Freeborn County Data Breach Notification Policy

(adopted effective July 19, 2022)

Part 1. Purpose. This policy is intended to assist Freeborn County, Minnesota and its departments and offices (hereafter the "County") to implement the requirements of Minnesota Statutes § 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 County employees must immediately report known or suspected breaches of security to the employee's supervisor, department head, or the Responsible Authority. The Freeborn County Attorney's Office (CAO) in consultation with the Responsible Authority, County Administration, and/or other appropriate County personnel shall determine whether notice of the breach is required and how the notice will be communicated.

Part 2. Applicability. This policy applies to breaches of the security of private or confidential data maintained by or on behalf of the County.

Part 3. Guidelines.

Subpart A. Responsible Authority. The Responsible Authority is responsible for compliance with this Policy. The Reasonable Authority is responsible for compliance with this Policy. The Responsibility Authority will oversee the implementation of the Policy, including:

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

The Responsible Authority may delegate implementation responsibilities to other County personnel as appropriate.

Subpart B. Reporting a Suspected Breach. Any employee or user who knows of or reasonably believes that a breach of security of private or confidential data has occurred must immediately report to their supervisor, department head or the Reasonable Authority.

Supervisors who receive a report of the breach must immediately report the incident to the department head and the Responsible Authority. The Responsible Authority must immediately notify the data owner of the reported breach, if necessary.

The report should include the date and time of the report, the date and time when the breach occurred (if known); the type of data involved; the number of affected individuals and other pertinent information.

County employees who report a breach under this policy must not be subject to retaliation. The Responsible Authority should make available to all employees information about this policy and how to report a security breach.

Subpart C. Breach Response Process. After a breach of security has been reported, the Responsible Authority must work with employee, the user, and the Department Head(s) of the employee and 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 County Information Technology (IT) security procedures or other policies shall be consulted.

If the breach is suspected on a County computing system that contains or has network access to private or confidential data, the Responsible Authority shall consult with County IT personnel and consider control

measures including but not limited to removing the computing system from the County Network.

1. Determining Breach. The Responsible Authority shall consult with the CAO 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:
        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) Acquisition. Minnesota Statute § 13.055, Subd. 2 requires governmental entities 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 that 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 County 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) 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 authorized person.
3. Contact Law Enforcement. The Responsible Authority shall consult with the CAO 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 County'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 CAO, in consultation with appropriate County personnel, including but not limited to the user and data owner, shall determine the scope of the notice. Notice of a breach much 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 Responsible Authority shall consult with the CAO on the wording of a notice. Notices shall generally be sent separate from other documents. The format should utilize subheadings and clear language.

   Notice shall include the following information:
   a) A general description of the data breach including when it occurred, 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 County has done to protect the individual's private/confidential information from further disclosure.
   d) County assistance (such as website information or phone number of a County resource) for further information about the incident.
   e) Information, such as websites, 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 CAO, in consultation with the Responsible Authority, 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; 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 the affected class of individuals to be notified exceeds $500,000, or the County does not have sufficient contact information to notify affected individuals. Substitute notice consists of all of the following:
   d) E-mail notice if the County has an e-mail address for the affected individuals;
   e) Conspicuous posting of the notice on the County's website for a minimum of 45 days; and
   f) Notifications 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 County shall notify, without reasonable 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
Phone: 1-888-397-3742

TransUnion:
Phone: 1-800-680-7289

Subpart F. Documentation. The Responsible Authority must complete a written summary for each reported breach, regardless of whether notice was given. The summary 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 Minnesota Statutes §13.37, Subd. 1(a). The summary shall be retained by the Responsible Authority in accordance with the applicable records retention policy and may also be requested by the County Administration office.

Part 4. Definitions.

Subpart A. Breach of the security of the data. Breach of the security data means the unauthorized acquisition of data maintained by the County, 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 subject of data maintained by the County.

Subpart D. County. "County" means all department and offices of Freeborn County regardless of department head, supervisor or responsible authority as designated by the Board of Commissioners.

Subpart E. Data owner. The County individual, department or office with primary responsibility for the content or function of private or confidential data.

Subpart F. 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 G. Information Technology Resources. Facilities, technologies, and information resources used for system member information proceeding, 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 H. Individual. Individual means a natural person. In the case of a minor or an incapacitated person as defined in Minn. Stat. Sec. 524.5-102, subdivision 6, "individual" includes a parent or guardian or an individual acting as a parent or guardian in the absence of a parent or guardian.

Subpart I. Person. Person means any individual, partnership, corporation, association, business trust

or a legal representative of an organization.

Subpart J. Private data. Private data means data on individuals made by statute or federal law applicable to the data (1) not public and (2) accessible to the individual subject of that data.

Subpart K. Responsible Authority. Responsible Authority is as defined in Minn. Stat. Sec. 13.01, Subd. 16.

Subpart L. Unauthorized acquisition. Also known as **"unauthorized access"**. 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 M. 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 N. User. Any individual, including but not limited to, employees, elected officials, appointees, interns, externs, administrators, independent contractors, and other unauthorized individuals using County information resources, whether or not the user is affiliated with the County.

13.025 GOVERNMENT ENTITY OBLIGATION.

Subdivision 1. **Data Inventory.** The responsible authority shall prepare an inventory containing the authority's name, title, address, and a description of each category of record, file, or process relating to private or confidential data on individuals maintained by the authority's government entity. Forms used to collect private and confidential data may be included in the inventory. The responsible authority shall update the inventory annually to make the changes necessary to maintain the accuracy of the inventory. The inventory must be available from the responsible authority to the public according to the provisions of sections 13.03 and 15.17. The commissioner may require responsible authorities to submit copies of the inventory and may request additional information relevant to data collection practices, policies, and procedures.

Subd. 2. **Public data access policy**. The responsible authority shall prepare a written data access policy and update it no later than August 1 of each year, and at any other time as necessary to reflect changes in personnel, procedures, or other circumstances that impact the public's ability to access data.

Subd. 3. **Data subject rights and access policy.** The responsible authority shall prepare a written policy of the rights of data subjects under section 13.04 and the specific procedures used by the government entity for access by the data subject to public or private data on individuals. The written policy must be updated no later than August 1 of each year, and at any other time as necessary to reflect changes in personnel procedures, or other circumstances that impact the public's ability to access data.

Subd. 4. **Availability.** The responsible authority shall make copies of the policies required under subdivisions 2 and 3 easily available to the public by distributing free copies to the public or by posting the policies in a conspicuous place within the government entity that is easily accessible to the public or by posting on the government entity's website.

History: *2012 c 290 s 10*