

What is data?

In your job at the University, you use, share, and store information and data every day. Data can exist in many forms, e.g., written, verbal, and electronic, and can be used in a variety of ways. Following are examples of University data:

- Information collected, stored, or reported for any purpose, in computer or paper files.
- Information included in financial transactions, lists, reports and records.
- Information about people, classes, projects, or processes.

The data you need and use to do your job at the University is a valuable University asset and must be protected appropriately.

What data is private and what data is public?

The University collects and maintains a variety of information, including information about its students, faculty, staff and others. This information is collected in order to conduct University business. Information is classified as private or public based on federal and state law.

Private information (e.g., Social Security Number, birth date, credit card numbers) can only be released to the subject (i.e., owner) of the information and to those within the University who have a legitimate need-to-know, outside agencies or departments with the subject's written permission, and others as allowed by law.

Public information is available to anyone who requests it, except when a student has requested that no public information about him/her be released without express written permission

For a list of what is public and private data, visit:
http://privacy.ahc.umn.edu/pub_pri_info.html

Do not store University private data on a laptop, PDA or flash drive. These devices are very easy to lose or steal. Staff should assume that these devices can be lost or stolen. Private data should only be stored on a secure server.

What is the University policy on private data?

State and Federal laws define and classify private and public data. University data security policies and procedures apply the laws and provide standards and guidelines for maintaining the confidentiality, integrity, and availability of private data.

For information on University-wide information technology policies, go to:

<http://www1.umn.edu/oit/policies/index.html>

How do I secure private data?

Physical Environment

To secure the physical environment, you should:

- Lock your office or work area when you leave for extended periods of time to restrict physical access to your computer.
- Secure laptops to your desk with a cable lock whenever possible.
- Keep paper files containing private data in locked file cabinets or in locked offices.
- Retrieve print-outs and faxes that contain private data immediately.
- Turn off computers that are unused for extended periods of time.
- Always dispose of documents containing private information by shredding or placing in secure, confidential recycling bins.
- Adjust your monitor or use a screen filter to protect private data from prying eyes.
- If required in your area, wear your security identification badge.

Technical Environment

To secure your workstation, you should:

- Use strong passwords and never share them with others.
- Get assistance from technical support staff before changing computer settings.

To secure your workstation, your technical support staff should:

- Install anti-virus software and set it to update automatically.
- Install a password-protected screen saver.
- Turn on automatic updates to keep computer operating systems (e.g., MS Windows®, MAC OSX®) current.
- Enable automatic updates for other software such as Adobe® Acrobat®.
- Enable a firewall for your operating system.

Work Processes

To incorporate security into your work processes, you should:

- Learn and apply University policy and procedure requirements.
- Update your knowledge of safe computing practices. Stay smart!
- Understand the risks associated with an inadequately secured work area.
- Be discreet when leaving messages about private matters.
- Always report security violations to your technical support staff, your supervisor or the appropriate University office.



How do I report a security violation?

Reporting Data Security Incidents

- Contact your technical support staff or supervisor.
- Contact abuse@umn.edu or call the Central Help Desk at 1-HELP (612 301 4357).

Reporting a lost/stolen or found device (e.g., PDA, laptop) or electronic storage media

If a portable device or electronic storage media that contains sensitive data is lost or stolen, or if you find any abandoned laptop, PDA, or flash drive, notify your supervisor and your area IT Help Desk. They will file a police report and notify OIT Security. This is in accordance with the reporting procedures that are defined in the USIS Security of Sensitive Data policy.

How do I secure my home computer?

If you use your home computer to access University of Minnesota systems, it is important to keep your computer secure and to regularly patch and update your software as needed.

For more information on securing a personal machine, go to: <http://www.safecomputing.umn.edu>

How do I stay secure using E-mail?

- Never open an e mail attachment from an unknown source. If you know the sender but it seems suspicious, you may want to contact the sender to verify the attachment before opening.
- Do not use non-University provided e mail accounts to send University-related information.

How do I stay secure using the internet?

- Be suspicious of any e-mail with urgent requests for personal financial information. Don't use the links in an e mail to get to a web page. If you have an account, go to the website directly.
- Don't believe everything that you read. Be skeptical. Check it out before acting on any information (www.snopes.com is a good resource). Treat websites and every new person you encounter on the Internet as a stranger.

Helpful web sites & contacts

www.safecomputing.umn.edu

onguardonline.gov

www.staysafeonline.org

www.spybot.info/en/index.html

www.ftc.gov/spam/

www.ahc.umn.edu/privacy/

www.umn.edu/privacy

Privacy & Security Office

612-624-7747

privacy@umn.edu



DATA PRIVACY and SECURITY

A Message From the President



The information we gather, use, and share at the University, whether for research, outreach, clinical care, or education, is a valuable University asset. Because this information is so important to those we serve and so vital to our work, it is imperative that we maintain the highest standards to secure the confidentiality and integrity of private information, and the availability and integrity of public data. Learning and incorporating good data management practices in the work we do every day ensures the value of the information we use, and it keeps the trust we have earned in the communities we serve.

Learning to manage data appropriately and securely is part of our shared responsibility.