Issue Date: xx/xx/xxxx | Review Date: xx/xx/xxxx

University of Wisconsin Colleges and University of Wisconsin-Extension Organization-wide Information Security Policy

1. Introduction

Protection of sensitive information is governed by a combination of federal and state laws, UW policies, and consumer Payment Card Industry (PCI) standards. UW Colleges (UWC) and UW-Extension (UWEX) have a legal obligation to prevent unauthorized access to sensitive information under these laws, policies and standards.

The Organization-wide Information Security Policy serves this purpose by informing UWC campuses, UWEX divisions, employees, senior officials/administrators, and contractors of their obligation to protect sensitive information and by specifying adherence to organizational procedures delineating how they must respond to the potential loss or compromise of sensitive information. Good governance involves identifying significant risks to the institutions – such as potential misuse, leak, or loss of personal information – and ensuring appropriate controls are in place to mitigate these risks. The benefits of good protection controls of sensitive information include maintaining trust with citizens and noncitizens; protecting valuable data on the institutions' customers, students and employees; enhancing creditability and promoting confidence and goodwill; and sustaining relationships with donors of nonprofit organizations by respecting the privacy of their information. This Policy also provides for individual accountability to create an incentive for compliance, thus ensuring the effective implementation of the Policy.

1.1. Purpose

The purpose of this Policy is to establish requirements, procedures and protocols that must be followed by all employees in handling and safeguarding sensitive information and the systems on which it is maintained. This document also outlines the roles and responsibilities for employees and delineates and defines sensitive information and related terms.

1.2. Objectives

The objectives of this Policy are to do the following:

1.2.1. Outline basic security needed in handling and safeguarding sensitive information.

1.2.2. Specify the procedure to be followed when an information security breach is suspected or confirmed.

1.2.3. Outline the information security roles and responsibilities for employees, managers, response teams, and other parties responsible for the organization's sensitive information.

1.2.4. Outline information security awareness training requirements.

1.3. Scope

Attacks on University information technology (IT) resources are infractions of the Acceptable Use Policy constituting misuse, or they may be vandalism or other criminal behavior. Reporting information security breaches occurring on the institution's systems and/or networks to appropriate authorities is a requirement of all persons affiliated with the institution in any capacity, including staff, students, faculty, contractors, visitors, program participants, and alumni. Suspected or confirmed information security breaches must be reported to University authorities.

1.4. Applicability

This Policy applies to all institution personnel at UWC and UWEX, including campuses and divisions, employees, management, contractors, student interns, limited term employees, project employees, program participants, visitors, and volunteers.

1.5. Authority

The policies and procedures are based on applicable laws, applicable industry standards, and UW System directives.

1.5.1. Federal laws:

- Federal Trade Commission Act
- Fair Credit Reporting Act
- Gramm-Leach-Bliley Act
- FTC's Disposal Rule
- Other federal laws (HIPAA, FERPA)

1.5.2. State laws:

- Wisconsin Act 138
- Wis. Stats. s. 895.507
- Wis. Stats. s. 134.98

1.5.3. UWC and UWEX Information Technology Resources Guidelines:

- Information Infrastructure Guide
- Appropriate Use Policy http://uwex.uwc.edu/it/policies/use.cfm

1.5.4. UW Board of Regents policies:

- 25-3 Policy on Use of University Information Technology Resources
- 21-4 Identity Theft Detection, Prevention, and Mitigation

1.5.5. Payment Card Industry (PCI) Security Standards Council:

- PCI Data Security Standards

1.6. Enforcement

Failure to comply may result in disciplinary action as provided under existing procedures applicable to students, faculty, and staff, or civil or criminal prosecution.

2. Definition

2.1. Sensitive Information

UWC and UWEX collect certain sensitive Information that must be handled in accordance to the kind of information it is and what laws or standards apply. In general, information obtained by UWC and UWEX may be subject to Open Records Law requests unless the information or documents (or portions thereof) are exempt from disclosure as specifically enumerated in the applicable statute, UWC or UWEX or UW System policy, and professional code, or practice within the applicable unit. Items may also be exempt from Open Records Law requests if they contain information that affects UWC or UWEX security measures or financial data.

