C. Administrative Fees

Suppliers awarded a master agreement must pay Sourcewell an administrative fee in consideration for the support and services provided by Sourcewell. The fee will be determined and negotiated within the master agreement award process, upon advice of the Director of Enterprise Solutions, by the CPO. Fees will be determined based upon total sales to Participating Entities for all contracted equipment, products, or services made during the term of, and pursuant to the requirements of, the master agreement. Suppliers may not charge Participating Entities more than the contracted price to offset the Administrative Fee. In the event the Supplier is delinquent in any administrative fees, Sourcewell reserves the right to cancel a master agreement and reject any proposal submitted by the supplier in any subsequent solicitation.

VII. PROCUREMENTS THAT MAY CONTAIN FEDERAL FUNDING

As required under certain United States federal rules regarding procurements (2 C.F.R.200.317 – 200.326 and Appendix II to Part 200) all Sourcewell cooperative purchasing master agreements will contain language to assist participating entities in meeting federal requirements and procurement standards.

VIII. DATA PRACTICES AND RECORDS RETENTION

All data created and maintained during the procurement process is subject to the Minnesota Data Practices Act (Minnesota Statutes Chapter 13) and Sourcewell's Records Retention Policy.


IX. APPROVAL

The Sourcewell Board of Director has approved the Program effective July 1, 2022.

DocuSigned by:
By 
Authorized Signature – Signed
6BD483766B484F1

By Greg Zylka
Name – Printed

Title Sourcewell Board of Directors Chair
Date 8/19/2022 | 9:59 AM CDT

DocuSigned by:
By 
Authorized Signature – Signed
9BEF5D6F88D140B...

By Sara Nagel
Name – Printed

Title Sourcewell Board of Directors Clerk
Date 8/19/2022 | 10:35 AM CDT



Personnel Policies

Background Checks

Rationale:

The purpose of this policy is to maintain a safe and healthy environment in order to promote the well-being of Sourcewell's employees and stakeholders. Sourcewell will seek a criminal history background check for independent contractors, interns, select volunteers, and finalist candidates who receive an offer of employment with Sourcewell, or such other background checks as indicated by this policy.

General Statement of Policy:

1. Sourcewell shall require that finalist candidates for positions who receive an offer of employment submit to a criminal history background check. The offer of employment shall be conditioned upon a determination by Sourcewell that a candidate's criminal history does not preclude the applicant from employment with Sourcewell.
2. Sourcewell specifically reserves any and all rights it may have to conduct background checks regarding current employees or candidates. Sourcewell will seek consent of individuals where required by law.
3. Sourcewell maintains the right to require additional information, or to use procedures currently in place or other procedures to gain additional background information concerning employees, applicants and volunteers.

Procedures:

1. An individual will not commence employment until Sourcewell receives the results of the criminal history background check. Sourcewell may conditionally hire an individual, pending successfully passing the background check prior to start of employment.
2. An individual who is offered employment must sign a criminal history consent form which provides permission for Sourcewell to conduct a criminal history background check. If the individual fails to provide Sourcewell with a signed Informed Consent Form at the time the individual receives a job offer, the individual will be considered to have voluntarily withdrawn their application for employment.
3. When required, candidates must provide fingerprints to assist in a criminal history background check. If the fingerprints provided by the candidate are unusable, the candidate will be required to submit another set of prints. In accordance with the Federal Privacy Act, when fingerprints are required, candidates will be provided a copy of the FBI Privacy Act Statement.
4. Copies of this policy shall be available in the human resource office and will be distributed to applicants for employment upon request. The need to submit to a criminal history background check may be included with the basic criteria for employment in the job posting and job advertisements.
5. The applicant will be informed of the results of the criminal background check(s) and the right to challenge the accuracy or completeness of the information contained in the background report or record to the extent required by law.

Legal References:

Minn. Stat. §364.021 (Public and private employment; consideration of criminal records)

Minn. Stat. §13.04, Subd. 4 (inaccurate or incomplete data)

Minn. Stat. §123B.03 (Background checks)

Minn. Stat. §299C.60-299C.64 (Minnesota Child, Elder, and Individuals with Disabilities Protection Background Check Act)

Drug Prevention

Sourcewell's Board of Directors recognizes:

1. The employment related rights and concerns of employees and independent contractors who may have drug or alcohol problems as well as the rights of clients and the public at large to continue to receive quality services regardless of the employees and independent contractors health condition.
2. Its obligation, as an employer, is to provide a safe work environment for all employees, independent contractors, clients, and the public at large.
3. Employees and independent contractors shall avoid the use or abuse of illicit drugs and alcoholic beverages while in any Sourcewell building or other Sourcewell premises, any Sourcewell owned vehicle or any other Sourcewell-approved vehicle, or any Sourcewell member building. Employees and independent contractors shall exercise good judgment and restraint at Sourcewell sponsored events/programs where drinking to an excess or engaging in behavior would cause people to look down upon Sourcewell.
4. Employees and independent contractors shall display exemplary behavior regarding appropriate use of medications while in the Sourcewell building, Sourcewell member building or any Sourcewell or member sponsored program.
5. Each employee and consultant is encouraged to identify indicators of use of alcohol or drugs by Sourcewell employees, independent contractors and to report such situations to the Manager of Human Resources, so the concerns can be addressed.
6. Priority will be placed on negotiation of contract language which provides appropriate leaves of absence and health benefits for Sourcewell employees and independent contractors who need alcoholism or drug abuse treatment or related services.

Equal Employment Opportunity Statement

This is to affirm the Sourcewell policy of providing Equal Opportunity to all employees and applicants for employment in accordance with all applicable Equal Employment Opportunity laws, directives, and regulations of Federal, State, and Local governing bodies or agencies thereof, specifically Minnesota Statutes 363.

Sourcewell is committed to equal employment opportunity in all of its employment practices. Management and supervisors recruit, employ, train, promote, discipline, and terminate employees solely on the basis of individual qualifications and merit and as is feasible under the standards and policies outlined in this guide and related policies. Decisions involving every aspect of the employment relationship are made without regard to an employee's race, color, creed, religion, sex, age, national origin, marital status, veteran status, sexual orientation, gender identity and expression, familial status, or any other status or characteristic protected under applicable state or federal law, unless it is a bona fide occupational requirement necessary to the normal operation of the business. Discrimination or harassment based on any of these factors is inconsistent with our philosophy and will not be tolerated at any time.

Sourcewell will take action to ensure that all employment practices are free of such discrimination. Such employment practices include, but are not limited to, the following: hiring, promotion, demotion, transfer, recruitment or recruitment advertising, selection, layoff, disciplinary action, termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship.

Sourcewell will use its best efforts to afford minority and female business enterprises with the maximum practicable opportunity to participate in the performance of subcontracts for projects in which Sourcewell engages.

Sourcewell will commit the necessary time and resources, both financial and human, to achieve the goals of Equal Employment Opportunity and inclusive workplace.

Sourcewell fully supports incorporation of non-discrimination statements and regulations in contracts.

The Director of Administration will be responsible for the dissemination of this policy. Directors, managers, and supervisors are responsible for implementing equal employment practices within each department. The HR department is responsible for overall compliance and will maintain personnel records in compliance with applicable laws and regulations.

Sourcewell has appointed its Director of Administration to manage the Equal Employment Opportunity Program. The Director of Administration's responsibilities will include monitoring all Equal Employment Opportunity activities and reporting the effectiveness of these programs, as may be required by Federal, State and Local agencies. The Executive Director/CEO of Sourcewell will receive and review reports on the program. If any employee or applicant for employment believes he/she has been discriminated against, please contact Sourcewell, Director of Administration, 202 12th Street NE, PO Box 219, Staples, MN 56479, 218-894-5464.

Nondiscrimination/Anti-Harassment, and Violence Prevention

Policy:

Everyone at Sourcewell has a right to feel respected and safe. It is the policy of Sourcewell to maintain a working environment that is free from discrimination, harassment, and violence of any kind. Sourcewell Has adopted this policy to protect employees against discrimination, harassment, intimidation, or threats of or actual violence that may occur in the workplace or off site during work-related activities.

It is the policy of the Sourcewell Board of Directors to comply with Federal and State law prohibiting discrimination and all requirements imposed by or pursuant to regulations issued thereto, to the end that no person shall on the grounds of race, color, creed, religion, sex, age, national origin, marital status, veteran status, sexual orientation, gender identity or expression, familial status, status with regard to public assistance, or disability be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under any educational program or in employment of recruitment, consideration, or selection, therefore, whether full-time or part-time under any program or activity operated by Sourcewell for which it received federal financial assistance.

Nondiscrimination:

To carry out the provisions of the nondiscrimination policy, the Board directs the Sourcewell Executive Director/CEO to take the following actions immediately:

1. Develop and implement a management system to comply with the provisions of the Title VI and VII of the Civil Rights Act of 1964, Title IX of the Education Amendments of 1972, Chapter 363.03, Minnesota Human Rights Act, and Section 504 of the Rehabilitation Act of 1993.
2. Evaluate on a continuous basis Sourcewell operations in terms of the requirements of Federal and State law prohibiting discrimination. This evaluation will include policies, practices, and procedures currently in effect.
3. Modify those aspects of Sourcewell operation which do not conform to Federal and State law prohibiting discrimination.
4. Take remedial steps to eliminate the present effects of past discrimination.
5. Maintain data for three years following completion of the evaluation as recommended under paragraph 2 of this section and upon request, provide to Department of Health, Education and Welfare a description of any modification made pursuant to paragraph 3 above.
6. Assign responsibility for the implementation of provision of civil right responsibilities.
7. Design and implement a training program to acquaint Sourcewell staff with civil right responsibilities.
8. Establish and publish a grievance procedure for staff as required under provisions to Title IX.
9. Prohibit discrimination against persons with disabilities, such person to be defined as anyone who:
 - a. Has a mental or physical impairment which substantially limits one or more major life activities (major life activities include activities such as caring for oneself, performing manual tasks, walking, seeing, hearing, speaking, breathing, learning, and working);
 - b. Has a record of such impairment; or
 - c. Is regarded as having such an impairment. (34 CFR 104.3(j))
10. Disseminate, upon request, Sourcewell non-discriminatory policy to member government agencies, non-public schools, education agencies, clients, the general public, and vendors.

Sexual Harassment

Sexual harassment is a form of sex discrimination, which violates Section 703 of the Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. 2000e, et seq., and Minn. Stat. 363.01-.14, the Minnesota Human Rights Act. Sexual violence is a physical act of aggression that includes a sexual act or sexual purpose.

Sexual Harassment/Sex Violence Defined:

- A) Sexual harassment consists of unwelcome sexual advances, requests for sexual favors, sexually motivated physical conduct, or other verbal or physical conduct or communication of a sexual nature when:
1. Submission to that conduct or communication is made a term or condition, either explicitly, of obtaining or retaining employment;
 2. Submission to or rejection of that conduct or communication by an individual is used as a favor in decisions affecting that individual's employment; or
 3. That conduct or communication has the purpose or effect of substantially or unreasonably interfering with an individual's employment, or creating an intimidating, hostile, or offensive employment environment.
- B) Sexual harassment may include but is not limited to:
1. Oral or written harassment or abuse;
 2. Pressure for sexual activity;
 3. Inappropriate patting or pinching;
 4. Intentional brushing against an employee's body;
 5. Demanding sexual favors accompanied by implied or overt threats concerning an individual's employment status;
 6. Demanding sexual favors accompanied by implied or overt promises of preferential treatment with regard to an individual's employment status;
 7. Any sexually motivated unwelcome touching; or
 8. Sexual violence, which is a physical act of aggression that includes a sexual act or sexual purpose.

Discriminatory Harassment

Harassment may include, but is not limited to, the following when related to religion, race, sex, sexual orientation, or gender:

1. Name calling, jokes or rumors;
2. Pulling on clothing;
3. Graffiti;
4. Notes or cartoons;
5. Unwelcome touching of a person or clothing;
6. Offensive or graphic posters or book covers; or
7. Any words or actions that make you feel uncomfortable, embarrass you, hurt your feelings or make you feel bad.

Prohibited Conduct

Sourcewell does not tolerate any type of workplace violence committed by or against employees. Employees are prohibited from making threats or engaging in violent activities. This may include, but is not limited to:

- Causing physical injury to another person
- Direct or indirect threats of violence

- Conduct that intimidates or coerces another employee, client, supplier, or business associate
- Displaying aggressive or hostile behavior that creates a reasonable fear of injury to another person or subjects another individual to emotional distress
- Intentionally damaging employer property or property of another employee

Reporting Procedures:

Sourcewell will act to investigate all complaints, either formal or informal, verbal or written, of sexual harassment, discriminatory harassment, direct or indirect threats of violence, or incidents of actual violence, and to take appropriate action.

- A) Human Rights Officer. The Board of Directors hereby designates the Executive Director/CEO as Sourcewell's Human Rights Officer to receive reports or complaints of sexual harassment or sexual violence from any individual, employee, or victim of sexual harassment or sexual violence. If the complaint involves the Human Rights Officer, the complaint shall be filed directly with the Chair of the Board of Directors.

Sourcewell shall conspicuously post the name of the Human Rights Officer, including a mailing address and telephone number.

- B) Any person who believes he or she has been the victim of sexual harassment by an employee of Sourcewell, or any third person with knowledge or belief of conduct which may constitute sexual harassment or sexual violence should report the alleged acts immediately to Sourcewell's Executive Director/CEO as designated by this policy. Sourcewell encourages the reporting party or complainant to use the report form available online.
- C) Submission of a complaint or report of sexual harassment or sexual violence will not affect the individual's future employment or work assignments.
- D) Use of formal reporting forms is not mandatory.

Sourcewell will respect the right to privacy of those involved to the extent possible as allowed by law, consistent with Sourcewell's legal obligations and the necessity to investigate allegations of harassment and violence and take appropriate action when the conduct has occurred.

