



Data Breach

Preparation
and Notification
for
Electronic
Data

TABLE OF CONTENTS

Overview	3
Purpose of this guide.....	3
Scope of this guide.....	3
Who should use this guide?.....	4
Key factors to consider.....	4
FAQs.....	6
What to expect from this guide	6
Part 1: Preparation	7
How do electronic data breaches occur?	7
Why should an agency create a data breach prevention and notification plan?.....	7
Who should be part of a Breach Response Team?	8
My Breach Response Team.....	9
Who will we need to notify?.....	10
What does a breach incident response look like?	10
Part 2: Preparedness Plan Audit	11
Preparedness audit checklist	12
Part 3: Breach Response	13
Ten steps in the first 24 hours.....	13
Next steps	14
Notifications	15
Appendix A: Communications Templates	16

OVERVIEW

You just received word that the private records of 1,700 people in your systems have been compromised. What do you do?

Electronic data breaches are not a matter of “if,” but “when.” And “breaches” are not limited to malicious actions, such as theft or hacking from persons outside of the entity, but may arise internally due to failure to follow policies designed to prevent improper access or disclosure.

Having a plan in place will help an agency:

- Determine if a breach, as defined by law, has occurred
- Get through the process as smoothly as possible
- Assure the agency contacts the right people
- Minimize damage to those impacted
- Comply with breach notification laws and contractual requirements
- Protect its reputation

This guide is a vital tool that can be used both to prevent breaches and to ensure preparedness in case of a breach.



Purpose of this guide

MN.IT Services developed this guide to assist agencies with effective preparation and response to data breaches. It is aimed at encouraging agencies to voluntarily put in place a Data Breach Preparation and Notification Plan (Plan).

It is important to note that this manual is intended to cover data breaches as defined in Minnesota Statutes, Section 13.055. All “data breaches” at state agencies require notification to the Office of the Legislative Auditor under Minnesota Statutes, Section 3.971. However, only “breach of the security of the data” breaches will trigger the notification requirements under Minnesota Statutes, Section 13.055.

Scope of this guide

A key challenge in responding to a data breach is determining if and when notification is an appropriate response. This guide provides general guidance on responding to a data breach. Agencies are responsible for evaluating a breach and making decisions on actions to take according to their own assessment of risks and responsibilities with regard to the particular circumstances.

This information provides guidance for agencies when responding to an *electronic* data breach. For other data breaches, contact your agency’s privacy officer.

Who should use this guide?

This guide has been developed for use by Minnesota's executive branch agencies, boards, councils and commissions, and other state government entities that use MN.IT's services.

Key factors to consider

Enterprise Information

The Office of MN.IT Services is responsible for setting information security policies and standards and overseeing the security of the state's executive branch information and telecommunications technology systems and services. As required by Minnesota Statutes, MN.IT will consult with agency heads and other compliance officials in state agencies to ensure that all federal information security requirements are incorporated into the policies and standards that govern the security of state data. To fulfill this responsibility a comprehensive information security program, headed by the Chief Information Security Officer (CISO) is in place to create, monitor and enforce state-wide information security policies and standards, identify and address vulnerabilities and risks, and manage security incidents.

Vendors with Data Access

Vendors with access to state data are expected to follow the [Enterprise Policies and Standards](#).

Employee Training

The [Enterprise Information and Security Training and Awareness Standard](#) states that government entities must institute information security awareness and education that provides:





- General security awareness for all employees and contractors.
- Specific role-based security training for information system users, technical staff, and security professionals.
- Evidence of individual information security training activities and reporting as required.

In addition to the focus on data security and breach preparedness, an agency must also ensure that all employees are trained on data breach prevention and preparedness. The training should include topics such as:

- Integrating data security efforts into daily work habits – locked printing, locking file cabinets, shredding paper documents, etc.
- Each employee's responsibility to follow the agency's policies.
- A method for reporting.
- Data classifications.
- Only accessing not public data for a work assignment.

If you have questions about security training, contact the Enterprise Security Office at GRC@state.mn.us.

Agency Policies

An agency should develop appropriate policies that implement measures, practices and procedures to reduce the risks of data breaches.

Collecting & Keeping Data

Some breaches or risks of harm can be avoided or minimized by not collecting particular types of private information or by only keeping it as long as necessary. Consider the following:

- What private information is necessary to collect? Private information that is not collected cannot be breached. Private and confidential data should only be collected and stored if needed for the administration and management of an entity's programs.
- How long does the private information need to be kept? An agency should take reasonable steps to destroy private information once it is no longer needed.

