SECURE OFFICE PROCEDURE

SLT 11.11

Date of Last Update:
April 19, 2015

Approved By:

- Senior Leadership Team

Responsible Office:
Information Technology

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:

a) Create, distribute and annually review the “Secure Office Procedure” document
b) Train all staff members whose jobs relate to sensitive data on both the “Secure Office Procedure” and Information Security Best Practices
c) Train departmental managers to be aware of the importance of the procedures and the need to enforce them

Staff Training

Employee awareness and education is an integral part of securing sensitive data for the university. The following procedures will be enforced to ensure proper training:

a) Upon hire, the Secure Office Procedure and Setting Strong Password documents are emailed to the new employee Secure Office Procedures Page 2 of 4
b) Secure Office Procedure and Setting Strong Password documents are sent annually to all employees via email
c) Internal training, specific to each area, will be provided to employees who have access to sensitive data
d) Information Technology will provide Best Practices information at IT seminars and offer to attend annual departmental meetings to cover the below topics:

i. Awareness of Social Engineering schemes

ii. Secure Office Procedures

iii. Strong Password creation

iv. Data storage

v. Data encryption

vi. Backups

vii. Anti-virus and Anti-spyware tools

viii. Non-secure technologies

GENERAL OFFICE SECURITY PRACTICES

The following procedures should be followed within office suites, individual offices or workrooms and mobile locations where data may be referenced:

a) Keys or keycards used for access to sensitive data should not be left unattended
b) Passwords should not be shared or written down and left in accessible locations
c) If you have a student that will regularly be using your machine, contact the IT Service Desk and request a staff account for that student. (Do NOT give out your password)
d) Make certain passwords aren't common information such as date of birth, names of children, pets, telephone numbers, etc.
e) When you leave your workstation, lock your computer screen
f) Lock up laptops, USB drives, external drives, etc. when unsupervised
g) Contact the IT Service Desk when a computer is to be passed to a new user. IT will clean the computer, removing previous data and place a clean image on the machine.
h) Printouts containing sensitive data should be removed from networked printers immediately and filed appropriately in secure cabinets
i) Dispose of sensitive data on hard copy by shredding immediately
j) Departmental front desk staff should confirm identity of all visitors (GVSU staff/student

workers or non-GVSU employees) who are entering their area(s)

i. Employees should feel comfortable requesting what unit someone is from and the purpose of their visit

ii. Employees should feel comfortable confirming meeting prior to allowing staff member/student employee to proceed within their departmental areas

iii. Confirm with the GVSU employee they are scheduled to meet

iv. Non-GVSU employees must be escorted to/from meeting area/work area

v. Request ID if necessary

vi. Provide front office staff the ability to view your calendar or print a schedule of your meetings in advance so they will expect attendees

k) All staff should be responsible to watch for or listen to any unusual activity and to be cognizant of their surroundings.

Sensitive Information

Sensitive data can be distributed via hard copy or electronic means within an office. When given the choice, store data electronically versus printing a hard copy. Consider scanning a document to store it electronically versus hard copy.

a) “Sensitive information” includes but is not limited to the following items, whether stored in electronic or printed format:

i. All FERPA protected data*

ii. Credit card number (in part or in whole)

iii. Credit card expiration date

iv. Cardholder name

v. Cardholder address

vi. Social Security Number

vii. Business Identification Number

viii. Employer Identification Number

ix. Paychecks

x. Paystubs

xi. Benefit information

xii. Giving information/history

xiii. Health information

xiv. Content of external grants or contracts

b) Securing hard copy sensitive data:

i. Lock cabinets containing sensitive data when not in use or when away for extended periods of time

ii. Storage rooms containing sensitive data should be locked at the end of the day or when unsupervised

iii. Desks, workstations, common work areas, printers, and fax machines should be cleared of all sensitive data when not in use

iv. Whiteboards, dry erase boards, writing tablets, etc. should be erased, removed or shredded when not in use

v. Documents to be shredded should be done so immediately or locked up until shredding can occur

vi. At the end of the day, all sensitive data should be in a locked drawer or cabinet

c) Securing electronic sensitive data. Please contact Information Technology if there are questions in how you are storing/sharing sensitive data electronically.

i. Refrain, when possible from storing sensitive data on your personal computer hard drive or any external personal devices. Instead use the network drive space.

ii. If storing sensitive data is required on your personal computer hard drive or an external device, encryption and password protection should be applied

iii. Engage the screensaver when workspace is unoccupied

iv. Computer workstations should be shut down completely at end of work day

v. Lock laptop or external devices containing sensitive data when not in use

vi. Make certain data and/or PC work station screens are not visible to the public (e.g.- near windows, entry/exit doors, etc.)

vii. If email is used to share sensitive data, encryption and/or 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 FERPA