Investigation and Recommendation:

By authority of the Sourcewell Board of Directors, the Human Rights Officer, upon receipt of a report or complaint alleging harassment or violence, shall immediately authorize an investigation. This investigation may be conducted by the Manager of Human Resources or by a third party designated by the Executive Director/CEO. If a third party is used, that party shall provide a written report of the status of the investigation within ten (10) working days to the Executive Director/CEO as Human Rights Officer, and if the Executive Director/CEO is the subject of the complaint, the report shall be submitted to the Chair of the Board of Directors.

In determining whether alleged conduct constitutes sexual or discriminatory harassment or violence, Sourcewell shall consider the surrounding circumstances, the nature of sexual advances, any protected status, the relationships between the parties involved, and the context in which the alleged incidents occurred. Whether a particular action

or incident constitutes sexual or discriminatory harassment or sexual violence requires a determination based on all the facts and surrounding circumstances.

In addition, Sourcewell may take immediate steps, at its discretion, to protect the complainant and employees pending completion of an investigation of alleged workplace bullying, harassment, or violence.

The Human Rights Officer shall make a report to the Board of Directors upon completion of the investigation.

Action:

Upon receipt of a recommendation that the complaint is valid, Sourcewell will take action as appropriate based on the results of the investigation.

The result of the investigation of each complaint filed under these procedures will be reported in writing by Sourcewell to the complainant as allowed by law.

Reprisal:

Sourcewell will take appropriate action toward any individual who retaliates against any person who reports alleged harassment, or violence or who retaliates against any person who testifies, assists, or participates in an investigation, proceeding, or hearing relating to a discrimination, harassment, or violence complaint. Retaliation includes, but is not limited to, any form of intimidation, reprisal, or harassment.

Right to Alternative Complaint Procedures:

These procedures do not deny the right of any individual to pursue other avenues of recourse, which may include filing charges with the Minnesota Department of Human Rights, initiating civil action, or seeking redress under state criminal statutes and/or federal law.

Sexual Harassment or Sexual Violence as Sexual Abuse:

Under certain circumstances, sexual harassment or sexual violence may constitute sexual abuse under Minn. Stat. 609.341, subd. 10 through 609.345; Minn. Stat. 609.321 through -.324; or Minn. Stat. 617.246. In such situations, Sourcewell shall comply with Minn. Stat. 626.556, Reporting of Maltreatment of Minors.

Nothing in this policy will prohibit Sourcewell from taking immediate action to protect victims of alleged sexual abuse.

Grievance Procedure:

Any person who has a complaint alleging that Sourcewell is not complying with this policy or alleging any actions prohibited by this policy shall present the complaint in writing along with the reasons for such complaint to the Sourcewell Executive Director/CEO, who has been designated to handle complaints.

The Executive Director/CEO shall investigate the complaint and determine whether Sourcewell is in fact in violation of State or Federal law prohibiting discrimination. A decision shall be made by the designated official and such decision shall be communicated to the complainant within 15 days of the initial reception of the complaint.

If the Executive Director/CEO finds that the complaint is justified, he/she shall initiate action to rectify the complaint.

If the Executive Director/CEO finds that the complaint is not justified, he/she shall so notify the complainant in written communication.

If the complainant is not satisfied with the findings of the Executive Director/CEO, an appeal may be made to the Board of Directors. The appeal must be requested in a written communication to the Sourcewell Executive Director/CEO no later than 15 days after receipt of the written decision of the designated official.

A hearing before the Sourcewell Board of Directors shall occur no later than 30 days after receipt of a written request for such hearing. The complainant may testify and may request that others testify in the complainant's behalf. The designated official will present the findings of the investigation called for in step 2. The Sourcewell Board of Directors shall reach a decision and notify the complainant of its findings no later than 15 days after the hearing. If the complainant is not satisfied with the decision of the Sourcewell Board of Directors, appeal may be made to one or more of the following offices:

Office of Civil Rights, Chicago Office
U.S. Dept. of Education
Citigroup Center
500 W. Madison St., Suite 1475
Chicago, IL 60661-7204
312-730-1560
E-mail: OCR.Chicago@ed.gov

Commissioner of Human Rights
Freeman Bldg, 625 Robert St. No.
St. Paul, MN 55155
651-539-1100
E-mail: info.MDHR@state.mn.us

Usage of the Hay System

Purpose:

To establish a system for job evaluation that is compliant with the Local Government Pay Equity Act passed in 1984.

Policy:

Sourcewell shall use the Hay System for “comparable value.” Comparable value is the job evaluation rating or points assigned to a job. New job descriptions and revised job descriptions are evaluated using the process established through use of the Hay System. The comparable value or job evaluation rating does not include seniority or performance; rather, it is an evaluation of job content. Job content is measured by the skill, effort, responsibility, and working conditions required of the job.

Once a job description has been evaluated, job points are assigned. Job points are used to establish the Grade of the position and determine placement on the salary schedule.

Job descriptions shall be reviewed every three years. Interim, if a significant change in duties has occurred or new duties have been assigned, the position may be considered for job evaluation rating. The immediate supervisor and employee will confirm the proposed job description changes and will present for review to the Manager of Human Resources. The Manager of Human Resources will conduct the job evaluation and present recommendations to the Director of Administration. The Director of Administration will present and request review by the Senior Leadership Team for final determination. Once agreement is reached, the proposed job description will be recommended for approval to the Sourcewell Board.

To determine placement on the salary schedule following an employee’s movement to a higher Graded position through job description revision:

1. Use employee’s current step on current Grade.
2. Advance two steps on the salary schedule (if there are no steps available, will use the percentage of pay between steps to establish two steps).
3. Locate closest step on higher Grade on salary schedule, but no less than that in #2 above, to establish the placement on the salary schedule.

To determine placement on the salary schedule following an employee’s movement to a lower graded position:

1. Use employee’s current step on current Grade.
2. Retreat two steps on the salary schedule (if there are no steps available, use Step one of the salary schedule).
3. Locate closest step on lower Grade on salary schedule, but no less than that in #2 above, to establish the placement on the salary schedule

To determine placement on the salary schedule following an employee’s movement to a lower grade through job description revision:

1. Locate closest step on lower Grade on salary schedule, but no less than current rate, to establish the placement on the salary schedule
2. Employee is held harmless

An employee who, through an internal selection process, is being recommended for hire into a new position (as opposed to a job revision) has the right to negotiate a step on the salary schedule they feel meets their expectations for the position as if they were a new hire. The immediate supervisor of the position and Human Resources will work together to determine appropriate placement on the salary schedule based on relevant experience.

Nepotism Policy

Purpose:

Sourcwell is committed to the highest standards of conduct and expects all employees to adhere to them. Employees must avoid conflicts of interest, situations that might be perceived as conflicts of interest or situations that might impair objective judgment or be perceived as biased. The purpose of the Nepotism policy is to prevent unfairness in the employment relationship between blood relatives, members of the same household, or related parties. A Sourcwell employee may not directly influence decisions related to the recruitment, hiring, or the terms and conditions of employment of a person who is a member of the employee's immediate family, with whom he or she shares a household, or with whom he or she has a personal relationship.

Definitions:

Immediate Family: Immediate Family includes mother, father, children, siblings, spouse, any step-relation, domestic partner, grandparents, uncles, aunts, cousins, and in-laws of the same relation as any of the foregoing.

Household: Household includes anyone with whom the employee shares a house, apartment, or other living arrangement.

Personal Relationship: Personal Relationship includes a romantic/intimate relationship or other relationship in which there is a strong bond between the individuals.

Policy:

Relationship by family or marriage constitutes neither an advantage nor a deterrent to employment by Sourcwell, provided that the individual meets the appropriate standards for the position to be filled and provided that the individual will not be in the chain of supervision of a spouse, family member, or person with whom the individual has a personal relationship.

Procedure:

Existing Sourcwell employees who become involved in one of the foregoing circumstances must disclose the potential or perceived conflict to Sourcwell. Every effort will be made to resolve the conflict without loss of employment to either employee; however, Sourcwell reserves the right to transfer one or both employees, to discharge one or both employees, or to demote one or both employees to resolve the conflict. Employees who fail to advise Sourcwell of the existence of a family, spousal, or personal relationship under one of these circumstances will be subject to discipline, up to and including discharge.

The employment of members of the same immediate family, of those who share a household, or of those with other types of personal relationships may create conflicts of interest or the perception of conflicts of interest. Sourcwell will use sound judgment in the placement of such employees in accordance with the following guidelines:

- Members of the same immediate family, same household, or those involved in a personal relationship (Related Parties) are permitted to work in the same Sourcwell department, provided that no direct reporting or supervisor-to-subordinate relationship exists. That is, no individual should have decision-making authority or significant influence over the hiring, work responsibilities, salary, hours, career progress, benefits, or other terms and conditions of employment of a Related Party.
- If an applicant is otherwise qualified and might be selected for an available position but is a Related Party to an existing Sourcwell employee in the same department, the selecting authority should consult with

the Manager of Human Resources on the applicability of this policy and its motivating concerns before completing the hiring process.

Employment may be denied under the following circumstances:

1. Where one family member would have the authority or practical power to supervise, appoint, remove, or discipline another;
2. Where one family member would be responsible for auditing the work of another;
3. Where other circumstances exist, which would place family members in a situation of actual or reasonably foreseeable conflict between the employer's interest and their own.

Applicants who are denied employment to a particular position for one of the foregoing reasons will be considered for other vacant positions for which they may be qualified. Failure to advise Sourcewell of the existence of one of these circumstances may result in a withdrawal of an offer of employment or actual discharge from employment.

Any exceptions to this policy must be approved by the Director of Administration and/or the Executive Director/CEO or his/her designee.

Outside Employment

Rationale:

Sourcewell was established by the State of Minnesota as a public agency intended to offer member school districts and other governmental agencies a variety of services on a user fee basis, or in response to a professional services agreement.

Policy:

For Sourcewell to maximize the effectiveness of its present and future services to members, employees may not participate in activities for personal pay that are inconsistent with the interests of Sourcewell.

Employees may work outside the areas of their professional expertise during non-contract hours at their option.

Employees may, with prior written approval of the Executive Director, work in the areas of their professional expertise during non-contract hours if such employment is consistent with the best interests of Sourcewell. Sourcewell's liability insurance would not cover such employment. In evaluating whether or not particular employment may be in conflict with Sourcewell interest, the Executive Director will consider the past, present, and future scope of Sourcewell activities.

It is intended that the Executive Director will not approve:

1. Work as an independent contractor for a member within the present or possible future scope of the Sourcewell's activities.
2. Work as an independent contractor for an institution, firm, agency, or other governmental unit in an area where such institution, firm, agency, or other governmental unit might have contracted for Sourcewell's services.
3. Work as a salesman, representative, or agent for any commercial firm or nonprofit organization with a present or contemplated customer or client relationship with Sourcewell or any of its members.

The Executive Director may approve:

1. Work requested by a member government agency. In such cases the government agency will contract with Sourcewell and the employee will be paid by Sourcewell.
2. Work requested by an institution, firm, agency, or other governmental unit. In such cases, the entity will contract with Sourcewell and the employee will be paid by Sourcewell.
3. Work not presently within the scope of Sourcewell but requested by an institution, firm, agency, other governmental unit, or private party; this work would not be paid by Sourcewell.

Parental Leave

Purpose:

The goal of the Parental Leave Benefit is to attract and retain employees, as well as give employees additional flexibility and time to bond with their new child, adjust to their new family situation, and balance their professional obligations.

Policy:

WHO IS ELIGIBLE?

Employees are eligible for the Parental Leave Benefit if the following requirements are met:

1. Full-time employee of Sourcewell scheduled to work at least a .75 FTE
2. Employed six (6) months prior to the birth/adoption
3. Biological mother or father of the newborn or the adoptive mother or father of a child being placed in his/her custody.
 - a. Domestic partners and same sex spouses are included in this coverage.
 - b. Surrogate mothers and sperm or egg donors are not included in this coverage.

Procedure:

The Parental Leave Benefit will be provided to Sourcewell employees who have met the requirements listed above and have been approved for leave. Employees may use up to two (2) weeks (10 working (business) days) of leave per birth or adoption. If other special circumstances arise, they may be considered if approved by the Manager of HR. The ten (10) business days are full days to be used consecutively. Holidays, as outlined in the Sourcewell handbook, are not considered a part of the ten (10) day allotment. This leave will be used only for parental leave and must be used within twelve (12) calendar weeks of the birth and/or placement of the child into the employee's adoptive care.

Sourcewell's Parental Leave Benefit provides the benefit of 100% of the employee's regular base pay for their approved leave. It does not include overtime or any additional pay. As applicable, any contributions from the employer, accruals, or additional benefits will continue during this leave as if the employee was working. Birth of multiples, foreseen and/or unforeseen conditions around the birth or adoption will not lengthen the leave.

In order to utilize this leave, the employee must complete ALL THREE (3) of the items detailed below prior to their leave.

1. Employee must complete a request for Parental Leave.
2. Required documentation to support the leave, including:
 - a. Birth – Documentation of the child's birth or expected birth. This document must contain the name of the employee applying for the leave and the child's birth date or estimated birth date.
 - b. Adoption – Documentation that the petition has been filed.
3. The employee must work out a written plan for this leave with Human Resources and their immediate supervisor **prior** to leave.

This leave will run concurrently with an FMLA leave, MN Parental Leave, and/or Short-Term Disability, when applicable.

Employee Conduct and Respectful Workplace

Sourcewell is committed to a work environment in which all individuals are treated with respect and dignity. Sourcewell expects employees and others engaged to provide services, such as temporary personnel consultants, and independent contractors, to follow these rules of conduct while on the premises, attending Sourcewell functions, or otherwise performing work-related activity.