Agencies have record-keeping obligations under the Official Records Act and Records Management Statute and agencies should therefore carefully consider retention practices.

What is a data breach?

Minnesota Statutes, Section 13.055, defines a “Breach of the Security of the Data” as occurring when all of the following conditions apply:

- A person with no reasonable, work-related, need to access private or confidential data.
- Views or takes the data.
- With the intent to use the data for purposes unrelated to his/her job.

NOTE: Good faith acquisition of, or access to government data by an employee, contractor, or agent of a state agency for the purposes of fulfilling their job responsibilities is not a breach, even if it results in accidental access to unauthorized data. If there is no intent to improperly use or maintain the unauthorized data, a breach (as defined by Minnesota Statutes, section 13.055) has not occurred.

How do data breaches under Minnesota Statutes, Section 13.055 occur?

Data breaches occur when an unauthorized party views or accesses government data with the intent to use the data for an unauthorized purpose. This may occur in the form of an employee deliberately viewing records that do not relate to his/her work assignments, or in the form of an external, criminal, attack by a hacker trying to access government databases.

What are my legal requirements regarding a data breach under Minnesota Statutes, Section 13.055?

Working with your agency’s legal counsel can help you determine your obligations, which is something you should explore before a data breach ever occurs. Your legal counsel will help to navigate the different applicable state and federal law, industry regulations, and contractual obligations. Some agencies will have special considerations for reporting a data breach and notifying affected

individuals. Working with your legal counsel can assist in determining whether an agency is obligated by law to notify affected individuals. The Information Policy Analysis Division (IPAD) of the Department of Administration is also a resource available to agencies.

Keywords

Not public data: data classified by statute, federal law, or temporary classification as confidential, private, nonpublic, or protected nonpublic.

Private data: not public data that is available only to:

- The data subject or a party with the informed consent of the data subject.
- Government employees with a work assignment that requires access to the data.
- Government entities with statutory authority to access or receive the data.
- Parties with authority to access the data in the form of a court order.

Confidential data: not public data that is available only to:

- Government employees with a work assignment that requires access to the data.
- Government entities with statutory authority to access or receive the data.
- Parties with authority to access the data in the form of a court order.

What to expect from this guide

This document is split into multiple sections: the preparations that need to be completed prior to a breach, the remediation and notification following a breach, and the post-breach reporting.



PART 1: PREPARATION



Preparation is the best defense.

Having an incident response plan helps to both prevent breaches and ensure that an entity is prepared if a breach should occur. Entities with an established plan are able to respond quickly in the event of a breach. And being able to act quickly can prevent further loss and public relations backlash.

If your agency does not have a plan, this guide will help you to create one. Having a well thought out plan could mean the difference between a breach which causes a brief disruption and one that causes a major meltdown.

How do electronic data breaches occur?

- Lost or stolen laptops, or removable storage devices, or smartphones that contain private data.
- Databases containing private data being hacked by individuals outside of the agency.
- Employees accessing private data without a work assignment.
- Misguided or misaddressed emails or faxes that contain not public data.
- Individual deceiving an agency into improperly releasing another person's private data.

Why should an agency create a data breach prevention and notification plan?

In the midst of a data breach is not the time to determine how an entity is going to handle a breach or who will be responsible for handling each of the different pieces. Yet without a plan, an entity is forced to do just that. Developing a data breach prevention and notification plan and having a set team before they are needed ensures that an entity is prepared to respond appropriately to a breach.



Who should be part of a Breach Response Team?

Cyber security is a shared responsibility. Creating a plan to bring together your business leaders and partners, such as MN.IT, will help you respond quickly and keep Minnesotans safe in the event of a breach.

One of the first things you should do is identify the team you will need to lead your agency's response through a breach incident and what their roles will be. This is your "Breach Response Team." Each member of the team should also have a backup.

Data breaches require collaborative teams that include a variety of roles. Each role should be analyzed to determine if it is needed in your agency's Response Team.

Start by selecting an incident lead, who will lead your agency in the event of a data breach. This person should likely be someone from the legal or privacy office. An incident lead should be able to:

- Manage and coordinate the agency's overall response efforts and the team.
- Act as the intermediary between the agency's management and team members tasked with reporting on progress and problems.
- Identify key tasks, manage timelines and document response times from beginning to end.
- Outline the resources needed to manage the breach.
- Summarize the steps needed to assess the scope of the breach.
- Analyze efforts post-breach to better prepare the agency and Response Team for the next incident.

