Data Security Classification Policy

Policy Statement

To protect the security and integrity of Sourcewell Technology (“SWT”) data, and comply with the Minnesota Government Data Practices Act ("MGDPA"), Chapter 13 of the Minnesota Statutes, SWT data must be classified appropriately. SWT uses data security classification and security level to ensure all data and the systems on which it is stored, accessed, transmitted, or have the ability to impact the security of the data have appropriate security controls to protect the confidentiality, integrity and availability of the data.

SWT’s adoption of this policy satisfies the requirement set forth in Minn.Stat. §13.05, subd. 5 to establish procedures to ensure appropriate access to not public data. SWT limits employees' access to not public data whose work assignment reasonably requires access, or who have a legitimate need to know, and to other entities or individuals authorized by law.

Data Inventory

Under the requirement set forth in Minn.Stat. §13.025, subd. 1, SWT has prepared a Data Inventory available at http://sourcewelltech.org which identifies and describes all not public data on individuals and not individuals maintained by SWT. To comply with Minn.Stat. §13.05, subd. 5, the Data Inventory identifies SWT employees who have access to not public data. In the event of a temporary duty assignment by a manager or supervisor, an employee may access not public data for as long as the work is assigned to the employee.

In addition to the employees listed in the Data Inventory, the following employees have access to not public data as necessary for their duties: Managing Director, Chief Operating Officer, Chief Technology Officer, Chief Legal Officer, Human Resources Director, Responsible Authority and Data Practices Compliance Official, Data Practices Compliance Official, Principal Security Architect/Principal Enterprise Architect, CISSP®, and Designee(s).

Employee position descriptions

Position descriptions may include provisions identifying any not public data accessible to the employee when a work assignment reasonably requires access.

Data sharing with authorized entities or individuals

State or federal law may authorize the sharing of not public data in specific circumstances. Not public data may be shared with another entity if state or federal law allows or mandates it. Individuals will be provided with Tennessen warnings as required under Minn.Stat. §13.04, subd. 2 in accordance with the nature of any

data request. Any sharing of not public data will be strictly limited to the data necessary or required to comply with applicable law.

Ensuring that Not Public data is not accessed

SWT ensures that not public data is accessed only by employees as necessary for their job responsibilities by following the procedures set forth in the separate Data Classification & Control Policy adopted on August 26, 2009.

Penalties for unlawfully accessing Not Public data

SWT will utilize the penalties for unlawful access to not public data as set forth in Minn.Stat. §13.09 if necessary. Penalties include suspension, termination and/or referring the matter to the appropriate prosecutorial authority who may pursue a criminal misdemeanor charge.

Data Classification

SWT data security classifications are:

Confidential (individuals) or Protected Nonpublic (not on individuals) - This classification includes data that is not public and is not accessible to the data subject. It is available to SWT employees with a legitimate need to know, or whose work assignments reasonably require access, and other entities or individuals authorized by law.

Private (individuals) or Nonpublic (not on individuals) - This classification includes data that is not public and is accessible to the data subject, and to SWT employees with a legitimate need to know, or whose work assignments reasonably require access, and other entities or individuals authorized by law.

Public - This classification includes data that is accessible by anyone for any reason.

Questions

Questions regarding this policy should be directed to either the:

Responsible Authority and Data Practices Compliance Official

Corey Tramm, Chief Technology Officer

1667 Snelling Ave. N.

St. Paul, MN 55108

Direct: 651-999-6502

Email: corey.tramm@sourcewelltech.org

-- or to:

Data Practices Compliance Official

Susan Mussell, Chief Legal Officer

1667 Snelling Ave. N.

St. Paul, MN 55108

Direct: 651-999-6216

Email: susan.mussell@sourcewelltech.org