Sourcewell is responsible for providing a safe and secure workplace and strives to ensure that all individuals associated with Sourcewell are treated in a respectful and fair manner. Though it is not possible to list all forms of behavior that are unacceptable, the following are examples of behavior that would be considered inappropriate and in direct conflict with this policy. Such behavior may result in disciplinary action, up to and including termination of employment. This list is not intended to be exhaustive:

- Theft, inappropriate removal/possession, or willful destruction of Sourcewell property or the property of a fellow employee.
- Working under the influence of alcohol or illegal drugs.
- Possession, distribution, sale, transfer or use of alcohol or illegal drugs in the workplace or while performing work-related duties.
- Fighting or threatening violence in the workplace or while performing work-related duties.
- Sexual or other harassment.
- Using excessively abusive, threatening, or obscene language.
- Using intimidation tactics or making threats.
- Sabotaging another's work.
- Making malicious, false, and harmful statements about others.
- Publicly disclosing another's private information.
- Unauthorized disclosure of confidential information.
- Falsifying Sourcewell records or reports, including personal time records or the time records of another employee.

Workplace Bullying

Sourcewell will not tolerate bullying behavior. A bully may be a student or an adult. Workplace bullying is deliberate, disrespectful, repeated behavior targeted toward an individual. It is abusive conduct that includes:

- Threatening, humiliating, or intimidating behaviors
- Work interference or sabotage that prevents work from getting done
- Verbal abuse

Sourcewell considers the following types of behavior examples of bullying:

- **Verbal bullying.** Slandering, ridiculing, or maligning a person or his or her family; persistent name-calling that is hurtful, insulting, or humiliating; using a person as the butt of jokes; abusive and offensive remarks.
- **Physical bullying.** Pushing, shoving, kicking, poking, tripping, assault, or threat of physical assault, damage to a person's work area or property.
- **Gestures.** Nonverbal gestures that can convey threatening messages.
- **Exclusion.** Socially or physically excluding or disregarding a person in work-related activities.

If you feel that your rights as an employee have been violated, please report the incident(s) to the Human Resource Manager or the Human Rights Officer (Executive Director/CEO), or, if the incident involves the Human Rights Officer, to the Chair of the Board of Directors.

Reporting procedures are found in the Nondiscrimination, Anti-Harassment, and Violence Prevention Policy.

Seniority List

In January of each year, Human Resources will review and revise the Seniority List to reflect any addition or deletion of personnel. This list will be posted for 10 days for employees to review. The list will include the classification, name, date of employment, and qualifications of the certified staff listed. Any employee who disagrees with the information contained on the list will notify human resources to make correction.

A final Seniority list will be placed on the agenda of a Regular Board meeting for approval by the Sourcewell Board of Directors. Upon approval of the Board, the Seniority list shall be binding on Sourcewell and any employees.

No bumping rights exist between classifications.

Out-of-State Work Policy

Rationale:

Sourcewell recognizes that talent resides all across the U.S. and we have the opportunity to recruit, hire and retain talent outside of Minnesota. For some positions a candidate who does not reside in Minnesota may be the best fit and able to add value to the team and the organization.

Purpose:

This policy outlines guidelines for employees who have been approved to reside and work outside the State of Minnesota. All out-of-state work must receive prior approval from the Director of Administration and Division Director in collaboration with the hiring manager. Not all positions are appropriate or feasible for out-of-state work.

Scope:

This policy applies to exempt employees whose primary work location is not in Minnesota. Sourcewell does not support work from any location outside of the U.S. This policy does not apply to temporary out-of-state **travel**.

Procedure:

Employees may work out-of-state on a regular or temporary basis depending on business needs.

Permanent out-of-state work employees must indicate their primary working address in the Out-of-State Telecommuting Agreement. This agreement outlines their responsibilities as a telecommuting employee. *In the event of relocation*, the out-of-state telecommuting agreement is void and an employee's out-of-state work capability will be assessed on a case-by-case basis; continued employment is not guaranteed.

Prior to beginning any temporary out-of-state work, employees must receive support and approval by the Director of Administration and Division Director in collaboration with their immediate supervisor. This may be declined by the organization for any reason including untenable employment laws.

Out-of-state work does not change the terms and conditions of your employment with Sourcewell. Out-of-state employees must follow all Board Policies and organization procedures. Failure to fulfill work requirements or adhere to policies and procedures while working out-of-state may result in termination.

Sourcewell will provide our out-of-state employees with equipment as outlined in the out-of-state telecommuting agreement for the location they are assigned. All other costs associated with an office or additional technology and equipment are the responsibility of the employee.

Out-of-state employees are expected to take proper measures to ensure the protection of organization data, proprietary information, and assets.

Sourcewell does not support nomad work arrangements. Nomad work is work being conducted while traveling from state to state. This is not the same as temporary out-of-state work where the employee is seeking to work from one location for a period of time (i.e. Florida – Nov. thru Mar.). Sourcewell cannot support nomad work due to untenable tax implications for both the employee and the organization.

Upon termination of employment, all organization property will be returned to the organization immediately.

Social Media Policy

The purpose of this Policy is to establish principles for the use of personal Social Media accounts to interact with Sourcewell's official Social Media sites or to engage in other activities related to Sourcewell and its programs and services.

Definitions

Content: means any posts, writings, material, documents, photographs, graphics, or other information that is created, posted, shared, distributed, or transmitted via a User's personal Social Media account.

Social Media: means any current or future technology containing user-driven content, including, but not limited to, social networking sites, such as Facebook, Instagram, and LinkedIn; video-sharing applications, such as YouTube; micro-blogging applications, such as X; collaboration applications, such as Wikipedia; and other online forums and emerging applications.

User: means any Sourcewell employee and individual or entity under contract with Sourcewell, including temporary workers, interns, independent contractors, and third-party service providers.

Policy

1. Scope

- a. This Policy applies to Sourcewell employees, members of its Board of Directors, and other individuals and entities under contract with Sourcewell including independent contractors. This Policy does not apply to professional use of Sourcewell's official Social Media accounts by individuals authorized by and under the supervision of Sourcewell's Chief Marketing Officer or their designee.

2. Official Social Media Accounts

- a. Sourcewell Marketing is solely responsible for creating, developing, administering, monitoring, and controlling Sourcewell's official Social Media accounts.
 - i. Users are prohibited from stating or inferring that any Social Media account they create is an official Sourcewell account.
 - ii. Users are prohibited from posting Content on Sourcewell's official Social Media accounts except as permitted by and in compliance with this Policy.
 - iii. Users may submit Content they created for posting on an official Sourcewell Social Media account by entering a Marketing ticket.

3. Personal Social Media Accounts.

- a. Users may use their personal Social Media account(s) to take any of the following actions provided they do so in compliance with this Policy:
 - i. Follow Sourcewell's official Social Media accounts;
 - ii. Like, share, or comment on Content on Sourcewell's official Social Media sites;
 - iii. Connect with clients, suppliers, and other professional contacts; or
 - iv. Post comments or other Content referencing Sourcewell and its programs and services.

- b. In using their personal Social Media account(s) to take the actions stated above:
 - i. Users are prohibited from posting any comment or other Content that violates state or federal law; this or other Sourcewell Board Policies, including, but not limited to, the Information Security Program Policy and the Procurement Policy; Sourcewell's Employee Handbook; or any agreement governing the relationship between an individual or entity under contract with Sourcewell.
 - ii. Users must comply with the Minnesota Government Data Practices Act (MGDPA), Sourcewell's Data Practices Policy, and other applicable state and federal laws governing data security and privacy. Further, Users are prohibited from using Social Media to share, post, or otherwise disclose Confidential or Private Information as defined by the MGDPA.
 - iii. Users should request permission from the individuals involved before posting images, personal details, or comments about other Sourcewell employees, members of the Board of Directors, clients, suppliers, third-party or professional service providers, or other stakeholders.
 - iv. Users are prohibited from posting any comment or other Content that is inappropriate or may be harmful to Sourcewell's reputation or that of its employees, clients, suppliers, third-party service providers, and other stakeholders, including, but not limited to:
 - 1. Any post that may reasonably be deemed to negatively affect morale or undermine Sourcewell's ability to effectively serve the public.
 - 2. Any post that may be viewed as malicious, obscene, threatening or intimidating, disparaging, or might constitute harassment or bullying or contribute to a hostile work environment on the basis of sex, race, national origin, age, color, creed, religion, disability, marital status, familial status, veteran status, sexual orientation, gender identity, or gender expression, status with regard to public assistance or membership or activity in a local human rights commission.
 - v. Users must obtain permission from the creator or the owner prior to posting Content protected by trademark or copyright.
 - vi. Users may post comment related to Sourcewell or its programs and services provided they do not claim to speak on Sourcewell's behalf or claim to express an official Sourcewell position, and, via their Social Media profile, they:
 - 1. Disclose their connection to Sourcewell; and
 - 2. Include a disclaimer stating, "Comments are my own."
 - vii. Users must comply with Social Media Guidelines issued by Marketing.

4. Monitoring and Reporting.

- a. Users are encouraged to report any suspicious activity, controversial information, and posts by individuals purporting to represent or speak on Sourcewell's behalf to the Chief Marketing Officer.
- b. Users must notify Marketing upon learning of any Social Media Content or online commentary that generates press attention.

5. Compliance

- a. Compliance with this Policy is mandatory. Employees and members of the Board of Directors who violate this Policy will be subject to appropriate disciplinary action or other remedial measures up to and including termination of employment, if warranted under the circumstances and permissible under

applicable law. Violation of this Policy by an independent contractor, consultant, or other third-party service provider may result in termination of that party's contract with Sourcewell.

Telecommuting / Work from Home Policy

I. Purpose

Provide employees with the guidelines and controls for working remotely consistent with Sourcewell's needs as part of a strategy to attract and retain a highly qualified and skilled workforce. Teleworking, or telecommuting, is the concept of working from home or another location on a full- or part-time basis.

Telework provides a broad array of benefits to Sourcewell and its employees, including:

- Allowing employees the flexibility to work from an approved alternative worksite while delivering quality services.
- Supporting continuity of operations, including during health and safety situations impacting the Sourcewell workforce.
- Reducing the need for office space and parking.
- Minimizing impact on the environment.
- Attracting and retaining skilled workers.

Telework is not:

- A viable work arrangement for all positions or well-suited to all employees.
- An accommodation to complete personal or other non-Sourcewell endeavors during work hours.
- A replacement for appropriate childcare.
- A formal, universal employee benefit.
- A contract or guarantee of continued employment.

II. Eligibility

A position's suitability for teleworking is based on operational needs and the duties and responsibilities of the position as defined in the position description. Employees requesting telework arrangements must have and maintain a satisfactory performance record.

With the assistance of the human resource department, the employee and their supervisor will evaluate the suitability of a telecommuting/work-from-home arrangement by following the Telecommuting Procedure and executing a Telecommuting Agreement.

Employees' existing terms and conditions of employment with the organization remain unchanged, including but not limited to salary, retirement, vacation, sick leave benefits, and insurance coverage. The employee remains subject to all organizational policies and procedures.

Sourcewell retains the right to refuse or deny any teleworking request from an employee. Sourcewell or the employee may terminate a Telecommuting Agreement at any time, for any reason.

III. Confidentiality and Access

Equipment and files should only be accessible to the employee and safeguarded from access by other household members and visitors. The employee's supervisor should have access at a reasonable time to equipment and any paper records kept at an employee's home. Sourcewell encourages the use of electronic documents and files.

IV. Data/Security

The telework location extends Sourcewell's main business/office site. As such, you are responsible for complying with all laws, rules, regulations, and policies regarding data practices and data privacy. You must safeguard data to preserve data security as required by the Minnesota Government Data Practices Act and Sourcewell policy.

Consistent with Sourcewell's expectations of information security for employees working at the office, telework employees will be expected to protect confidential information accessible from their alternate work location. Steps include using locked file cabinets and desks, regular password maintenance, and other measures appropriate for the job and the environment.

V. Data Retention and Data Requests

Data created and maintained while teleworking is Sourcewell data regardless of whether the data was created and maintained on Sourcewell-owned equipment or your equipment and is subject to Sourcewell's data practices and records management policies. The employee is responsible for maintaining proper retention and disposal procedures for data at the telework location. The employee is responsible for returning any Sourcewell data upon request.

VI. Compliance with Law and Policies and Procedures

Teleworking arrangements must comply with federal, state, and municipal laws that apply to Sourcewell employees. This includes, but is not limited to, the Fair Labor Standards Act (FLSA) and the Occupational Safety and Health Act (OSHA). All employees who telework must adhere to all organizational Policies and Procedures.

VII. Equipment, Workspace, and Connectivity

Sourcewell will provide standard computer/technology equipment. The equipment selection shall be made by Sourcewell, subject to change at any time. Sourcewell is responsible for maintaining and supporting Sourcewell-owned equipment, including hardware and software.

Maintenance and repair of any technology equipment supplied and purchased by the employee is the employee's responsibility. Sourcewell accepts no responsibility for damage or repairs to employee-owned equipment.

The employee is responsible for all costs associated with the setup or maintenance of the employee's home office, such as remodeling, furniture, lighting, repairs, or modifications to the home office workspace.

The employee must provide a high-speed internet connection at home. The employee is responsible for all associated costs, including initial setup, ongoing billings, and related repairs and services.

VIII. Liability

The telework location extends Sourcewell's main business/office site. Therefore, Sourcewell will continue to be liable for job-related accidents in the employee's home workspace or alternate work location during the employee's agreed-upon working hours. Employees are responsible for notifying their supervisor and human

resources of any injuries in accordance with the organization's workers' compensation procedures.

Sourcewell assumes no liability for injuries occurring in the employee's home workspace or alternate work location outside the agreed-upon work hours.

Sourcewell is not liable for loss, destruction, or injury that may occur in or to the employee's home. This includes family members, visitors, or others that may become injured within or around the employee's home.

IX. Ad Hoc Arrangements

Temporary teleworking arrangements may be approved for inclement weather, special projects, or business travel. These arrangements are approved as needed, with no expectation of ongoing continuance.

Flexible work arrangements may be made for employees on family or medical leave to the extent practical for the employee and the organization and with the consent of the employee's health care provider, if appropriate.

All informal Ad Hoc arrangements are made case-by-case, focusing first on the organization's business needs.

END POLICY

Mileage Reimbursement Policy

Purpose

The intent of this policy is to appropriately reimburse employees for travel expenses incurred while performing qualified business activities. Employees using their personal vehicles for business use will be reimbursed at the current IRS mileage rate in effect at the time of travel.