Other employees an agency may want on their Response Team and what their responsibilities might entail are attached in the following table.



My Breach Response Team

NAMES	ROLE
Primary _____ Backup _____	Incident Lead
Primary _____ Backup _____	In-house counsel (or the Attorney General's Office) <ul style="list-style-type: none">• Helps minimize risk of litigation and fines.• Determines whether it is necessary to make notifications.• Provides guidance on both state and federal breach laws in your industry.• Responsible for communicating with Law enforcement and other impacted groups or data owners.
Primary _____ Backup _____	Executive team member <ul style="list-style-type: none">• Ensures directional leadership, backing and resources.
Primary _____ Backup _____	MN.IT CIO <ul style="list-style-type: none">• Provides information about breached technology and communicates with third-party technology vendors.
Primary _____ Backup _____	Human Resources member <ul style="list-style-type: none">• Provides guidance on communications to and about employees.
Primary _____ Backup _____	Compliance/Privacy officer <ul style="list-style-type: none">• Provides guidance about public and not public data.
Primary _____ Backup _____	Marketing/Communications member <ul style="list-style-type: none">• Writes and coordinates internal and external communications.• Track and analyze media coverage and quickly respond to any negative press during a breach.
Primary _____ Backup _____	Customer Relations team member <ul style="list-style-type: none">• Coordinates communications to consumer end-users.

Who will we need to notify?

Preparation for who you need to notify will depend upon the data that has been breached.

- Per Minnesota Statutes, Section 3.971, an agency must notify the Office of the Legislative Auditor when there is the possibility of improper access or use of not public data.
- You should contact the Governor's office if you are notifying individuals and/or the Office of the Legislative Auditor.
- You may need to contact others based on requirements for your agency's industry (e.g. CJI, PCI, IRS, HIPAA, etc.).
- You must notify those who have had their data compromised per Minnesota Statutes, Section 13.055. It is a good idea to ask your customers how they want to receive communications from you. Their response is how you should send a notification to them.

Comparing Minnesota Statutes, Section 3.971 and Section 13.055

MINNESOTA STATUTES, SECTION 3.971	MINNESOTA STATUTES, SECTION 13.055
When an entity has knowledge of improper access or use of not public data, regardless of how the unauthorized party intended to use the data, the Office of the Legislative Auditor must be notified.	<ul style="list-style-type: none">• When a person with no reasonable, work-related, need to access private or confidential data,• Views or takes the data,• With the intent to use the data for purposes unrelated to his/her job,• The subjects of the data must be notified.

What does a breach incident response look like?

- Discover breach.
 - The most costly breaches result from either malicious or criminal attacks, such as hacking. However, negligent employees are the top cause of data breaches in the United States.
 - There has been a breach that generally triggers a notice per [Minnesota Statutes, Section 13.055](#), when all of the following apply:
 - **A person with no reasonable, work-related, need to access private or confidential data,**
 - **Views or takes the data,**
 - **With the intent to use the data for purposes unrelated to his/her job.**

- Assemble Internal Response Team
- Investigate the breach and determine if notification is required
- Begin notification process (if required).
 - A government entity must disclose any breach of private or confidential data to affected individuals who are the subjects of the data when they reasonably believe a qualifying breach under Minnesota Statutes, Section 13.055 has occurred. The required notice to individuals must:
 - Be in writing.
 - Inform the individual that a report will be prepared about the breach investigation.
 - State that an individual may request a copy of the report by mail or email.
 - Be sent without unreasonable delay.
- Mail/email notifications (if required).
 - Government entities may provide the written notice to affected individuals either by first class mail or by electronic notice.
 - An entity may choose substitute notice if the cost of providing the written notice exceeds \$250,000 or the group of individuals it must notify exceeds 500,000, or the entity does not have sufficient contact information. Substitute notice consists of all of the following:
 - Email notice if the entity has an email address for affected individuals.
 - Post the notice on the website of the entity, if the entity maintains a website.
 - Provide notification to major media outlets that reach the general public within the government entity's jurisdiction.
- Notify Law enforcement and other impacted parties
- Respond to inquiries
 - Be prepared to respond to questions and concerns related to the breach



PART 2: PREPAREDNESS PLAN AUDIT

Creating a preparedness plan clears one of the major hurdles in setting up the agency for success if a data breach occurs. However, a plan can only help an agency to succeed if it is both comprehensive and current. An agency must make it a priority to review and update the plan on a regular basis, along with training the Response Team on an annual basis. Semi-routinely, the Response Team should consider different scenarios that could occur and review the plan to determine whether it would address each one. Different possible scenarios to review could include an internal breach, external attack, and/or loss or theft of state equipment.





