Guideline 5.23.1.4 Information Security Incident Response

Part 1. Purpose. This guideline establishes the minimum requirements for Information Security Incident Response within Minnesota State Colleges and Universities (system). Information Security Incident Response controls and minimizes the impact of an information security incident by establishing a process to report and address the incident.

Part 2. Applicability. This guideline applies to all system information resources, and to all uses of those resources. This guideline establishes minimum requirements for incident response. Institutions may adopt additional requirements, consistent with this guideline and board policy 5.23.

Part 3. Guidelines.

Subpart A. Each system college, university and the system office shall adopt an Incident Response Plan addressing the requirements set out in this guideline. Incident Response Plans shall include reasonable and appropriate methods to control and remediate information security incidents affecting critical information technology resources that are controlled by an institution.

Subpart B. Information Security Incident Definition. An information security incident for the purposes of this guideline means a situation that presents a significant or imminent threat to the security of system information technology resources or information resources; it includes, but is not limited to the following:

1. Unauthorized access or compromise of information resources or information technology resources with perceived malicious intent;
2. A significant threat or actual loss of not-public data via information technology resources;
3. A reasonable basis to believe that system information technology resources are being used for criminal activity.

Subpart C. Plan Components. The Incident Response Plan should include appropriate procedures to address the issues outlined below for security incidents.

1. **Detection and Reporting.** The method(s) of detecting and reporting an incident should be identified, as well as the path of information flows.
2. **Initial Classification and Notification.** Each incident should be evaluated to ensure it is handled with the appropriate urgency, and the correct individuals are notified for the type of incident being investigated. External processes may be initiated when necessary.
3. **Containment.** Initial steps to immediately stop the spread of the incident.
4. **Eradication.** Steps taken to remove the cause of the incident.

5. **Recovery.** Steps taken to return the computer systems to a full production mode.
6. **Incident Closure.** Complete all documentation and review the incident to determine how the systems, processes, or incident response plan could be improved to prevent recurrence in the future, or decrease recovery time.

Subpart D. Team Composition. Incident response teams should be prepared for a variety of security incidents, and include members who can provide expert advice for potential needs. Team members will be activated as necessary depending on the nature of the incident, and external resources may be used to fulfill some roles. The resources outlined below must be identified in the plan.

1. **Incident Handler.** The individual, versed in the applicable Incident Response Plan, who is designated as responsible for implementing the plan, activating team members as necessary, coordinating communications, and keeping administration informed of developments as necessary and appropriate.
2. **Technical Contacts.** Individuals familiar with the applicable computing environment, and who have the knowledge and access necessary to make any required changes to the systems or network.
3. **Office of the General Counsel.** Per the Breach Notification Standard/Guideline, must be consulted in any incident in which non-public data has or is reasonably believed to have been compromised, and also should be consulted in cases involving alleged criminal activity, child pornography, or investigations focusing on an individual.
4. **Information Security Office.** The ISO within the system office may be included any time additional assistance is desired to handle a security incident and should be included for incidents in which General Counsel is involved.
5. **Public Affairs Offices.** May be required in the event of a significant breach of security, if internal systems are not available, or the public web site is affected. Public Affairs shall be consulted before any statement is provided to the media about a system security incident.
6. **Human Resources Offices.** Assist in coordinating communications with and investigations of employees who may be affected by a security incident either as victims or having alleged involvement in the incident;
7. **Labor Relations.** Assists human resources office in relations between the incident response team and represented employees who may be affected by an investigation.
8. **Internal Audit.** May be required in cases involving potential criminal conduct, violations of code of ethics, misuse of state resources, or other instances that may lead to fraud charges.
9. **Local Campus Authority.** As defined by the Breach Notification Standard, the LCA must be notified in any case in which non-public data is believed to have been breached.
10. **Institution Finance Department.** Must be notified when the security incident involves PCI Data or other financial information, and is responsible for immediately notifying the card brands.
11. **Institution Academic and Student Affairs Offices.** May assist if the security incident involves academic or education records or the incident affects faculty or students.

12. **Forensics.** System or external experts who may assist with technical investigation procedures that may be necessary to handle the incident. Incidents involving PCI data are to be investigated by a Visa-approved Qualified Incident Response Assessor.
13. **Law Enforcement.** To report incidents that may have criminal legal consequences, only after consultation with the Office of General Counsel or Attorney General's Office.
14. **Other.** Sources of help, such as external computer security incident response teams, security experts, etc. may be utilized as desired or appropriate.

Subpart E. Links to Established Processes. The Incident Response Plan must include links to relevant system or campus policies or procedures where they exist. For example:

1. Breach Notification
2. Continuity of Operations
3. Disaster Recovery

Subpart F. Testing. The Incident Response Plan must be tested at least annually. This test should include the items outlined below at a minimum.