Procedure

For staff who are telecommuters with a principal work location of an approved home office and live within 75 miles of designated office headquarters (Staples or St. Paul):

- Mileage to designated headquarters would not be reimbursed
- Mileage to alternate headquarters would be reimbursed minus the lesser of a round-trip to designated headquarters or 150 miles
- Any other mileage for work-related purposes would be reimbursed for the full distance between their home (principal work location) and work assignment (i.e., conference, airport, member/client site, etc.)

For staff who are telecommuters with a principal work location of an approved home office and live more than 75 miles from designated office headquarters (Staples or St. Paul):

- Mileage to designated or alternate headquarters would be reimbursed minus 75 miles (150 miles round-trip)
- Any other mileage for work-related purposes would be reimbursed for the full distance between their home (principal work location) and work assignment (i.e., conference, airport, member/client site, etc.)
- Per diems may be reimbursed for trips to headquarters at the manager's discretion
- Lodging expenses for a trip to headquarters must be pre-approved at the manager's discretion and paid for using Sourcewell-issued P-card

If a staff member ceases to telecommute on a regular and continuous basis mileage to designated headquarters would no longer be reimbursed regardless of distance.

Expenses for parking fees and tolls are eligible for reimbursement in addition to the mileage rate.

Sourcewell cannot reimburse employees for parking tickets, moving violations fines, vehicle towing charges, or personal vehicle repairs or maintenance.

Definitions

Business Use: Travel to and from destinations for the sole purpose of conducting business activities on behalf of Sourcewell.

Principal Work Location: The principal office/workspace location as identified in the Telecommuting Agreement.

Work from Home Arrangement: The main business/office site is the employee's principal work location.

Telecommuter: Working primarily from home or base from home and working outside of the main business/office site. The employee's principal work location is at their residence.

Military Differential Pay Policy

As an employer of choice, Sourcewell wishes to further support and recognize its employees who are engaged in active military service with the National Guard or any military reserve component by adopting this Military Pay Differential Policy. "Active military service" is defined by Minnesota Statutes § 190.05, subdivision 5, and includes periods of active Federal service, active State service, and federally funded State active service.

Sourcewell will pay a qualifying employee an amount equal to the employee's salary differential for each scheduled workday that the person is ordered to serve in active military service. The salary differential is calculated via a pay chart-to-chart comparison, which will include any pay chart adjustments and scheduled raises at Sourcewell or with the military during the period of active service. The differential calculation does not include any civilian or military pay or benefits beyond the applicable and respective salary charts. Employees are eligible only if active-duty military pay chart wages are less than Sourcewell civilian pay chart wages. Payments will be made in a lump sum after the employee service member has returned to employment with Sourcewell. Periodic pay schedules (as opposed to a lump sum) may be considered in the event of hardship and at the sole discretion of Sourcewell. Any periodic pay schedule and terms will be reduced to writing and communicated to the employee and must be approved by the Executive Director upon the recommendation of Human Resources.

The following periods of military service are exempt from this policy, and an employee will not be entitled to differential pay for these exempt periods:

1. Basic Training, advanced individual training, annual training, and periodic inactive duty training.
2. Special and incidental training is periodically made available to National Guard and reserve component members.
3. Service performed in accordance with Minnesota Statutes § 190.08, subdivision 3.

To be eligible for differential pay, an employee must return to employment with Sourcewell and meet the reinstatement requirements of any applicable federal or state law. The cumulative period of differential payments under this policy must not exceed four years.

Food and Non-Alcoholic Beverage Policy

1. Purpose

- a. Generally, food and beverage purchases are not allowable. This Food and Non-Alcoholic Beverage policy (F&NAB Policy) will guide Sourcewell employees and elected officials on allowable expenditures of public funds for food and beverage purchases. Food and beverage purchases must meet public purpose legal requirements (Public Purpose Doctrine) defined by the Minnesota Supreme Court as follows:
 - i. There is express or implied statutory authority to support the purchase.
 - ii. The purchase will benefit the Region 5 community as a whole.
 - iii. The purchase directly relates to Sourcewell's statutory functions.
 - iv. The purchase does not have, as its primary objective, the benefit of a private interest – i.e., the purchase does not constitute a gift as legally defined. (See Sourcewell Gift Policy.)
- b. Express or implied authority for an expenditure must be found in state statute. Express authority is specific and is usually straightforward; if authority to support a food or beverage purchase is not clearly stated as an allowed expenditure, you should contact the Sourcewell Chief Financial Officer. The Chief Financial Officer may seek advice from the General Counsel.
- c. Providing food and beverages with Sourcewell funds is not an allowable expenditure except as provided for in this policy. Purchases of alcohol or tobacco are never permitted.

2. Allowable food and beverage expenditures

- a. The purchase of food and beverage is allowed if it meets all requirements of the Public Purpose Doctrine outlined above and one or more of the following circumstances apply:
 - i. Member, Participating Entity and Partnership Events
 1. Food and beverages may be purchased for events held for designated members or participating entities and partners when:
 - a. The purpose of the event is education, training, planning, or the provision of specific services; and
 - b. Food and beverages (i.e., breakfast, lunch, or dinner) are necessary because the timing and length of the event do not allow for meal breaks, or the food and beverage cost is nominal (e.g., snacks) and incidental to the event.

ii. Public Outreach Events

1. Food and beverages may be purchased for events held for public outreach purposes when:
 - a. Most anticipated participants are not Sourcewell employees; and
 - b. The purpose of the event is to solicit public input from or impart information to the public about Sourcewell's public agency functions and services; and
 - c. Food and beverages (i.e., breakfast, lunch, or dinner) are necessary because the timing and length of the event do not allow for a meal break, or the food and beverage cost is nominal (e.g., snacks) and incidental to the event.

iii. Official Meetings

1. Food and beverages may be provided during meetings of the Sourcewell Board, official committees, and advisory groups when:
 - a. Food and beverages (i.e., breakfast, lunch, or dinner) are necessary because the timing and length of the event do not allow for a meal break, or the food and beverage cost is nominal (e.g., snacks) and incidental to the event.

iv. Internal Meetings of the Sourcewell Senior Leadership (SLT) Team, Organizational Planning Sessions and Workgroups, Departmental Meetings

1. Food and beverages may be provided during SLT meetings, organizational planning sessions, workgroups departmental and similar meetings when:
 - a. The meeting has three or more participants and does not allow for interruptions for meal breaks; and
 - b. Food and beverages may not be provided at departmental meetings more frequently than once per month and, in every instance, only when all other requirements of this policy are satisfied.

v. Training and Professional Development

1. Food and beverages may be provided during training and professional development when:

- a. The training or professional development does not allow for interruptions of meal breaks.

vi. Interview Panels

1. Food and beverages may be provided for interview panels when the interview schedule exceeds six hours and does not allow for a reasonable break accommodation for a meal.

vii. New Employee Lunch

1. Food and beverages may be purchased to provide lunch to welcome new employees.

viii. Organizational-wide Events

1. Because Sourcewell is an organization with a highly distributed workforce, food and beverages may be provided at up to four organizational-wide events per fiscal year.

3. Employee Meal Per Diems

- a. Sourcewell follows the GSA established nontaxable rates to reimburse employees for their meals while on official business travel. Per the GSA, travel status is defined as being away from the employee's primary work location in excess of 12 hours. The reimbursable guidelines are as follows:

i. Breakfast

1. Breakfast per diem may be claimed if the employee is in travel status and leaves their primary work location before 6:00 a.m. or is away from home overnight.

ii. Lunch

1. Lunch per diem may be claimed if the employee is in travel status away from their primary work location or is away from home overnight.

iii. Dinner

1. Dinner per diem may be claimed only if the employee is in travel status away from their primary work location until after 6:00 p.m. or is away from home overnight.

- b. Day travel away from the employee's primary work location exceeding either 8 working hours (including travel) or 75 miles is eligible for lunch per diem. Per diem should be

entered at the location where the employee spent the majority of the day.

- c. Employees are paid an additional taxable meal per diem in addition to the established nontaxable GSA rates. The Chief Financial Officer will review and set rates annually. The additional taxable meal per diem amendment process will coincide with GSA rate study cycles of October 1st through September 30th.

4. Per Meal Expenditure Guidelines

- a. In all instances, the per-person amount expended for food and beverages should approximate the GSA per diem schedule per meal rate as closely as possible. Any per person amount exceeding 300% of the GSA per diem schedule will be investigated for necessity. The GSA per diem schedule includes tipping. Per Diem Rates | GSA: <https://www.gsa.gov/travel/plan-book/per-diem-rates>
- b. For meals outside of the continental United States where the GSA schedule does not provide a meal rate, the Department of Defense (DoD) meals and incidental expenses (M&IE) will be used to calculate the allowable meal expenditure amount. Per Diem Rate Lookup | Defense Travel Management Office (dod.mil) <https://www.travel.dod.mil/Travel-Transportation-Rates/Per-Diem/Per-Diem-Rate-Lookup/>

5. Preapproval and Authorization

- a. Preapproval and Authorization of food and beverage expenditures is not required but is strongly encouraged any time an employee is not certain a food and beverage expenditure is required or reasonable.

6. Other Considerations

- a. Employees should make every effort to minimize the necessity of meal expenditures.
- b. Itemized receipts are required to support all expenditures using a Sourcewell P-card. Failure to include itemized receipts for food and beverage expenditures will result in progressive corrective action, including revocation of the Sourcewell purchasing card.
- c. Employee per diem reimbursement for food and beverage-related travel expenses is covered in the Sourcewell Employee Handbook.
- d. Any policy violation will result in progressive corrective action, including revocation of

Sourcewell's purchasing card.

See Board Policy "Procurement Card."

Information Security Policies

Article I. Introduction.

1.1 Purpose.

1.1.1 Information Security Policies. The purpose of this document (“these Policies”) is to delineate the policies Sourcewell has adopted to:

- A. Comply with its statutory and regulatory obligations with respect to privacy and data security; and
- B. Support its efforts to protect the security, confidentiality, integrity, and availability of the data it collects, stores, uses, or disseminates and the systems Sourcewell uses to perform these functions.

1.1.2 Supporting Documentation. These Policies are supplemented by applicable standard operating procedures and information technology and information security standards and practices which describes the specific administrative, physical, and technical safeguards and controls used to fulfill the obligations described in these Policies.

1.2 Scope.

1.2.1 Technology Resources. These Policies apply to all data, systems, activities, and assets owned, controlled, or used by Sourcewell (“Technology Resources”), including, but not limited to, infrastructure; communication systems and devices; information systems and services; computer hardware, software, and devices; and any new technologies implemented by Sourcewell.

1.2.2 Users. These Policies apply to any individual (“User”) who accesses or uses Sourcewell’s Technology Resources. This includes Sourcewell employees as well as any consultant, independent contractor, service provider, or vendor (“Third Party”) engaged by Sourcewell. Employee-specific privacy and data security processes and expectations are outlined in more detail in Sourcewell’s Employee Handbook.

1.3 Sanctions. Any Sourcewell employee found to be in violation of these policies may be subject to disciplinary action up to and including termination of employment. Employees who violate local, state, or Federal law may also be subject to civil or criminal prosecution. Any Third Party that violates this Policy may be found in breach of contract or face civil and criminal prosecution.

1.4 No Expectation of Privacy and Monitoring. **Users shall have no expectation of privacy while using Sourcewell’s Technology Resources.** Sourcewell reserves the right to review, search, monitor, and control use of its Technology Resources and to retrieve, alter, or delete any data created, received, transmitted, or stored by any User on or through Sourcewell’s Technology Resources to the extent permitted by applicable law. The use of Technology Resources constitutes the User’s authorization for Sourcewell to take these actions.

1.5 Training. Sourcewell will provide resources and training opportunities where necessary to help Users understand their obligations under these Policies. Employees must complete information

Artificial Intelligence Policy

Sourcewell maintains an Information Security Program (the “Program”) which establishes the governance structure for all information technology assets used by or on behalf of Sourcewell. The purpose of this Artificial Intelligence Policy (“AI Policy”) is to establish a governance structure for all AI systems used by or on behalf of Sourcewell. Use of such systems must comply with this Policy and all other provisions of Sourcewell’s Information Security Program.

Definitions

Artificial Intelligence: “Artificial intelligence” or “AI” is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

Algorithm: “Algorithm” is a series of logical steps through which an agent (typically a computer or software program) turns particular inputs into particular outputs.

AI system: “AI system” is any system, software, sensor, or process that automatically generates outputs including, but not limited to, predictions, recommendations, or decisions that augment or replace human decision-making. This extends to software, hardware, algorithms, and data generated by these systems, used to automate large-scale processes, or analyze large data sets.

Policy

1. Scope

- a. This AI Policy applies to:
 - i. All AI systems used by or on behalf of Sourcewell; and
 - ii. Staff (full-time, part-time), interns, consultants, contractors, and board members who may be purchasing, configuring, developing, operating, or maintaining Sourcewell’s AI systems or who may be using AI systems to provide services to Sourcewell.

2. Guiding Principles for Responsible AI Systems

- a. These principles describe Sourcewell’s approach with regards to how AI systems are purchased, configured, developed, operated, or maintained.
 - i. Human-Centered Design: AI systems are developed and deployed with a human-centered approach that evaluates AI powered services for their impact on the public.
 - ii. Security & Safety: AI systems maintain confidentiality, integrity, and availability of data through safeguards that prevent unauthorized access and use. Implementation of AI systems is reliable and safe, and minimizes risks to individuals, society, and the environment.

- iii. Privacy: Privacy is preserved in all AI systems by safeguarding personally identifiable information (PII) and sensitive data from unauthorized access, disclosure, and manipulation.
- iv. Transparency: The purpose and use of AI systems is proactively communicated and disclosed to the public. An AI system, its data sources, operational model, and policies that govern its use are understandable and documented.
- v. Equity: AI systems support equitable outcomes for everyone. Bias in AI systems is effectively managed with the intention of reducing harm for anyone impacted by its use.
- vi. Accountability: Roles and responsibilities govern the deployment and maintenance of AI systems, and human oversight ensures adherence to relevant laws and regulations.
- vii. Effectiveness: AI systems are reliable, meet their objectives, and deliver precise and dependable outcomes for the utility and contexts in which they are deployed.
- viii. Workforce Empowerment: Staff are empowered to use AI in their roles through education, training, and collaborations that promote participation and opportunity.