Preparedness Audit Checklist

Update data breach Response Team contact list

- Check that contact information for members of the Response Team is current.
- Remove anyone who is no longer part of the Response Team.
- Redistribute the updated list to the appropriate parties.

Verify that the breach response plan is comprehensive

- Update the plan, as needed, to account for any major agency changes.
- Verify that each Response Team member understands their role during a breach. Create example scenarios for your Response Team to address.

Review notification guidelines

- Ensure that the notification portion of your response plan takes into account the latest state legislation.
- Update notification letter templates, as needed, to reflect any new laws.

- Agencies with HIPAA, IRS, SSA, CJI, PCI, etc. data reporting requirements need to ensure that they have the proper contacts and reporting process in place.

Check up on third parties that have legal access to your data

- Review how third parties are managing your data and if they are meeting your data protection standards.
- Ensure third parties are up to date on any new legislation that may affect you during a breach.
- Verify that third parties understand the importance of notifying you immediately of a breach and working with you to resolve it.
- Ensure contracts have breach notification requirements included.

Review staff security awareness

- Ensure all employees are up to date on proper data protection procedures.
- Review how to spot and report the signs of a data breach within everyday working environments.



PART 3: BREACH RESPONSE

Although there is no single way of responding to a data breach and each breach will need to be dealt with on a case-by-case basis, the following Breach Response Checklist can assist an agency to move forward in a quick and coordinated manner.

A breach has occurred. What you do in the next hours and days will help you halt the security threat, uncover and preserve information and protect your agency's reputation. Below are the steps you need to take now.



Ten steps in the first 24 hours

- Record the date and time** the breach was discovered and when the response efforts began.
- Alert and activate** the Breach Response Team in order to begin executing your preparedness plan.
- Contact your MN.IT CIO.** Your agency-based CIO will work with MN.IT's Forensics Team to stop any additional data loss and will properly gather and protect evidence that may be needed for law enforcement purposes.
- Contain the breach.** For example, recover the mishandled paper files, shut down the system that was breached, revoke computer access privileges.
- Document everything** known about the breach – who discovered it, who reported it, to whom was it reported, who else knows about it, what type of breach occurred, what data was compromised, what systems are affected, what devices are missing, etc.
- Determine the cause and extent** of the breach.
- Determine who is or who may be impacted.**
- Review protocols** regarding notification about the incident.
- Assess priorities** and risks based on what you know about the breach.
- Launch crisis communications process.**

Next steps

Once you have begun or completed the above checklist, ensure that your plan is on track and continue with the following steps:

Fix the Issue that Caused the Breach

- MN.IT's Forensic team will delete any hacker tools.
- A determination will be made as to whether there are any other security gaps or risks.
- Affected equipment will be replaced with clean machines as needed.
- Security precautions will be implemented to ensure that the same type of breach cannot happen again.
- Document when and how the breach was contained.

Continue Working with Forensics

- Analyze backup, preserved or reconstructed data sources.
- Ascertain the number of suspected people affected and the type of information that was compromised.
- Begin to align compromised data with customer names and addresses for notification.

Identify Legal Obligations

- Revisit state and federal regulations and contractual regulations governing your data.
- Determine all entities that need to be notified – customers, employees, the media, other agencies, the Governor's Office, etc.
- Ensure that all notifications occur within any mandated timelines.

Reports

- Compile daily breach reports to ensure that necessary management is kept up to date.
- Create a high-level overview of priorities and progress, as well as problems and risks.

Identify Conflicting Initiatives

- Make the Response Team and management aware of any upcoming business initiatives that may interfere with response efforts.
- Decide whether to postpone these efforts and for how long in order to focus on the breach response.
- Address security gaps or risks.
- Take infected machines offline as instructed by the Forensics Team.
- Ensure a similar breach will not happen again.
- Have forensics delete hacker tools after legal evidence has been preserved.
- Analyze backup, preserved or reconstructed data sources.
- Begin to align compromised data with customer names and addresses for notification.

