Guideline 5.23.1.13 Breach Notification

Part 1. Purpose. This guideline is intended to assist Minnesota State Colleges and Universities (System) to implement the requirements of Minn. Stat. Sect. 13.055 and provide timely and appropriate notice to individuals who are affected by a breach of the security of their private or confidential data. All System employees must immediately report known or suspected breaches of security to the designated System individual or office. The Office of General Counsel (OGC) or Attorney General's Office (AGO), in consultation with campus or other appropriate System personnel shall determine whether notice of the breach is required and how the notice will be communicated.

Part 2. Applicability. This guideline applies to breaches of the security of private or confidential data maintained by or on behalf of Minnesota State Colleges and Universities.

Part 3. Guidelines.

Subpart A. Local Campus Authority. The Chancellor or college or university president must designate an individual as the local campus authority (LCA) who is responsible for compliance with this guideline. For the purpose of this guideline, the system office is considered a campus and must appoint an LCA. The LCA will oversee the implementation of the Guideline, including:

- appropriate notice and training for the workforce;
- appropriate notice and consultation with system office personnel;
- periodic review of the procedures; and
- the creation and maintenance of documents in accordance with applicable campus records retention schedules.

The LCA may delegate implementation responsibilities to other campus personnel as appropriate.

Subpart B. Reporting a Suspected Breach. Any user who knows of or reasonably believes that a breach of the security of private or confidential data has occurred must immediately report to his or her supervisor or other designated individual or system office.

Supervisors who receive a report of the breach must immediately report the incident to the LCA. The LCA or user must immediately notify the data owner of the reported breach, if necessary.

The report should include date and time of report; when breach occurred (if known); the type of data involved; the (approximate) number of affected individuals and other pertinent information. An institution may develop a reporting form to be used for this purpose.

System employees who report a breach under this guideline must not be subject to retaliation.

Local campus authorities should make available to all users information about this guideline and how to report a security breach.

Subpart C. Breach Response Process. After a breach of security has been reported, the LCA must work with the user to take necessary steps to contain and control the integrity of the electronic or other data handling systems affected by the reported breach and conduct a preliminary internal assessment of the scope of the breach. Applicable System Information Technology (IT) security procedures or other guidelines shall be consulted.

If the breach is suspected on a System computing system that contains or has network access to private or confidential data, the user shall consult with system office IT personnel and consider control measures including but not limited to removing the computing system from the campus network.

1. **Determining Breach.** The LCA or designee shall consult with the OGC and/or AGO to determine whether a breach of security of data has occurred. Due consideration should be given to the potential for damage to individuals if no breach is determined and notice is not provided.
    (a) **Incidents**. Examples of the types of incidents that may result in a notice-triggering breach include, but are not limited to:
        i. Evidence of unauthorized access into a system containing private/confidential data;
        ii. Missing or stolen laptop, desktop, storage device or any other information technology resource containing files with private/confidential data;
        iii. Documents containing private/confidential data sent in any form to a wrong recipient;
        iv. System containing private/confidential data that has been compromised; or
        v. Employee misuse of authorized access to disclose private or confidential data.
    (b) **Acquistition.** Minn. Stat. Sect. 13.055, Subd. 2 requires state agencies to notify individuals if their private or confidential data has been or is reasonably believed to have been acquired by an unauthorized person. In making that determination, the following factors, among others, may be considered:
        i. Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device or document containing unprotected private or confidential information;
        ii. Indications that the information has been downloaded or otherwise acquired;
        iii. Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported;
        iv. The encryption protection of the data, if any;
        v. Duration of exposure;
        vi. The extent to which the compromise of electronic data indicates a directed attack, such as a pattern showing the machine itself was specifically targeted; or
        vii. Indications that the attack was intended to seek and collect private or confidential data.

2. **Timing of Notification**. If a breach has been determined, in most instances the data owner has primary responsibility to notify affected individuals. Notice is to occur without unreasonable delay. The system should strive to provide notice within ten business days of determining that notice is required unless delay is appropriate due to: a) the legitimate needs of a law enforcement agency; or b) any measures necessary to determine the scope of the breach and restore the reasonable security of the data.

   Immediate notification may be appropriate in the event of a breach that could have immediate deleterious impact on individuals whose data may have been acquired by an unauthorized person.

3. **Contacting Law Enforcement.** The LCA or designee(s) shall consult with the OGC or the AGO before contacting law enforcement agencies if the breach of security is believed to involve illegal activities. Information may be shared with law enforcement consistent with applicable data privacy laws. If law enforcement is contacted, it should be informed of the System's practice to provide notice to affected individuals within ten days. If law enforcement advises that such notice would impede an active criminal investigation, notice may be delayed. Delayed notice should be sent out as soon as law enforcement advises that it would no longer impede the criminal investigation.

4. **Whom to Notify**. The OGC or AGO, in consultation with appropriate System personnel, including but not limited to the user and data owner, shall determine the scope of the notice. Notice of a breach must be sent to any individual whose private or confidential data has been or is reasonably believed to have been acquired by an unauthorized person. If specific individuals cannot be identified, notice should be sent to groups of individuals likely to have been affected, such as all whose information is stored in the database or files involved in the breach. Appropriate measures should also be taken to prevent notice lists from being over-inclusive.

