SENSITIVE

Computer Data

Whose data are *you* protecting?

- Prospective Students
- Current Students
- Past Students
- Alumni
- Continuing Education
- Prospective Employees
- Current Employees
- Past Employees
- Your own personal data

What data are *sensitive?*

Any data protected by FERPA, HIPAA, or any other legislated act. Here are some examples (this is not the entire list of data considered sensitive):

- THE BIG THREE:
  - Name
  - Social Security Number
  - Date of Birth
- STUDENT DATA
  - Grades data
  - Degree data
  - Registration (including transcript data)
  - All Financial Aid data
- GENERAL DATA
  - Mother's maiden name
  - Bank ISO and credit card numbers
  - Addresses
  - Health history
  - Giving history
- EMPLOYEE DATA
  - Race
  - Sex
  - Veteran Status
  - Disability
  - Leave information
  - Medical or health insurance
  - Disciplinary information
  - Performance evaluations

IS&T can help...

IS&T is committed to providing the tools required to help maintain data security. If you have sensitive data, store it on the secured network server provided by IS&T for this purpose. If you do not currently have secure network server storage available, please contact us to discuss your needs.

Questions about sensitive data security?
Contact Michael Holstein, Manager, Data and Network Security
Phone: 216-875-9662
Email: michael.holstein@csuohio.edu

General Policy for University Information and Technology Resources:
www.csuohio.edu/offices/ist/technologypolicies/UniversityInformationandTechnologyResourcesGeneralPolicy.pdf

Technology Policies:
www.csuohio.edu/offices/ist/technologypolicies

Rev. 05/14

FACULTY & STAFF

University Data and Your Responsibility

Faculty and staff guide to responsible data use and security

engaged learning™

Cleveland State University
Information Services and Technology

Your Responsibilities

1. Know and understand the Technology Resources General Policy and the Technology Policies
2. Understand what data are sensitive
3. Do not provide sensitive data for other departments or individuals
4. Report policy violations
5. Enforce data security in your area

NEVER

- Store social security numbers and/or birthdates on your computer.
- Store sensitive student or employee data, especially social security numbers and birthdates, on any department computers (servers, desktops, laptops, PDAs, CDs, or USB drives).
- Email files containing sensitive data.
- Request social security number and/or birthdate on web forms unless authorized by a data custodian and transmitted on a secure web connection approved by the Manager, Data and Network Security.
- Assign students or student employees query or download ability to sensitive data files.
- Share your password.
- Authorize your staff to access sensitive data unless it's absolutely required.
- Provide sensitive data to another staff member.

ALWAYS

- Store sensitive data on the IS&T provided network server.
- Password protect files in those rare instances when they must be emailed (no social security numbers or birthdates).
- Become authorized and knowledgeable on how to obtain sensitive data from the system.

PREVENTIVE MEASURES

- Keep your laptop computer in a locked cabinet when not in use to make it harder to steal.
- Use security lockdown devices to make it harder for people without the correct tool to open the casing to steal parts (but check with IS&T that this does not affect the warranty).
- When you go out, always lock the door – even if you are just going out for a short time.

ACCOUNTABILITY

Everyone that uses sensitive University data must be authorized to do so. Data should never be provided to anyone other than by officially designated University departments. Being able to access sensitive data does not give you the authority to provide this data to others.

If there is a legitimate need for you to review student or employee information and you are not authorized, contact the owning department (Registrar, HRD) with your request. Access will be granted after the appropriate paperwork is completed.