Report to Upper Management

- Compile regular reports for upper management.
- Include priorities, progress, problems and risks.

Identify Conflicting Initiatives

Keep Response Efforts on Track

Notifications

Not all breaches require notification under Minnesota Statutes, Section 13.055. If agency data was encrypted or an employee accidentally accessed but didn't misuse the data, an agency may not need to notify data subjects. However, agencies are required to notify the Office of the Legislative Auditor in all breach or potential breach situations. Be sure to seek and follow legal advice before deciding whether to notify or not.

As a state agency, you will determine whether a breach occurred, along with how and when notifications should take place. Consider the following things.

State law and federal mandates

Refer to your preparation plans for notification information. As a reminder:

For the State of Minnesota:

- You must notify impacted individuals when private or confidential data about those individuals have been breached under the definitions in Minnesota Statutes, Section 13.055
- You must notify the Office of the Legislative Auditor on any improper or potentially improper use of not public data per Minnesota Statutes, Section 3.971

For Federal:

You'll need to know whether federal law overseeing your industry requires a shorter timeline. CJI, IRS, HIPAA and others may have stricter standards. Check with your legal representative for clarification.

Law enforcement considerations

If law enforcement is involved in your incident, they may request that you wait to notify individuals to avoid impacting an ongoing investigation.

Making contact

Customers

When

Communicate with customers as soon as you have the list of impacted customers and the draft letter available.

How

Notify customers based on how they have asked to be communicated with by your agency.

Senior Management

When

As soon as the breach team is assembled, the team should be making hourly updates on the first day, with regular updates (as needed) in the following days.

Media

When

The media should be contacted as soon as you have information to release. It may not be everything that you will know at a later time, so you will need to provide updates, as needed.

How

Your agency's Communications office should have a list of key media contacts. This is the list that should be used when sending out a release.

Templates

For draft communication templates, see Appendix A.



APPENDIX A: COMMUNICATIONS TEMPLATES

Customers

Sample Breach Notification Letter

Dear [Name]

[Entity] takes seriously its responsibility to protect information about the individuals it serves. I am writing to inform you of a concern regarding possible unauthorized access of your private information.

On [date], [Entity] discovered that [description of the issue/what occurred]. The records included [description of data].

OPTIONAL: At this time, your data has not been used inappropriately; rather, we have determined that your data could have been viewed by an unauthorized person.

The [description of issue] was immediately corrected upon discovery.

Upon completion of our investigation, you have the right to receive a report on the facts and details of the investigation. If you would like a copy of the report, please contact us to request delivery of the report via mail or email.

We recommend that you take precautionary measures to protect yourself, such as accessing and monitoring your personal credit reports. Under federal law, you have the right to receive, at your request, a free copy of your credit report every 12 months from each of the three consumer credit reporting companies. A credit report can provide information regarding those who have received information about your credit history within a certain period of time. You may request a free credit report online at www.annualcreditreport.com or by telephone at 1-877-322-8228.

When you receive your credit reports, check for any transactions or accounts that you do not recognize. If you see anything you do not understand, call the telephone number listed on the credit report or visit the Federal Trade Commission's Web site on identity theft at <http://www.consumer.gov/idtheft/>.

[Entity] deeply regrets that this occurred and apologizes for any uneasiness and inconvenience this may cause you. If you have any questions, please contact [name, address, email, phone].

Sincerely,

[NAME]

Media

Draft Initial Media Release

[Agency] announces [number of customers] affected by unauthorized access to systems

St. Paul, Minn. ([MONTH DAY, YEAR]) – [Insert agency here] has learned that our [name of system] was unlawfully accessed. Information may have been compromised, including [specific information]. This does not include [information that was not compromised].

The incident occurred [date or date range]. While our forensics experts cannot verify the information that was actually compromised, we believe it is generally [type of data], affecting [number of customers] customers.

We contacted [law enforcement agency contacted] when we learned of this situation and they immediately began an investigation. While we believe this is an isolated incident, we continue to investigate this internally, as well. [Executive quote here about what steps have been taken to assure this type of incident does not happen again].

We also have notified affected customers about the incident. We are offering them a free, [length of time] subscription to a credit monitoring service. “We regret the inconvenience that this incident this may cause to our customers,” said [Executive Name].