3. Roles and Responsibilities

- a. The Information Technology Officer (ITO) is responsible for directing Sourcewell technology resources, policies, projects, services, and coordinating the same with other Sourcewell departments. The ITO shall designate the Director of IT Systems and Services to actively ensure AI systems are used in accordance with this policy and all other provisions of Sourcewell's Information Security Program.
- b. The Director of IT Systems and Services is responsible for overseeing the enterprise security infrastructure, cybersecurity operations, updating security policies, procedures, standards, guidelines, and monitoring policy compliance.
- c. Sourcewell staff (full-time, part-time), interns, consultants, contractors, and board members are responsible for following this policy and following updates to this policy and all other provisions of Sourcewell's Information Security Program and shall check compliance with these documents at least annually.
- d. The ITO or designee shall notify Sourcewell departments when an update to this policy or other provisions of Sourcewell's Information Security Program is released.
- e. The Chief Legal Officer or designee is responsible for advising of any legal issues or risks associated with AI systems usage by or on behalf of Sourcewell departments.
- f. The Chief Executive Officer or designee, may at their discretion, inspect the usage of AI systems and require a department to alter or cease its usage of AI systems or a partner's usage of AI systems on behalf of Sourcewell.
- g. The Chief Procurement Officer or designee is responsible for overseeing the procurement of AI systems and requiring vendors to comply with Sourcewell policy standards through contractual agreements.

4. Purchasing, Configuring, Developing, Operating, Or Maintaining AI Systems

- a. Uphold Guiding Principles for Responsible AI Systems;
- b. Conduct an AI Review to assess the potential risk of AI systems. The Director of IT Systems and Services is responsible for coordinating reviews of AI systems prior to use by Sourcewell as detailed in Sourcewell's Information Security Program;
- c. Obtain technical documentation about AI systems or create equivalent documentation for internally developed AI systems as detailed Sourcewell's Information Security Program;
- d. Require suppliers and contractors to comply with this AI Policy and Sourcewell's Information Security Program;
- e. In the event of an incident involving the use of AI systems, follow an Incident Response Plan as detailed in Sourcewell's Information Security Program.

5. Prohibited Uses of Artificial Intelligence

- a. Sourcewell prohibits the use of certain AI systems due to the sensitive nature of the information processed and potential risks. This includes the following prohibited purposes:
 - i. Real-time and covert biometric identification, including, but not limited to, facial recognition and iris scanning;
 - ii. Emotion analysis, or the use of computer vision techniques to classify human facial and body movements into certain emotions or sentiment (e.g., positive, negative, neutral, happy, angry, nervous);
 - iii. Fully automated decisions that do not require any meaningful human oversight but substantially impact individuals;
 - iv. Social scoring, or the use of AI systems to track and classify individuals based on their behaviors, socioeconomic status, or personal characteristics;
 - v. Cognitive behavioral manipulation of people or specific vulnerable groups;
 - vi. Autonomous weapons systems; and
 - vii. Uploading or otherwise sharing protected information in AI systems and platforms.

6. Violations of the AI Policy

- a. Violations of any section of this AI Policy, including failure to comply with Sourcewell's Information Security Program may be subject to disciplinary action up to and including termination. Violations made by a third party while operating an AI system for on behalf of Sourcewell may result in termination of contract and/or pursuit of damages. Use of AI systems in violation of state or federal law may be referred to law enforcement for prosecution.

security training within the timeframes required by Sourcewell. Failure to participate in required training may constitute a violation of this Policy.

- 1.6 Information Security Coordinator. The Sourcewell Board of Directors has appointed the Manager of IT Operations to serve as Sourcewell’s Information Security Coordinator. References to the Information Security Coordinator or Sourcewell IT in these Policies means the Information Security Coordinator or any IT staff authorized by and under the supervision of the Information Security Coordinator.
 - 1.6.2 Authority. The Information Security Coordinator is authorized to develop, implement, maintain, and enforce these Policies and any related policies, standards, and processes they deem necessary and appropriate, including, but not limited to, the Information Security Program.
 - 1.6.3 Policy Review. On or before May 1st each year, the Information Security Coordinator must initiate review of this Policy and engage other departments and stakeholders, including Human Resources and Legal, as appropriate.

Article II. MGPDA, HIPAA, and Other Applicable Laws

Various information security laws, regulations, and industry standards apply to Sourcewell and the data Sourcewell Users collect, store, use, and disseminate. Sourcewell is committed to comply with applicable laws, regulations, and standards, which include, but are not limited to, the following:

- 2.1 Minnesota Government Data Practices Act (“MGDPA”). The MGDPA at Minnesota Statutes, Chapter 13, govern the collection, creation, storage, maintenance, and dissemination of data held by Minnesota governmental entities (“Government Data”), including Sourcewell. Sourcewell’s Data Practices Policy, Data Inventory, and Records Retention Schedule, which outlines its policies with respect to the classification, disclosure, and disposition of Government Data. The Data Practices Policy, Data Inventory, and Records Retention Schedule can be found under “Legal Policies” in the Board Policy Book.
- 2.2 Health Insurance Portability and Accountability Act (“HIPAA”).¹ Sourcewell serves as the Sponsoring Association and provides administrative services for the Better Health Collective, a government joint risk pool for employee benefits. In that capacity, certain Users have access to and use Protected Health Information (“PHI”)² governed by HIPAA. An entity, like Sourcewell, that conducts functions governed by HIPAA and other functions that are not may designate itself as a hybrid entity for HIPAA compliance purposes. Sourcewell has designated itself as a hybrid entity. The following documents Sourcewell’s intent to comply with the HIPAA and the HITECH Act applicable to this designation.
 - 2.2.1 Designated Health Care Component. Sourcewell’s Department of Insurance and Risk Management (“IRM”) is solely responsible for conducting the functions governed by

¹ 45 CFR Parts 160, 162, and 164

² “Protected Health Information (PHI)” means any health information that is transmitted and maintained and that identifies an individual or can be used to identify an individual.

HIPAA and the only department that employs Users with access to PHI. Therefore, Sourcewell has designated IRM as its sole healthcare component.

- 2.2.2 Safeguards. IRM Users do not disclose PHI to other departments in a manner that would be prohibited if IRM and other departments were separate legal entities. IRM Users also protect electronic PHI from other Sourcewell departments in the same manner as it would be required if IRM and other departments were separate legal entities. Finally, if a User performs duties for IRM and a non-healthcare component, the User does not use or disclose PHI created or received in the course of or incident to their IRM work in a manner that would be prohibited under HIPAA.
- 2.2.3 Privacy and Security Officer. Sourcewell has appointed its IRM Manager as the Privacy and Security Officer for its healthcare components.
- 2.3 Family Education Rights and Privacy Act (“FERPA”).³ Sourcewell serves as a third-party service provider to educational entities throughout the United States. In that capacity, certain Users have access to and use Personally Identifiable Information⁴ governed by the FERPA. FERPA requires Sourcewell to implement safeguards to protect this data. This Policy is intended to demonstrate Sourcewell’s compliance with these obligations.
- 2.4 Other State Laws. Statutes in some states outside Minnesota provide for additional statutory protections for student data beyond those provided for in FERPA. Sourcewell developed these Policies to include data protections required by FERPA and those common to most customers, including those in other states. As a result, when a customer asks Sourcewell to agree to additional customer-specific requirements:
 - 2.4.1 Review and Approval. Legal and the Information Security Coordinator must review all related documentation, including the customer’s information security policies or standards and any related agreements requiring Sourcewell to comply.
 - 2.4.2 Compliance. If Sourcewell Legal and the Information Security Coordinator agree that Sourcewell is willing and able to comply with customer-specific information security policies or standards, the Information Security Coordinator is responsible for notifying affected Users and ensuring they have the resources needed to comply with the additional requirements.

Article III. Access Controls and Acceptable Use

Sourcewell has implemented the following safeguards and controls to protect Sourcewell’s Technology Resources.

- 3.1 Requests for Access. Authorized staff may request to add, change, or terminate access for internal Users under their supervision and external Users with a demonstrated need that cannot be reasonably met through other means. Staff requesting access are responsible for ensuring

³ 34 CFR Part 99.

⁴ “Personally Identifiable Information” means records that are directly related to a student and which identifies the student or which would allow a person to identify the student with reasonable certainty.

Users under their supervision comply with these Policies and for notifying Sourcewell IT when a User leaves the organization, or their engagement is terminated.

3.2 Identity and Access Management. Sourcewell uses identity and access management controls to provide User accounts with appropriate access privileges.

3.2.1 In general. Sourcewell IT will only grant access to Sourcewell's Technology Resources to authorized Users. Users will only receive access to the Technology Resources required to perform their responsibilities.

3.2.2 Unique User Accounts. Sourcewell IT will assign each User a unique account, password, passphrase, or other credentials to provide for individual accountability. Users are prohibited from sharing their credentials with others. Where necessary, Sourcewell IT will use systems logs or other technical controls to identify and/or mitigate unauthorized access.

3.2.3 Entity Authentication. Any User accessing Sourcewell's Technology Resources must be authenticated. The level of authentication must be appropriate to the data being accessed and the User's role.

3.2.4 Unauthorized Access. Users are prohibited from gaining unauthorized access to Sourcewell's Technology Resources or in any way damaging, altering, or disrupting these Resources.

3.3 Acceptable Use Policy. Sourcewell provides Users with Technology Resources to support its business requirements and functions. This section describes Sourcewell's policy with respect to the use of these Technology Resources and explains the steps Users must take to protect them.

3.3.1 General Use of Information Technology Resources. Access to and use of Technology Resources is a privilege and not a right. Unacceptable use of Technology Resources may result in disciplinary action up to and including termination of employment. Users who violate local, state, or Federal law may also be subject to civil or criminal prosecution.

A. Acceptable use includes all authorized access to and use of Sourcewell's Technology Resources as needed to fulfill a User's assigned duties and functions. Minimal personal use is acceptable to the extent it does not interfere with the User's performance of their responsibilities or impair another User's ability to theirs.

B. Unacceptable use includes all unauthorized access to and use of Sourcewell's Technology Resources for purposes including, but not limited to:

1. Transmitting, receiving, or storing Government Data in violation of Sourcewell's Data Practices Policy or other applicable state and federal privacy laws.
2. Achieving personal gains or other activities that may create a real or perceived conflict of interest with Sourcewell.

3. Creating undue security risks or negatively impacting the performance of Sourcewell's Technology Resources.
4. Causing embarrassment, loss of reputation, or other harm to Sourcewell.
5. Hacking, spoofing, or launching denial of service attacks.
6. Gaining or attempting to gain unauthorized access to others' networks or systems.
7. Sending fraudulent email messages.
8. Distributing or attempting to distribute malicious software.
9. Spying or attempting to install spyware or other unauthorized monitoring or surveillance tools.
10. Committing acts such as terrorism, fraud, or identity theft.
11. Downloading, storing, or distributing child pornography or other obscene or illegal materials.
12. Violating another's intellectual property rights.
13. Uploading, downloading, or disseminating defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene, or otherwise inappropriate or offensive messages or media.
14. Distributing joke, chain letter, commercial solicitations, or hoax emails or other mass messaging or spamming.
15. Disrupting the workplace environment, creating a hostile workplace, or invading the privacy of others.
16. Using encryption or other technologies in an attempt to hide illegal, unethical, or otherwise inappropriate activities.
17. Installing or distributing unlicensed or pirated software.

3.3.2 Desktop, Laptop, and End-User Controls. Users may only access Sourcewell's Technology Resources using Sourcewell-provided user accounts on approved devices that support Sourcewell's current minimum information security standards.

3.3.3 Social Media. Users must comply with Sourcewell's Social Media Guidelines, found in Sourcewell's Employee Handbook, when using their personal Social Media accounts to interact with Sourcewell's official Social Media sites or to engage in other activities related to Sourcewell and its programs or services.

- 3.3.4 Mobile Devices and Bring Your Own Device to Work. Any use of personnel mobile devices, including laptops, smartphones, and tablet computers, to connect to Sourcewell's Technology Resources must be approved in advance by Sourcewell IT. If Sourcewell IT permits any User to use their own device for this purpose, the User must agree to use such devices subject to this Policy and any additional policies, procedures, standards, and processes Sourcewell implements. Further:
- A. Sourcewell may require the User to install specific security controls on the device, including device management software, access controls, encryption, and remote wiping capabilities.
 - B. The User must allow Sourcewell IT to review the device and remove any Government Data, if their relationship with Sourcewell terminates, the User changes devices or services, and in other similar situations. The User must also promptly provide Sourcewell IT with access to the device when requested for Sourcewell's legitimate business purposes.
 - C. Devices with access to Sourcewell email or other Technology Resources must be protected by password/passphrase or another approved authentication method. Such devices must be physically secured by the user at all times.
 - D. The User is prohibited from connecting a mobile device containing Government Data to any unsecured network without technology security controls in place. Unsecured networks include home networks, hotel networks, open or for-pay wireless hotspots, convention networks, or any other network that Sourcewell has not approved or does not control.
- 3.3.5 Remote Access. Sourcewell IT has implemented technology solutions and controls which provide users with remote access capabilities to approved Technology Resources. Users with remote access privileges may only use Sourcewell-provided means and multifactor authentication to access Sourcewell's Technology Resources. Users are prohibited from installing or setting up any other remote connections, including remote desktop software. Remote access connections to Sourcewell Technology Resources must be configured to time out or be disconnected as prescribed in existing information technology and information security standards and related standard operation procedures.
- 3.3.7 External Network Connections. Sourcewell IT and the Information Security Coordinator must review and approve all extranet and other connections to Sourcewell's Technology Resources before implementation. A signed business agreement between Sourcewell and any organization seeking access must accompany any request for extranet connection. Connectivity will be limited to only those assets required to perform the specified functions. Extranet connections will be monitored and may be deactivate if unusual or inappropriate traffic is detected.
- 3.3.8 Wireless Network Connections. Users are prohibited from connecting any wireless access points, routers, or other similar devices to Sourcewell Technology Resources without prior approval from Sourcewell IT and the Information Security Coordinator.

