Policy ☒ Procedure ☒ Guideline ☐

TYPE: University All

TITLE: Ensuring Security of Not Public Data

ORIGINALLY APPROVED: 4/1/15

CURRENT VERSION EFFECTIVE: 4/1/15

RESPONSIBLE UNIVERSITY OFFICER: President

OWNER: Data Practices Compliance Official (DPCO)

CONTACT: Data Practices Compliance Official (DPCO)

REASON FOR POLICY:

The adoption of this policy by St. Cloud State University satisfies the requirement in Minnesota Statutes, section 13.05, subd. 5, to establish procedures ensuring appropriate access to not public data. By incorporating employee access to not public data in SCSU's Data Inventory (required by Minnesota Statutes, section 13.025, subd. 1), in the individual employee's position description, or both, SCSU's policy limits access to not public data to employees whose work assignment reasonably requires access.

Many federal and state laws regulate the collection, handling and disclosure of University data, including the Family Rights to Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, the Minnesota Government Data Practices Act, and Payment Card Industry regulations. Exposure of confidential data through improper disclosure or security risk is a violation of these laws, and can result in the institution's incurring legal liability, financial liability, loss of reputation, and loss of trust. In addition, Minnesota law requires all state entities to notify individuals if there is a security breach involving their protected data.

The use of mobile computing devices (e.g., laptops, PDAs, cell phones, USB drives) increases the vulnerability of university electronic data to theft and unauthorized disclosure and mandates additional requirements for securing non-public data as set forth in MnSCU Policy 5.22 and 5.23 and associated procedures and guidelines.

POLICY:

This policy defines the data management environment and assigned roles and responsibilities for protecting St. Cloud State University's non-public information from unauthorized access, disclosure, or misuse. It is the responsibility of every University employee who accesses non- public data and information to secure and protect that data. It is the responsibility of every University employee who is responsible for potential data breach to cooperate with the Data Practice Compliance Official to notify individuals whose data may have been exposed.

PROCEDURE:

Data Inventory

Under the requirement in Minnesota Statutes, section 13.025, subd. 1, SCSU has prepared a Data Inventory which identifies and describes all not public data on individuals maintained by SCSU. To comply with the requirement in section 13.05, subd. 5, SCSU has also modified its Data Inventory to identify the employees who have access to not public data.

In the event of a temporary duty as assigned by a manager or supervisor, an employee may access certain not public data, for as long as the work is assigned to the employee.

In addition to the employees listed in SCSU's Data Inventory, the Responsible Authority, the Data Practices Compliance Official (DPCO), SCSU Administrators, and MnSCU staff to include the General Counsel and Attorney General, may have access to all not public data maintained by SCSU if necessary for specified duties. Any access to not public data will be strictly limited to the data necessary to complete the work assignment.

Employee Position Descriptions

Position descriptions may contain 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 a federal or state law allows or mandates it. Individuals will have notice of any sharing in applicable Tennessen warnings (*see* Minnesota Statutes, section 13.04) or SCSU will obtain the individual's informed consent. Any sharing of not public data will be strictly limited to the data necessary or required to comply with the applicable law.

Ensuring That Not Public Data Are Not Accessed Without a Work Assignment

Within SCSU, divisions may assign tasks by employee or by job classification. If a division maintains not public data and not all employees within its division have a work assignment allowing access to the data, the division will ensure that the not public data are secure. This policy also applies to divisions that share workspaces with other divisions within SCSU where not public data are maintained.

Recommended actions for ensuring appropriate access include:

- Assigning appropriate security roles, limiting access to appropriate shared network drives, and implementing password protections for not public electronic data
- Password protecting employee computers and locking computers before leaving workstations
- Securing not public data within locked work spaces and in locked file cabinets
- Shredding not public documents before disposing of them

Penalties for Unlawfully Accessing Not Public Data

SCSU will utilize the penalties for unlawful access to not public data as provided for in Minnesota Statutes, section 13.09, if necessary. Penalties include suspension, dismissal, or referring the matter to the appropriate prosecutorial authority who may pursue a criminal misdemeanor charge.

RELATED DOCUMENTS: Minn. Statute 13; MnSCU Policy 5.22 (and associated Procedures); MnSCU Policy 5.23 (and associated guidelines); Not Public Data Inventory

Questions regarding this policy should be directed to SCSU's Data Practices Compliance Official (DPCO):

Judith Siminoe
200 Administrative Services
St. Cloud State University
jpsiminoe@stcloudstate.edu