1. Inclusion of institution team members to ensure each member is aware of the plan and that the appropriate individuals are notified within the test scenario.
2. System office or external resources as necessary to validate institution incident response plans against external processes.
3. A walk-through of the plan components, and the actions that would be taken in the test scenario(s).
4. A review of the test to determine how the systems or processes should be improved.
5. Updating the Incident Response Plan based on the results of the test.

Subpart G. Confidentiality. Information that is created, collected and maintained in connection with an information security incident is subject to the Minnesota Government Data Practices Act (MGDPA), Minnesota Statutes §13, and may be subject to other privacy laws depending on the content of the data. Information security incident documentation may include, in whole or in part, "security information," and should be labeled and handled appropriately, distributing only on a need-to-know basis.

1. **Confidentiality During an Incident.** Security information pertaining to an active investigation must be protected throughout the incident and within the incident response team. Information disseminated among team members should be limited to those with a need to know.

Part 4. Definitions.

Subpart A. Access. Approved authorization to view, modify or delete system information/data. Access shall be authorized to individuals or groups of users depending on the application of law, system policy or guideline. Technical ability to access information is not necessarily equivalent to legal authority.

Subpart B. Authorized Individual. Employee, consultant, volunteer or other individual who is approved and allowed access to information within the system to perform an activity on behalf of an institution. The individual may have access to any class of information, according to policy.

Subpart C. Breach. Any accidental or deliberate non-compliance with policies or other security controls.

Subpart D. Data. Information collected, stored, transferred or reported for any purpose, whether in computers or in manual files. Data can include: financial transactions, lists, identifying information about people, projects or processes, and information in the form of reports. Because data has value, and because it has various sensitivity classifications defined by federal law and state statute, it must be protected.

Subpart E. Information Resources. Data collected, created, received, maintained or disseminated by any system user, regardless of its form, storage media, security classification, or conditions of use.

Subpart F. Information Technology Resources. Facilities, technologies, and information resources used for system member information processing, transfer, storage, and communications. Included in this definition are computer labs, classroom technologies, computing and electronic communications devices and services, such as modems, e-mail, networks, telephones (including cellular), voice mail, fax transmissions, video, multimedia, and instructional materials. This definition is not all inclusive, but rather, reflects examples of system equipment, supplies and services.

Subpart G. Institution. One of the separate entities, or having to do with an organizational entity as described under system.

Subpart H. May. A statement that is optional.

Subpart I. Minnesota Government Data Practices Act (MGDPA). Per Minnesota Statutes §13, MGDPA regulates the collection, creation, maintenance and dissemination of government data in state agencies, statewide systems, and political subdivisions. It establishes a presumption that government data are public and are accessible by the public for both inspection and copying unless there is a federal law, a state statute, or a temporary classification of data that provides that certain data are not public.

Subpart J. Must. A statement that is required for a compliant implementation.

Subpart K. Must Not. A statement that is prohibited for a compliant implementation.

Subpart L. Not Public Data. Data that is considered confidential, private, nonpublic or protected nonpublic data as defined in the MGDPA or any other relevant state or federal statute or system legal guideline. For examples of data classifications, see standard 5.23.E, Notice of Breach of Security, Part 4: Reporting a Suspected Breach.

Subpart M. Payment Card Industry (PCI) Data. Payment card information, as defined by the Payment Card Industry Security Standards Council. PCI data is subject to the PCI Data Security Standards. Such information includes payment account numbers (PANs) plus expiration dates, cardholder names, or verification codes, or data stored on track 2 of the payment card.

Subpart N. Should. A statement that is recommended but not required.

Subpart O. Should Not. A statement of practices that are not recommended but which may be followed.

Subpart P. Security Information. As defined by MGDPA, Minnesota Statutes §13, "government data the disclosure of which would be likely to substantially jeopardize the security of information…against theft, tampering, improper use… [or] illegal disclosure". Security information should be labeled as such and handled appropriately, distributing only on a need-to-know basis.

Subpart Q. System. Denotes the Minnesota State Colleges and Universities Board of Trustees, the system office, the state colleges and universities, and any part or combination thereof.

Part 5. Authority. Board policies 1A.1 and 5.23 delegate authority to the vice chancellor to develop system guidelines, consistent with Board policy and system procedure, for the purposes of implementing Board policy 5.23.

Approval Date: 11/04/09,
Effective Date: 05/04/10,

Date and Subject of Revision:

1/25/12 - The Chancellor amends all current system procedures effective February 15, 2012, to change the term "Office of the Chancellor" to "system office" or similar term reflecting the grammatical context of the sentence.