Users are prohibited from connecting wireless access points (WAPs) directly to Sourcewell's trusted network.

Article IV: Protecting and Managing Sourcewell's Information Technology Environment

4.1 Protecting Information Assets. Sourcewell IT installs and configures its computers according to current technical standards and procedures, including anti-virus software, standard security controls, and approved operating system version and software patches. Only Sourcewell-supplied or approved software, hardware, and information systems may be installed in Sourcewell's IT environment or connected to its network.

4.1.1 End-User Computers and Access.

- A. End-user computers are configured to request authentication from Sourcewell's domain at startup and user login. Sourcewell may deny network access to end-user computers that do not meet current standards.
- B. User accounts are configured to require strong passwords/passphrase and multifactor authentication. To protect against password/passphrase guessing and other brute force attacks, Sourcewell will deactivate a user's account after five (5) failed login attempts. Reactivation may be based on a timeout or manual reset. Authentication credentials must be encrypted during transmission across any internal or external network.

4.1.2 Passwords and User Credentials. Sourcewell has implemented automated password/passphrase rules to ensure that users are required to use strong passwords/passphrases. IT procedures and technical standards define these password rules and other authentication means. Users are required to protect all user credentials, including passwords, passphrases, tokens, badges, smart cards, or other means of identification and authentication. Specifically, Users are prohibited from:

- A. Disclosing passwords, passphrases, one-time use codes, or another authentication means to anyone, including anyone who claims to be from Sourcewell IT;
- B. Writing down passwords/passphrases or otherwise recording them in an unsecure manner
- C. Using save password features for applications
- D. Using the same password/passphrase for different systems or accounts, except where single sign-on features are automated; and
- E. Reusing passwords/passphrases

4.1.3 Perimeter Controls. Sourcewell IT uses perimeter controls to secure its network against external attacks. Firewalls are also used and configured according to current technical standards and procedures to separate Sourcewell's trusted network from the internet or internet-facing environments. Sourcewell may, at its discretion, implement additional

perimeter controls, including intrusion detection and prevention services, data loss prevention software, specific router or other network configurations, or network monitoring. Users are prohibited from creating internet connections outside perimeter controls.

4.1.4 Data and Network Segmentation. Sourcewell IT uses technical controls, such as firewalls, access control lists, or other mechanisms, to segment some data or areas of its network. Users are prohibited from altering segmentation plans without approval from Sourcewell IT.

4.1.5 Encryption.

- A. Sourcewell may encryption stored data (data-at-rest) and transmitted data (data-in-transit) using generally accepted encryption algorithms and products approved by the Information Security Coordinator. Sourcewell IT will periodically review encryption products and algorithms for any known risks.
- B. Encryption algorithms use keys to transform and secure data. Because they allow decryption of the protected data, Users must use proper key management, which includes selecting encryption keys to maximize protection levels, ensuring keys are available when needed to support data decryption by using secure storage methods and creating and maintaining secure backups, tracking access to keys, and changing keys on a periodic basis according to risks.

4.1.6 Data and Media Disposal. When Sourcewell IT retires or otherwise removes Technology Resources, it will scrub or otherwise render data contained thereon unreadable and unrecoverable. This process may include destroying data media according to applicable waste disposal regulations or using data wiping software that meets generally accepted data destruction standards.

4.1.7 Log Management and Retention. Sourcewell IT logs systems and user activities on all Technology Resources. Security controls or other network elements may also produce logs, which are secured, retained, and disposed according to Sourcewell's Data Practices Policy, Data Inventory, and Records Retention Schedule. Logs are periodically reviewed to identify any activities that may indicate a security incident.

4.1.8 Physical Security. Sourcewell IT uses physical safeguards to avoid theft, intrusions, unauthorized use, or other abuses of its Information Assets. Users must comply with Sourcewell's current physical security standards, which are outlined in more detail Sourcewell's Employee Handbook.

4.1.9 Disaster Preparedness (Business Continuity and Disaster Recovery). Sourcewell IT has implemented and periodically tests its disaster preparedness plans, which support continuity of operations and systems availability if a disaster or other unplanned business impacting event occurs. System administrators perform regular data backups for the information assets they maintain. Backup strategies balance the business criticality of the data, the resources required, any impact to Users and Technology Resources. Sourcewell IT also documents and periodically tests data and systems restoration procedures.

4.2 Managing Information Assets. Sourcewell IT must approve and manage all additions and changes to Sourcewell's production IT environment to avoid unexpected business impacts. Sourcewell IT also ensures that its development environments comply with this Policy and current IT standards to minimize information security risks.

4.2.1 Procurement. Only Sourcewell IT or those authorized by the Information Security Coordinator may procure Technology Resources for use in or connection to Sourcewell's network. Any such procurement must comply with Sourcewell's Procurement Policy. These requirements apply regardless of whether the Resource is purchased, open source, or made available to Sourcewell at no cost. Sourcewell IT and Legal must be consulted early in the procurement process to ensure that legal and information security risks are identified and managed prior to implementation. This is particularly true with respect to any cloud computing service providers that are intended to access, store, or manage Government Information; document sharing services; and other internet-based service providers that will collect, create, store, or otherwise manage Government Data on behalf of Sourcewell.

4.2.2 Asset Management. Sourcewell IT is responsible for tracking and documenting all Technology Resources. Inventory tracking must include operating system levels and all installed software and software versions to support vulnerability identification and mitigation. All Government Data is assigned a data owner who is responsible for tracking the location, use, disposal, and disposal of the data under their control.

4.2.3 Authorized Environments and Authorities. Only authorized IT personnel may install and connect hardware or software in Sourcewell's IT environment. Users are prohibited from converting end-user computers to servers or other shared resources without assistance from IT. Sourcewell IT will limit administrative or privileged systems access to those individuals with a business need to know. Administrative access and related information must be distributed to more than one individual to minimize risks. The Information Security Coordinator must review and approval any new or modified internet connections or internet-facing environments prior to deployment.

4.2.4 Change Management. Sourcewell IT maintains a change management process to minimize business impact and disruption to its production IT environment. Users must submit change requests to Sourcewell IT and include an action plan with assigned roles and responsibilities, implementation milestones, testing procedures, and a rollback plan if the change fails. Sourcewell IT will track identified problems, fixes, and releases during software development and will include code archiving or versioning tools to ensure earlier versions can be recovered and rebuilt, if needed.

4.2.5 Application and Software Development

A. To avoid any undue or unexpected impact to Sourcewell's production IT environment, applications and other software development and testing must take place in reasonably segmented environments with segregation of duties between development and operations. Developers may be granted limited access to production environments where personnel and expertise availability is limited, but only for specific troubleshooting or support purposes.

- B. Security by design principles must be used to identify potential information security risks and resolve them early in the development process. Project team members must seek guidance from the Sourcewell IT team, Information Security Coordinator, critical vendors, industry experts, and industry best practices to identify and avoid application-level security risks. Defensive coding techniques, regular code reviews, and application-level scanning may also be used to identify and remediate any information security issues before release.

Article V: Incident Reporting and Response

5.1 Definitions.

"Breach of the security of the data" means the unauthorized acquisition, access, use, or disclosure of Government Data maintained Sourcewell.

"Contact information" means name and mailing address or e-mail address for the data subject.

"Unauthorized acquisition" means that a person has obtained, accessed, or viewed Government Data without the informed consent of the data subject or statutory authority with the intent to use the data for nongovernmental purposes.

"Unauthorized person" means any person who accesses Government Data without a work assignment that reasonably requires access or, regardless of the person's work assignment, for a purpose not otherwise permitted under the MGDPA.

5.2 Notice to Individuals and Investigation Report.

5.2.1 Notice of Breach.

- A. Government Data. As quickly as possible upon discovery of a breach of Government Data, Sourcewell must provide written notice to any individual who is the subject of the data or whose data was, or is reasonably believed to have been, acquired by an unauthorized person. The notice may not be unreasonably delayed consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the security of the data. Notice of breach must inform the individual that an investigation report will be prepared; how the individual may obtain the report; and that the individual may request delivery of the report by mail or e-mail.
- B. Protected Health Information. If the breach involves Protected Health Information, notice of breach must be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the incident. Notice regarding breach of PHI must include:
 - 1. The date of the breach and of when it was discovered, if known;
 - 2. The types of PHI that were involved in the breach;

3. Any steps individuals should take to protect themselves from potential harm resulting from the breach
4. A brief description of what Sourcewell is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
5. Contact procedures for individuals to ask questions or obtain additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address

5.2.2 Investigative Report. Upon completion of an investigation into any breach in the security of data and final disposition of any disciplinary action, including exhaustion of all rights of appeal under any applicable collective bargaining agreement, Sourcewell must prepare a report on the facts and results of the investigation. If the breach involves unauthorized access to or acquisition of data by an employee, contractor, or agent of Sourcewell, the report must at a minimum include:

- A. A description of the type of data that were accessed or acquired
- B. The number of individuals whose data was accessed or acquired; and
- C. If there has been final disposition of disciplinary action, the name of each employee determined to be responsible for the unauthorized access or acquisition.

5.2.3 Security Assessments. At least annually, Sourcewell IT will conduct a comprehensive security assessment of any personal information maintained by Sourcewell.

Article VI: Third Party Service Providers

The Information Security Coordinator is responsible for tracking, evaluating, and overseeing third-party service providers that interact with Sourcewell's Technology Resources.

- 6.1 Service Provider Approval Required. Users must obtain approval from Legal and the Information Security Coordinator before engaging a service provider to perform functions that involve access to Sourcewell's Technology Resources.
- 6.2 Contract Obligations. Service providers that access Sourcewell's Technology Resources must agree by contract to comply with applicable laws and these Policies. Sourcewell may require service providers to demonstrate their compliance by submitting to independent audits or other forms of review or certification based on risks.

Article VII. Risk and Compliance Management

Sourcewell supports a risk management cycle to enforce these Policies and to identify information security risks; to develop standards, procedures, safeguards, and controls; and to verify that safeguards and controls are working properly. This includes, but is not limited to, the following:

- 7.1 Risk Assessment and Analysis. The Information Security Coordinator conducts periodic assessments to identify information security risks across Sourcewell's IT environment, including application software, databases, operating systems, servers, other network components, and other connected devices. Assessment activities may include analyses, audits, reviews, scans, and penetration testing. **Users are prohibited from taking any actions to avoid, impact, or otherwise impede risk assessments.**
- 7.2 Remediation and Mitigation Plans. The Information Security Coordinator maintains and oversees remediation and mitigation plans to address any findings resulting from a risk assessment.
- 7.3 Vulnerability Management and Disclosure.
 - 7.3.1 External Discovery and Management. Manufacturers, security researchers, and other external sources may identify security vulnerabilities in hardware, software, and other equipment, and notify impacted organizations and individuals. In most cases, the manufacturer or developer will provide a patch or fix to remediate the vulnerability.
 - 7.3.2 Internal Management. The Information Security Coordinator also maintains a process to identify and track applicable vulnerabilities, scan devices for current patch status, and notify system administrators and other impacted parties. Users must cooperate with necessary updates and make all Sourcewell-owned devices available to IT for timely patching and related activities, as requested.
- 7.4 Compliance Management. The Information Security Coordinator maintains responsibility for enforcing these Policies. If The Coordinator suspects a User may have acted in violation of these Policies, the Information Security Coordinator may contact the User to resolve the issue.

Information Security Program Policy

Contents

Purpose	2
Scope	2
Roles and responsibilities	2
Information Security Policy	4
Access Control (NIST AC 3.1)	4
Awareness and Training (NIST AT 3.2)	5
Audit and Accountability (NIST AU 3.3)	6
Configuration Management (NIST CM 3.4)	6
Identification and Authentication (NIST IA 3.5)	7
Incident Response (NIST IR 3.6)	7
Maintenance (NIST MA 3.7)	8
Media Protection (NIST MP 3.8)	8
Personnel Security (NIST PS 3.9)	8
Physical Protection (NIST PE 3.10)	9
Risk Assessment (NIST RA 3.11)	9
Security Assessment and Monitoring (NIST CA 3.12)	9
Systems and Communication Protection (NIST SC 3.13)	10
Systems and Information Integrity (NIST SI 3.14)	10
Planning (NIST PL 3.15)	10
Systems and Services Acquisition (NIST SA 3.16)	11
Supply Chain Risk Management (NIST SR 3.17)	11
Data Compliance Policy	11
Acceptable Use Policy	12
Exceptions	14
Revision History	Error! Bookmark not defined.

Purpose

The purpose of this Information Security Program Policy (the “Policy”) is to define Sourcewell’s mandatory minimum information security requirements. These requirements may be exceeded, as needed, based on Sourcewell’s business needs and specific legal and federal requirements. However, all Sourcewell information technology assets and systems must, at a minimum, achieve the security levels required herein.

This Policy acts as an umbrella document for all information security policies and associated standards and controls, which are documented in Sourcewell’s Information Security Program.

This Policy and Sourcewell’s Information Security Program work together to:

- Protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets;
- Manage the risk of security exposure or compromise;
- Assure a secure and stable information technology (IT) environment;
- Identify and respond to events involving information asset misuse, loss, or unauthorized disclosure;
- Monitor systems for anomalies that might indicate compromise; and
- Promote and increase the awareness of information security

Scope

This Policy encompasses all Sourcewell systems, automated and manual, including systems managed or hosted by third parties for or on behalf of Sourcewell. It addresses all information, regardless of the form or format, which is created or used in support of any Sourcewell business activity.

This Policy applies to staff (full-time, part-time), interns, consultants, contractors, and board members who may purchase, configure, develop, operate, use, or maintain Sourcewell’s information security systems and technology resources to provide services to the organization, including all onsite hardware and software and cloud solutions.