Subpart D. Notice.

1. **Content**. The LCA or designee shall consult with the OGC or AGO on the wording of a notice. System communications personnel may also be consulted, where appropriate. Notices shall generally be sent separate from other documents. The format should utilize subheadings and clear language. The Model Letter may be used for notification.

   If the Model Letter is not used, include the following information in the notice:

   (a) A general description of what happened, and when, to the extent known

   (b) The nature of the individual's private or confidential information that was involved (not listing the specific private/confidential data).

   (c) Information about what the institution has done to protect the individual's private/confidential information from further disclosure.

   (d) Institution assistance (such as website information or phone number of a campus resource) for further information about the incident.

   (e) Information, such as Web sites, about what individuals can do to protect themselves against identity theft including; contact information for nationwide credit reporting agencies; the Federal Trade Commission and appropriate state agency resources.

2. **Method of Notification.** The OGC or AGO in consultation with the LCA or designee(s) shall determine the appropriate method of notice as follows:

   (a) **Written notice** by first class mail to each affected individual; or

   (b) **Electronic notice** to each affected individual if communication normally occurs in that medium, and the procedure is otherwise consistent with the provisions regarding electronic records and signatures contained in 15 U.S.C. Sect. 7001. Any college or university that wishes to utilize electronic notification must consult with the OGC or AGO; or

   (c) **Substitute notice** may be provided if the cost of providing the written notice required to each affected individual would exceed $250,000, or that the affected class of individuals to be notified exceeds 500,000, or the institution does not have sufficient contact information to notify affected individuals. Substitute notice consists of all of the following:

   (d) **E-mail notice** if the institution has an e-mail address for the affected individuals;

   (e) **Conspicuous posting** of the notice on the institution website for a minimum of 45 days; and

   (f) **Notification to major media** outlets that reach the general public.

Subpart E. Coordination with Credit Reporting Agencies. Credit reporting agencies (agencies) assist individuals in responding to a notice of a security breach. Such agencies should be notified in advance of sending notice of security breach incidents that may significantly increase calls to agencies for assistance.

If notice is required to be given to 1,000 or more individuals at one time, the System shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis as defined in 15 U.S.C. Sect. 1681a, of the timing, distribution and content of the notice to be sent. Such contacts shall include but not be limited to the following:

- **Equifax:**
  U.S. Consumer Services
  Equifax Information Services, LLC.
  Phone: 1-800-525-6285
- **Experian:**
  Experian Security Assistance
  P.O. Box 72
  Allen, TX 75013
  1-888-397-3742
- **TransUnion:**
  Phone: 1-800-680-7289

Subpart F. Documentation. The LCA or designee must complete a Breach of Security Incident Response Summary for each reported breach, regardless of whether notice is given. The form should be completed beginning at the time of the initial report or as soon thereafter as practical.

Where appropriate, all documentation related to the breach and investigation shall be labeled and maintained as not public pursuant to the applicable data privacy classification including, but not limited to, "security information" as defined by Minn. Stat. Sect. 13.37. Subd. 1(a). The form shall be retained by the LCA in accordance with the applicable records retention policy and may also be requested by the system office.

Part 4. Definitions.

Subpart A. Breach of the security of the data. Breach of the security of the data means the unauthorized acquisition of data maintained by the System, in any medium, that compromises the security and classification of the data, but not including the good faith acquisition by an employee, contractor or agent of the system if not provided to an unauthorized person.

Subpart B. Confidential data. Confidential data means data on individuals which is made not public by statute or federal law applicable to the data and is inaccessible to the individual subject of that data.

Subpart C. Contact information. Contact information means either: name and mailing address, or name and e-mail address for each individual who is the subject of data maintained by the institution.

Subpart D. Data owner. The institution individual or department with primary responsibility for the content or function of private or confidential data.

Subpart E. Government data. Government data means all data collected, created, received, maintained or disseminated by any government entity regardless of its physical form, storage media 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. Person. Person means any individual, partnership, corporation, association, business trust or a legal representative of an organization.

Subpart H. Private data. Private data means data on individuals which is made by statute or federal law applicable to the data not public and accessible to the individual subject of that data. See Examples of Data Classifications in Related Documents section below.

Subpart I. System. System means all institutions of Minnesota State Colleges and Universities and the system office.

Subpart J. Unauthorized acquisition. Unauthorized acquisition means that a person has obtained government data without the informed consent of the individuals who are the subjects of the data or statutory authority and with the intent to use the data for non-governmental purposes.

Subpart K. Unauthorized person. Unauthorized person means any person who accesses government data without permission or without a work assignment that reasonably requires the person to have access to the data.

Subpart L. User. Any individual, including but not limited to, students, administrators, faculty, other employees, volunteers, and other authorized individuals using System information resources, whether or not the user is affiliated with the System.

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.

Date of Adoption: 8/29/11,
Date of Implementation: 8/29/11,

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.

8/29/11- language in this new guideline was originally adopted as ITS Standard 5.23.E on December 5, 2006, and was implemented December 5, 2006. ITS Standard 5.23.E remained in place until the adoption of System Guideline 5.23.1.13 on August 29, 2011.