For the purpose of the Policy, the following are considered sensitive information and are not subject to Open Records Law disclosure:

2.1.1. Institutional data is defined as Restricted Data by law (such as Wisconsin Act 138) because the data could, by itself or in combination with other such data, be used for identity theft, fraud, or other such crimes.

2.1.2. Wisconsin Act 138 defines sensitive information as individually identifiable information. Personal Identifiable Information (PII) is any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the U.S. PII includes:

- Individual’s social security number
- Individual’s date of birth
- Individual’s driver’s license number or state identification number
- Individual’s financial/banking information (such as account number, including a credit or debit card account number or any security code, access code, or password that would permit access to the individual’s financial account)
- Individual’s tax information
- Individual’s deoxyribonucleic acid (or DNA) profile, as defined in s. 939.74 (2d) (a)
- Individual’s unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation

2.1.3. Public disclosure restrictions are imposed on the following information as well:

- Student educational records including grades, identification number, etc.
- Information in medical records such as health, medical or psychological information
- Employment information including identification number, home address, retirement account allocations and investments and designations of beneficiaries, garnishments, tax levies, wage assignments
- Information from a consumer report
- Individual’s passport numbers, alien registration numbers or military ID.

2.1.4. Institution data, whose public disclosure is restricted by law, contract, UWC or UWEX policy, professional code, or practice within the applicable unit, discipline, or profession.

- Documentation of grievance, arbitration, and disciplinary proceedings
- Human subjects research information, if the subjects have been promised anonymity
- Information about pending research misconduct proceedings
- Trade secrets or other proprietary business information owned by a third party and provided to the institution upon a promise of confidentiality for the conduct of research, testing, or training, or in connection with a potential investment or transfer of technology by UWC or UWEX. Information includes proprietary databases, business processes and methods, strategic plans and marketing programs, proprietary computer software program, manufacturing processes, etc.
- Proprietary computer applications or source code to which UWC or UWEX holds a license that restricts further or public distribution
- Exam questions and answers/scoring keys until distributed by the professor
- Bids and proposals until they are opened or the deadline for their submission has passed
- Financial aid applications and related tax and financial information
- Information and records protected by the attorney-client privilege
- Law enforcement investigation records
- Private financial data, and other information disclosed under the University's conflict of interest policies

2.1.5. Records of the University's security measures.

- Passwords for access to University facilities or computer systems
- Security codes and combinations for locks
- digital keys and passcodes, digital signature
- Security plans
- Security procedures
- Threat assessments and preparedness strategies
- Law enforcement deployment plans
- Operational instructions for emergency personnel and law enforcement officers.

2.1.6. Institutional data whose value would be lost or reduced by disclosure in advance of the time prescribed for its authorized public release, or whose disclosure would otherwise adversely affect the University financially.

- Research data or results prior to publication or the filing of a patent application
- Non-patentable technical information or know-how that enhances the value of a patented invention or that has independent commercial value
- Information relating to the University's intention to buy, sell, or lease property whose disclosure could increase the cost of that property for the University or decrease what the University realizes from that property (like real property appraisals)
- Computer applications to which the University owns the source code

2.2. Assessing Risk

Understanding the four major areas of risk assists in implementing the appropriate level of controls. Questions for the four areas are:

- Legal and organizational risks – What are the regulatory penalties for mishandling protected data? What legal recourse would the impacted individuals have? Is there a plan in place to respond to a privacy incident?
- Infrastructure risks – How the protected information flows in and out of the organization? How the information is transmitted/transferred? How many times the data is converted from one form to another? Was the data being transferred or copied and whether the post-transfer residual data is treated with the same set of rules as the originating data? Are shredders, encryption, locked vaults and lockers used as countermeasures to leaking data?
- Application risks – Who and what handles the information? Were privacy issues identified in the requirements defining the application?
- Business process risks – Was the data used for its intended purpose? Did measures to protect printed information follow the same principles used to protect electronic data? Was the desk clean? Drawers and filing cabinets locked?