Roles and responsibilities

Senior Leadership Team (“SLT”) and the Sourcewell Board of Directors are responsible for:

- Providing clear direction and consideration of security controls in the data processing infrastructure and computing networks;
- Providing resources to maintain information security controls consistent with this Policy;
- Implementing business continuity and disaster recovery plans;
- Evaluating and accepting risk on behalf of Sourcewell;
- Identifying information security responsibilities and goals and integrating them into relevant processes;
- Supporting the consistent implementation of information security policies and standards;
- Supporting security through clear direction and demonstrated commitment of appropriate resources;
- Promoting awareness of information security best practices through the regular dissemination of materials provided by the Information Security Coordinator (“ISC”);

- Determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of data and information;
- Participating in the response to security incidents;
- Complying with notification requirements in the event of a security incident or breach of information and data;
- Adhering to specific legal and regulatory requirements related to information security;
- Communicating legal and regulatory requirements to the ISC or designated representatives; and
- Communicating this Policy and associated standards, controls, and the consequences of non-compliance to the workforce and third parties.

Information Technology Officer (“ITO”) is responsible for:

- Providing in-house expertise, as needed;
- Developing and supporting the information security program and strategy, including measures of effectiveness;
- Establishing and maintaining information security policy and standards;
- Assessing compliance with security policies and standards;
- Advising IT leadership on secure system engineering and software development;
- Providing incident response coordination and expertise;
- Maintaining ongoing contact with relevant information security groups/associations and authorities;
- Providing SLT with timely notification of current threats and vulnerabilities;
- Providing information security awareness materials and training resources;
- Identifying and implementing all processes, policies, and controls relative to security requirements defined by Sourcewell and this Policy;
- Implementing the proper controls based on the information classification and categorization;
- Implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization; and
- Fostering staff participation in protecting information assets and in identifying, selecting, and implementing appropriate and cost-effective security controls and procedures.

Information Security Coordinator (“ISC”)/Director of IT Systems and Services is responsible for:

- Maintaining an appropriate level of current knowledge and proficiency in information security through professional development hours related to information security;
- Maintaining familiarity with business functions and requirements;
- Assessing compliance with information security policies, legal, and regulatory requirements;
- Evaluating and understanding information security risks and how to appropriately manage them;
- Representing and assuring security architecture considerations are addressed;
- Advising ITO on security issues related to procurement of products and services;
- Escalating security concerns according to applicable reporting and escalation procedures;
- Disseminating threat information to appropriate parties;
- Monitoring external sources for indications of data breaches, defacements, etc.;
- Participating in the response to and handling of security incidents;
- Providing training on secure operations to appropriate technical staff;

- Participating in the development of Sourcewell's policies and standards; and
- Promoting information security awareness.

IT leadership is responsible for:

- Providing clear direction and consideration of security controls in the data processing infrastructure and computing networks;
- Providing resources to maintain information security control consistent with this Policy;
- Identifying and implementing processes, policies, and controls relative to information security requirements defined by Sourcewell and this Policy;
- Providing training on secure operations to appropriate technical staff;
- Fostering staff participation in protecting information assets and in identifying, selecting, and implementing appropriate and cost-effective security controls and procedures; and
- Implementing approved business continuity and disaster recovery plans.

Workforce staff are responsible for:

- Understanding baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted to them;
- Protecting information and resources from unauthorized use or disclosure;
- Protecting sensitive information from unauthorized use or disclosure;
- Abiding by Acceptable Use of Information Technology Resources Policy below;
- Monitoring systems and networks for anomalies;
- Implementing the proper controls for information based on the classification designations; and
- Reporting suspected information security incidents or weaknesses to the ISC.

Information Security Policy

It is Sourcewell's policy to implement information security standards and controls in conformance with the most recent version of NIST Special Publication 800-171 or an alternate publication defining similarly robust levels of information security. Any attempt to override or evade the requirements outlined below constitutes a violation of this Policy.

Access Control (NIST AC 3.1)

Sourcewell shall implement and maintain access controls and enforcement standards and processes as follows:

- a. Define and document the types of system accounts allowed and prohibited;
- b. Create, enable, modify, and remove system accounts in accordance with established procedures, prerequisites, and criteria;
- c. Authorize system users, group, and role memberships, and access privileges for each;
- d. Authorize access to systems based on access authorization and intended system use;
- e. Conduct routine monitoring of system accounts;
- f. Disable users, group, and role membership accounts when:
 - i. Account has expired;
 - ii. Account has been inactive for 90 days;
 - iii. Account is no longer associated with a user or individual;
 - iv. Account is in violation of Sourcewell policy; and
 - v. Significant risks associated with account user/owner are discovered;

- g. Ensure account owners, supervisors, and other personnel use the IT ticketing process to notify IT:
 - i. When user accounts are no longer required;
 - ii. When users are terminated or transferred; and
 - iii. When system usage or the need-to-know changes for the user;
- h. Force user reauthentication after 30 minutes of user inactivity;
- i. Require authorization for logical access to information and technology resources;
- j. Limit authorized access to only those privileges necessary to accomplish assigned tasks;
- k. Review and update user and system account privileges on an annual basis;
- l. Restrict privileged access rights to IT staff assigned security responsibilities and tasks;
- m. Require IT staff assigned privileged access rights to use non-privileged account access when performing non-security related tasks;
- n. Prohibit non-privileged user accounts from executing privileged functions;
- o. Log execution of all privileged functions;
- p. Limit consecutive invalid logon attempts and automate controls when threshold is exceeded;
- q. Establish and document usage restrictions, configuration requirements, and connection requirements for authorized remote access to technology resources;
- r. Use authorized and managed access control mechanisms for all remote access connections;
- s. Establish and document usage restrictions, configuration requirements, and connection requirements wireless access to technology resources;
- t. Disable wireless networking capabilities when not intended for use and prior to deployment;
- u. Require authentication and encryption for all wireless access to technology resources;
- v. Establish and document usage restrictions, configuration requirements, and connection requirements for mobile devices;
- w. Require authorization for use and connection of mobile devices to technology resources;
- x. Require full-device or container-based encryption for mobile devices used to access Sourcewell information; and
- y. Prohibit use of external systems to access technology resources or process or to store or transmit Sourcewell information, unless specifically authorized.

Awareness and Training (NIST AT 3.2)

Sourcewell shall implement an information security awareness and training program as follows:

- a. Provide security literacy training to system users:
 - i. As part of initial training for new users and annually thereafter;
 - ii. Following a significant change in systems or operational procedures; and
 - iii. On recognizing and reporting of insider threat, social engineering, and social mining;
- b. Review and update security literacy training content as needed based on new organizational policies, procedures, and standards and following significant changes to systems;
- c. Provide role-based security training to personnel:
 - i. Before authorizing access to systems or information, before performing assigned duties, and annually thereafter; and
 - ii. When required by system changes and following significant changes in organizational policies, procedures, and standards; and
- d. Review and update role-based training content annually and as needed based on new organizational policies, procedures, and standards or significant system changes.

Audit and Accountability (NIST AU 3.3)

Sourcewell shall implement and maintain audit and accountability management standards and processes as follows:

- a. Retain audit log records for 6 months;
- b. Generate audit log records which contain information as outlined below;
 - i. Type of event that occurred;
 - ii. When and where event occurred;
 - iii. Sources and outcomes of event;
 - iv. Identity of the individuals, subjects, objects, or entities associated with event; and
 - v. Provide additional information for audit log records, as needed;
- c. Review and update event types captured on an annual basis;
- d. Alert systems engineers immediately in the event of audit logging process failure;
- e. Review and analyze system audit records monthly for indications of inappropriate or unusual activity;
- f. Report inappropriate and unusual activity to ISC;
- g. Document audit log time stamp source of truth and configure systems to synchronize with it using Coordinated Universal Time (UTC) format;
- h. Correlate audit logs across different systems for wide situational awareness;
- i. Preserve original content and time stamps of audit log records;
- j. Protect audit logs and audit logging tools from unauthorized access, modification, and deletion; and
- k. Restrict access to management of audit logging functionality to privileged users and system engineers.

Configuration Management (NIST CM 3.4)

Sourcewell shall implement and maintain configuration management standards and processes as follows:

- a. Document and implement baseline configuration settings for all systems;
- b. Review, update, and document system configuration setting on an annual basis, and when system components are installed or modified;
- c. Restrict configuration settings to least functionality necessary to meet operational requirements;
- d. Document and approve deviations and exceptions to established configuration settings;
- e. Review, approve/disapprove, and document configuration setting changes with explicit consideration for security impacts;
- f. Test and verify configuration setting changes provide only secure, mission-essential capabilities;
- g. Identify and document prohibited and restricted system functions, ports, protocols, connections, and services;
- h. Review and validate system configuration settings annually to identify unnecessary and nonsecure functions, ports, protocols, connections, and services;
- i. Document software programs authorized for use and review/update on an annual basis;
- j. Implement, deny-all allow-by-exception, configuration setting policies for the execution of authorized software programs on systems;
- k. Document and maintain system component inventories including physical location, hardware, software, and firmware versions;
- l. Review and update the system component inventories on an annual basis;
- m. Identify and document the location of information and the system components on which the information is processed and stored; and

- n. Document and manage system configurations and procedures used for systems and devices used in high-risk areas and/or travel locations.

Identification and Authentication (NIST IA 3.5)

Sourcewell shall implement and maintain identification and authentication standards and processes as follows:

- a. Assign and use unique identifiers for all individual, groups, role, service, and device accounts and associate unique identifiers with processes acting on behalf of these accounts;
- b. Prevent the reuse of unique identifiers for six (6) months;
- c. Authenticate all individual, groups, role, service, and device accounts before establishing connections to technology resources;
- d. Re-authenticate users and systems when sessions time-out or disconnect intentionally or un-intentionally;
- e. Require authentication prior to execution of privileged functions for privileged user accounts;
- f. Require forced reauthentication for privileged and non-privileged accounts at least every 12 hours;
- g. Use of multifactor authentication (MFA) technologies for privileged and non-privileged accounts wherever operationally possible;
- h. Use replay-resistant authentication, such as challenge-response and one-time authenticators, as operationally appropriate;
- i. Cryptographically protect authenticators, such as passwords/passphrases, while stored and in transit;
- j. Document and manage process for lost, compromised, and revoked authenticators;
- k. Obscure authentication feedback displayed by systems to prevent authentication information from appearing in plain readable text;
- l. Force new password/passphrase change upon first use and after account recovery; and
- m. Enforce composition and complexity rules for passwords/passphrases.

Incident Response (NIST IR 3.6)

Sourcewell shall implement and maintain incident response standards and processes as follows:

- a. Implement incident-handling capabilities that are consistent with the incident response plan to include preparation, detection and analysis, containment, eradication, and recovery;
- b. Document roles and responsibilities for all staff members assigned incident-handling duties;
- c. Provide resources and methods to document and track all information security incidents;
- d. Require staff to report all suspected incidents to their supervisor and the ISC immediately;
- e. Provide for incident response training on an annual basis for staff based on assigned roles and responsibilities;
- f. Provide for training within 30 days for all staff assuming incident handling roles or responsibilities;
- g. Provide for training on an annual basis for all staff with incident handling roles or responsibilities;
- h. Test the effectiveness of the incident response capability on an annual basis;
- i. Review, and update as appropriate, incident response training content annually and following incidents;
- j. Document and define reportable incidents and address incident information handling and sharing;
- k. Designate and document responsibilities of organizational entities, personnel, or roles;

- l. Distribute copies of the incident response plan to incident-handling personnel;
- m. Review, and update as appropriate, incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing; and
- n. Protect the incident response plan from unauthorized disclosure.

Maintenance (NIST MA 3.7)

Sourcewell shall implement and maintain system maintenance standards, processes, and tools as follows:

- a. Approve, control, and monitor the use of systems, devices, and tools used in system maintenance;
- b. Check media with diagnostic and test programs for malicious code before it is used;
- c. After use, verify there is no information on maintenance equipment by sanitizing or destroying the equipment, or retaining the equipment within the facility;
- d. Approve and monitor nonlocal maintenance and diagnostic activities;
- e. Implement multi-factor authentication and replay resistance for nonlocal maintenance and diagnostic sessions;
- f. Terminate session and network connections when nonlocal maintenance is completed;
- a. Implement a process for authorizing maintenance personnel;
- b. Maintain a list of authorized maintenance organizations or personnel;
- c. Verify that non-escorted personnel who perform maintenance systems possess the required access authorizations; and
- d. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorization.

Media Protection (NIST MP 3.8)

Sourcewell shall implement media protection standards and processes as follows:

- a. Physically control and securely store system media that contains Sourcewell information;
- b. Restrict access to information on media to authorized personnel or roles;
- c. Sanitize media that contain information prior to disposal, release out of Sourcewell control, or release for reuse;
- d. Mark media that contain information to indicate distribution limitations, handling caveats, and applicable information markings;
- e. Maintain accountability for media that contain information during transport outside of controlled areas;
- f. Document activities associated with the transport media that contain information;
- g. Prohibit the use of removable system media without an identifiable owner;
- h. Protect the confidentiality of backup information; and
- i. Implement cryptographic mechanisms for backup storage.

Personnel Security (NIST PS 3.9)

Sourcewell shall implement and maintain personnel security standards and processes as follows:

- a. Ensure procedures, standards, and guidelines include pre-employment screenings;
- b. When an individual's employment is terminated:
 - i. Disable credentials associated with the individual with eight (8) hours; and
 - ii. Retrieve organization-issued computing and security-related property; and

- c. When individuals are reassigned or transferred to another position in the organization:
 - i. Review ongoing operational need for current logical and physical access to the systems and facilities; and
 - ii. Modify access authorization to correspond with any changes in operational need.

