# SECURITY AWARENESS POLICY PC 11.11

## POLICY STATEMENT

It is the responsibility of all employees of the University to protect sensitive data against loss or theft. Awareness, education and practice of the following procedures can assist in this matter. These procedures are in place to help protect employees, customers, contractors and the university from damages related to the loss or misuse of sensitive information.

This document refers to securing sensitive data and physical hardware within an office environment or mobile environment where data may be referenced (at home or on a laptop). It is not meant to address electronic data stored on university servers.

## PROCEDURES

**Goals**

In order to effectively protect and secure university data, the following goals have been established:

1. Educate users on cyber safety
2. Educate users on computer security
3. Educate users on secure office environment
4. Educate users on sensitive data

**Cyber Safety Resources** Employee awareness and education is an integral part of securing sensitive data for the university. The following resources will be available to all employees:

1. Annual mandatory cyber security training
2. Cyber Safety website
3. Monthly Cyber Safety newsletters
4. Computer Virus and Malware Policy

**Computer Security Resources**

Employee awareness and education is an integral part of securing your GVSU computer. The following resources will be available to all employees:

1. Email Policy
2. Acceptable Use Policy
3. Confidentiality, Data & Security Policy
4. Setting Strong Passwords
5. Using Password Managers

**Secure Office Resources**

Employee awareness and education is an integral part of securing a GVSU office. The following security practices should be followed within office suites, individual offices, workrooms and mobile locations where sensitive data may be referenced:

1. Keys or keycards used for access to sensitive data should not be left unattended
2. Passwords should not be shared or written down and left in accessible locations
3. If you have a student that will regularly be using your machine, contact the helpdesk and request a staff account for that student (Do NOT give out your password)
4. Passwords should not be common information such as date of birth, names of children, pets, telephone numbers, etc.
5. When you leave your workstation, lock your computer screen
6. Secure laptops, USB drives, external drives, etc. when unsupervised. Sensitive data, including personal identifiable information, should not be stored on portable media devices.
7. Contact the IT Helpdesk when a computer is to be transferred to a new user. IT will clean the computer, removing previous data and place a clean image on the machine.
8. Printouts containing sensitive data should be removed from network printers immediately and filed appropriately in secure cabinets
9. Dispose of sensitive data on hard copy by shredding immediately
10. All staff should be responsible to watch for or listen to any unusual activity and to be cognizant of their surroundings.
11. Departmental front desk staff should confirm identity of all visitors (GVSU staff/student workers or non-GVSU employees) who are entering their area(s)
    a. Employees (including student workers) should confirm what unit someone is from and the purpose of their visit
    b. Employees (including student workers) should confirm meeting prior to allowing staff member/student employee to proceed within their departmental areas
    c. Confirm with the GVSU employee they are scheduled to meet
    d. Non-GVSU employees must be escorted to/from meeting area/work area
    e. Request ID if necessary

**Sensitive Data**

Sensitive data can be distributed via hard copy or electronic means within an office. Sensitive data includes but is not limited to the following items, whether stored in electronic or printed format:

- All personally identifiable information and FERPA protected data*
- Credit card number (in part or in whole)
- Credit card expiration date
- Cardholder name
- Cardholder address
- Social Security Number
- Business Identification Number
- Employer Identification Number
- Paychecks
- Paystubs

- Benefit information
- Giving information/history
- Health information
- Content of external grants or contracts
- Passport Number

**Securing hard copy sensitive data:**

- Lock cabinets containing sensitive data when not in use or when away for extended periods of time
- Storage rooms containing sensitive data should be locked at the end of the day or when unsupervised
- Desks, workstations, common work areas, printers, and fax machines should be cleared of all sensitive data when not in use
- Whiteboards, dry erase boards, writing tablets, etc. should be erased, removed or shredded when not in use
- Documents to be shredded should be done so immediately or locked up until shredding can occur
- At the end of the day, all sensitive data should be in a locked drawer or cabinet

**Securing electronic sensitive data**

Please contact Information Technology if there are questions/concerns in how you are storing/sharing sensitive data electronically.

- Refrain, when possible from storing sensitive data on your personal computer hard drive or any external personal devices. Instead use the network drive space.
- If storing sensitive data is required on your personal computer hard drive or an external device, encryption and password protection should be applied.
- Engage the screensaver when workspace is unoccupied.
- Computer workstations should be shut down completely at end of work day.
- Lock laptop or external devices containing sensitive data when not in use.
- Make certain data and/or computer work station screens are not visible to the public (e.g. - near windows, entry/exit doors, etc.)
- If email is used to share sensitive data, encryption and password protection should be used. The following statement should accompany the body of the email:
  "This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited."

*See information regarding FERPA data at www.gvsu.edu/registrar and click on Academic Policies and then FERPA.

**GVSU Security Framework References**

- NIST ID.GV-1; PR.AT-1; PR.AT-3; PR-AT-4; PR-AT-5