Physical Protection (NIST PE 3.10)

Sourcewell shall implement and maintain standards and processes for physical protection as follows:

- a. Remove individuals from the access lists when access is no longer required;
- b. Monitor access and respond to physical security incidents;
- c. Escort visitors and control visitor activity;
- d. Secure keys, combinations, and other physical access devices;
- e. Issue unique credentials to individuals for physical access;
- f. Access to non-local systems, equipment, and their respective operating environments shall be controlled by leveraging the hosting vendors processes and procedures;
- g. Review and update lists of persons assigned approved physical access on an annual basis and when changes in assigned persons role or job duties are made;
- h. Monitor physical access to facilities, systems, equipment, and their respective operating environments and review access control system logs on a quarterly basis;
- i. Retain physical access control logs for a minimum of six (6) months from the date of creation;
- j. Ensure procedures, standards, and guidelines identify permitted alternate work sites; and
- k. Restrict and monitor physical access to facilities locations that house transmission and distribution lines and wiring.

Risk Assessment (NIST RA 3.11)

Sourcewell shall implement and maintain risk assessment processes and standards as follows:

- a. Assess the risk of systems and unauthorized disclosure of Sourcewell information processing, storage, or transmission processes and procedures;
- b. Perform risk assessments on an annual basis and when changes are made to system configurations and/or system boundaries;
- c. Monitor and scan systems for vulnerabilities on a routine basis and when new vulnerabilities are otherwise identified;
- d. Remediate system vulnerabilities within 60 days of being identified; and
- e. Document in a Risk Log all findings and remediation plans for risks identified in security assessments, monitoring, vulnerability scans, and audits.

Security Assessment and Monitoring (NIST CA 3.12)

Sourcewell shall implement and maintain processes and controls for security assessment and monitoring as follows:

- a. Perform and document security assessments on an annual basis and when changes are made to system configurations and/or system boundaries;
- b. Develop and document action plans to remediate weaknesses or deficiencies identified during security assessments, independent audits/reviews, and continuous monitoring activities;
- c. Implement continuous or ongoing monitoring processes and procedures for all applicable systems and operating environments; and
- d. Implement documented information exchange agreements when information is exchanged with entities and/or systems outside of organizational control.

Systems and Communication Protection (NIST SC 3.13)

Sourcewell shall implement and maintain processes and controls for systems and communication protection as follows:

- a. Use managed interfaces and connections to connect external systems;
- b. Control and monitor managed interfaces and connection;
- c. Require subnetworks for all publicly accessible system components which are physically or logically separated from system networks;
- d. Implement controls to prevent unauthorized and unintended information transfers in shared system resources;
- e. Use 'deny by default-allow by exception' for all network communication traffic;
- f. Implement cryptographic protections to protect information while in transit and while at rest;
- g. Terminate network communication connections upon session termination or after 60 minutes of inactivity;
- h. Maintain a list of approved types of cryptography and process and procedures for the creation and management of cryptographic keys;
- i. Prohibit remote activation of collaborative computing devices and applications such as whiteboards, microphones, and cameras;
- j. Maintain a list of approved mobile code and mobile code technologies; and
- k. Implement controls to protect session authenticity for all systems and network communications.

Systems and Information Integrity (NIST SI 3.14)

Sourcewell shall implement processes and controls for system and information integrity as follows:

- a. Identify, document, and correct system flaws;
- b. Install security-relevant software and firmware updates within 30 days of their release date;
- c. Implement approved malicious code protection mechanisms at all system entry and exit points;
 - i. Update malicious code protection mechanisms as new releases are available in accordance with configuration management policies and procedures;
 - ii. Configure malicious code protection mechanisms to perform routine scans of the system and real-time scans of files downloaded, opened, or executed; and
 - iii. Block malicious code, quarantine malicious code, or take other mitigation actions in response to malicious code detection;
- d. Require IT staff to review security alerts, advisories, and directives from manufacturers and other external organizations on an ongoing basis;
- e. Create and distribute internal security alerts, advisories, and directives as necessary;
- f. Monitor all systems, operating environments, and devices on an ongoing basis for unusual and unauthorized activities or conditions; and
- g. Process, transmit, and store all information in accordance with applicable laws, regulations, policies, standards, and guidelines.

Planning (NIST PL 3.15)

Sourcewell shall implement and maintain planning processes and controls as follows:

- a. Develop, document, and disseminate to organizational staff policies, standards, and procedures to satisfy the security requirements for the protection of Sourcewell information;
- b. Review and update policies, standards, and procedures on an annual basis;

- c. Review and update policies, standards, and procedures when significant changes are made to systems;
- d. Develop and document individual system security plans that:
 - i. Include system components, operating environment, connections to other systems, risk and threat matrix, and an overview of systems security requirements;
 - ii. Identify the information types processed, stored, and transmitted by the system;
 - iii. Establish rules describing the responsibilities and expected behavior for system usage and protecting protected information; and
 - iv. Protect the system security plans from unauthorized disclosure; and
- e. Require individuals to acknowledge that they have read, understand, and agree to abide by the rules of behavior before authorizing access to protected information and the system.

Systems and Services Acquisition (NIST SA 3.16)

Sourcewell shall implement and maintain processes and controls for systems and services acquisition as follows:

- a. Require acquisitions to include, but not be limited to, security capabilities, functions and mechanisms, and evidence from development and assessment activities;
- b. Require timely replacement of system components no longer supported by the developer, vendor, or manufacturer;
- c. Establish processes, procedures, and techniques for monitoring compliance with established security requirements for all external systems and services, including shared responsibilities with external providers;
- d. Provide options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced; and
- e. Require providers of external system services used for the processing, storage, or transmission of protected information to comply with established security requirements.

Supply Chain Risk Management (NIST SR 3.17)

Sourcewell shall implement and maintain processes and controls for supply chain risk management as follows:

- a. Include strategies for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services;
- b. Require annual review of supply chain risk management plans; and
- c. Implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.

Data Compliance Policy

Various information security laws, regulations, and industry standards apply to Sourcewell, and the data Sourcewell users collect, store, use, and disseminate. Sourcewell is committed to complying with applicable laws, regulations, and standards, which include, but are not limited to, the following:

1. Minnesota Government Data Practices Act (“MGDPA”). The MGDPA at Minnesota Statutes, Chapter 13, governs the collection, creation, storage, maintenance, and dissemination of data held by Minnesota governmental entities (“Government Data”), including Sourcewell. Sourcewell’s Data Practices Policy, Data Inventory, and Records Retention Schedule, which outlines its policies regarding the classification, disclosure, and disposition of Government

Data. The Data Practices Policy, Data Inventory, and Records Retention Schedule can be found under “Legal Policies” in the Board Policy Book.

2. Health Insurance Portability and Accountability Act (“HIPAA”). Sourcewell serves as the Sponsoring Association and provides administrative services for the Better Health Collective, a government joint risk pool for employee benefits. In that capacity, certain users have access to and use Protected Health Information (“PHI”) governed by HIPAA. Any entity, like Sourcewell, that conducts functions governed by HIPAA and other functions that are not may designate itself as a hybrid entity for HIPAA compliance purposes. Sourcewell has designated itself as a hybrid entity. The following documents Sourcewell’s intent to comply with the HIPAA and the HITECH Act applicable to this designation. The HIPAA Hybrid Entity Policy can be found under “Legal Policies” in the Board Policy Book.
3. Family Education Rights and Privacy Act (“FERPA”). Sourcewell serves as a third-party service provider to educational entities throughout the United States. In that capacity, certain Users have access to and use Personally Identifiable Information (“PII”) governed by the FERPA. FERPA requires Sourcewell to implement safeguards to protect this data. This Policy is intended to demonstrate Sourcewell’s compliance with these obligations.
4. Other State Laws. Statutes in some states outside Minnesota provide for additional statutory protections for student data beyond those provided for in FERPA. Sourcewell developed these Policies to include data protection required by FERPA and those common to most customers, including those in other states. As a result, when a customer asks Sourcewell to agree to additional customer-specific requirements:
 - a. Review and Approval. Sourcewell Legal and Information Security Coordinator must review all related documentation, including the customer’s information security policies or standards and any related agreements requiring Sourcewell to comply.
 - b. Compliance. If Sourcewell Legal and Information Security Coordinator agree that Sourcewell is willing and able to comply with customer-specific information security policies or standards, Information Security Coordinator shall be responsible for notifying affected users and ensuring they have the resources needed to comply with the additional requirements.

Acceptable Use Policy

Sourcewell provides employees and others with network resources and systems (“Technology Resources”) to support its business requirements and functions. This section describes Sourcewell’s policy with respect to the use of these Technology Resources and explains the steps Sourcewell employees and others with access to Sourcewell’s Technology Resources (“Users”) must take to protect them.

General Use of Information Technology Resources. Access to and use of Technology Resources is a privilege and not a right. Unacceptable use of Technology Resources may result in disciplinary action termination of employment. Users who violate local, state, or federal law may also be subject to civil or criminal prosecution.

1. Acceptable use includes all authorized access to, and use of Sourcewell’s Technology Resources as needed to fulfill a user’s assigned duties and functions. Minimal personal use is acceptable to the extent it does not interfere with the user’s performance of their responsibilities or impair other’s ability to theirs.
2. Unacceptable use includes all unauthorized access to and use of Sourcewell’s Technology Resources for purposes including, but not limited to:
 - a. Transmitting, receiving, or storing Government Data in violation of Source well’s Data Practices and Information Security Program Policy or other applicable state and federal privacy laws.

- b. Achieving personal gains or other activities that may create a real or perceived conflict of interest with Sourcewell.
- c. Creating undue security risks or negatively impacting the performance of Sourcewell's Technology Resources.
- d. Causing embarrassment, loss of reputation, or other harm to Sourcewell.
- e. Hacking, spoofing, or launching denial of service attacks.
- f. Gaining or attempting to gain unauthorized access to others' networks or systems.
- g. Sending fraudulent email messages.
- h. Distributing or attempting to distribute malicious software.
- i. Spying or attempting to install spyware or other unauthorized monitoring or surveillance tools.
- j. Committing acts such as terrorism, fraud, or identity theft.
- k. Downloading, storing, or distributing child pornography or other obscene or illegal materials.
- l. Violating another's intellectual property rights.
- m. Uploading, downloading, or disseminating defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene, or otherwise inappropriate or offensive messages or media.
- n. Distributing jokes, chain letters, commercial solicitations, or hoax emails or other mass messaging or spamming.
- o. Disrupting the workplace environment, creating a hostile workplace, or invading the privacy of others.
- p. Using encryption or other technologies to hide illegal, unethical, or otherwise inappropriate activities.
- q. Installing or distributing unlicensed or pirated software

No Expectation of Privacy and Monitoring

Except where applicable law provides otherwise, users have no expectation of privacy when using Sourcewell's Technology Resources, including, but not limited to, transmitting and storing files, data, and messages.

To enforce compliance with Sourcewell's policies and protect Sourcewell's interests, Sourcewell reserves the right to monitor any use of its network and systems to the extent permitted by applicable law. By using Sourcewell's systems, users agree to such monitoring. Monitoring may include (but is not necessarily limited to) intercepting and reviewing network traffic, emails, or other messages or data sent or received and inspecting data stored on individual file directories, hard disks, or other printed or online media.

Desktop, Laptop, and End-User Controls

Users may only access Sourcewell's Technology Resources using Sourcewell-provided user accounts on approved devices that support Sourcewell's current minimum information security standards.

Social Media

Users must comply with Sourcewell's social media Policy, found in the Board Policy Book, when using their personal social media accounts to interact with Sourcewell's official Social Media sites or to engage in other activities related to Sourcewell and its programs or services.

Mobile Devices and Bring Your Own Device to Work

Any use of personnel mobile devices, including laptops, smartphones, and tablet computers, to connect to Sourcewell's Technology Resources must be approved in advance by Sourcewell IT. If Sourcewell IT permits any User to use their own device for this purpose, the User must agree to use such devices subject to this Policy and any additional policies, procedures, standards, and processes Sourcewell implements. Further:

1. Sourcewell may require the user to install specific security controls on the device, including device management software, access controls, encryption, and remote wiping capabilities.
2. The user must allow Sourcewell IT to review the device and remove any Government Data, if their relationship with Sourcewell terminates, the user changes devices or services, and in other similar situations. The user must also promptly provide Sourcewell IT with access to the device when requested for Sourcewell's legitimate business purposes.
3. Devices with access to Sourcewell email or other Technology Resources must be protected by password/passphrase or another approved authentication method. Such devices must be physically secured by the user.
4. The User is prohibited from connecting a mobile device containing Government Data to any unsecured network without technology security controls in place. Unsecured networks include home networks, hotel networks, open or for-pay wireless hotspots, convention networks, or any other network that Sourcewell has not approved or does not control.

Remote Access

Sourcewell IT has implemented technology solutions and controls which provide users with remote access capabilities to approved Technology Resources. Users with remote access privileges may only use Sourcewell-provided means and multifactor authentication to access Sourcewell's Technology Resources. Users are prohibited from installing or setting up any other remote connections, including remote desktop software. Remote access connections to Sourcewell Technology Resources must be configured to time out or be disconnected as prescribed in existing information technology and information security standards and related standard operation procedures.

External Network Connections

Sourcewell IT must review and approve all extranet and other connections to Sourcewell's Technology Resources before implementation. A signed business agreement between Sourcewell and any organization seeking access must accompany any request for extranet connection. Connectivity will be limited to only those assets required to perform the specified functions. Extranet connections will be monitored and may be deactivated if unusual or inappropriate traffic is detected.

Wireless Network Connections

Users are prohibited from connecting any wireless access points, routers, or other similar devices to Sourcewell Technology Resources or trusted network without prior written approval from Sourcewell IT.

Exceptions

Sourcewell recognizes that specific business needs and local situations may occasionally call for an exception to this Policy. Exception requests must be made in writing and submitted to the

Information Security Coordinator and IT using the IT ticketing processes. The Information Security Coordinator must approve in writing, documenting the exception, and periodically review all exceptions.

Do not assume that the Information Security Coordinator will approve an exception simply because they have previously approved a similar exception. Each non-compliant situation requires a review of the specific facts and risks to Sourcewell's Technology Resources.

To request an exception, contact the Information Security Coordinator using existing IT ticket/request processes.