2.3. Information Security Breach

A breach in security is defined as an unauthorized acquisition of information for which the institutions (UWC and UWEX) have a duty to protect. The information is typically maintained in an electronic format by the institutions. For purpose of this Policy, a suspected information security breach has occurred when any employee has reason to believe a university-owned and managed information system has been accessed by unauthorized individuals, or when an employee has reason to believe confidential information has been disclosed to a person not authorized to receive it.

2.4. Notice Triggering Incident

In March 2006, Wisconsin’s Personal Information Disclosure Act (statute Section 134.98), was passed. The Act requires an entity, including government agencies, to notify the subject of personal information if an unauthorized acquisition of their personal information has occurred.

3. Roles and Responsibilities

Sensitive information protection can be considered a process of establishing an appropriate balance between privacy and multiple competing interests. To minimize intrusiveness, maximize fairness, and create legitimate enforceable expectations of privacy, the sensitive information protection program must consider the following roles:

3.1. Roles

Roles to consider are as follows:

- Data subject - Individual whose personal data is controlled.
- Data controller – Campus or department controlling the sensitive data.
- Privacy officer – An institution’s privacy oversight and contact function.

- Privacy commissioner – The governmental oversight authority, usually on the federal or state level.
- Service providers – In circumstances where third parties are involved in data processing.

3.2. Sensitive information control principles

Information security is everyone's responsibility. The UWC and UWEX community is responsible for understanding the risks, threats, costs and incidents associated with securing information. The following is a set of principles governing the processing of sensitive information:

3.2.1. Accountability – A department is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the department's compliance with this set of principles.

3.2.2. Identifying purposes – The purposes for which personal information is collected shall be identified by the department at, or before, the time the information is collected.

3.2.3. Consent – The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

3.2.4. Limiting collection – The collection of personal information shall be limited to that which is necessary for the purposes identified by the department. Information shall be collected by fair and lawful means.

3.2.5. Limiting use, disclosure and retention – Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information must be retained only as long as necessary for the fulfillment of those purposes.

3.2.6. Accuracy – Applications and employees will use measures to assure personal information is recorded accurately and that errors are corrected in a timely manner.

3.2.7. Safeguards – Personal information shall be protected by security safeguards that are appropriate to the sensitivity of the information.

3.2.8. Openness – The organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

3.2.9. Individual access – Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

3.2.10. Challenging compliance – An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the department's compliance.

3.3. Responsibilities

3.3.1. Executive/Management (Chancellor, Vice-Chancellors, Deans)

- Approve Organization-wide Information Security Policy
- Provide training opportunities for work force on their roles and responsibilities in protecting sensitive or restricted information
- Enforce sanctions

- Designate Privacy Officer or Committee and/or Risk Management Director

3.3.2.Chief Information Officer & Central IT

- Responsible for all IT functions within the institution to support UWC and UWEX's goals and missions
- Develops IT infrastructure that meets all applicable federal and state laws as well as other industries such as ISO/IEC 27002, Payment Card Industry and others regarding information security management
- Defines standards and architectures for implementation across the institution's departments, divisions, campuses, and service providers
- Develops processes and practices supporting the flow of information stored in computerized systems to ensure adequate information security
- Develops and maintains security controls to protect sensitive information from unauthorized disclosure.
- Develops plans to ensure that IT services can recover and continue should a serious incident or disaster occur
- Develops and maintains enterprise-wide Wide Area Network and firewall infrastructure.
- Develops and maintains enterprise-wide services, applications and solutions
- Develops and maintains the enterprise data center(s)

3.3.3.Information Security Officer

- Develops and maintains the Organization-wide Information Security Policy and corresponding standards, policies and procedures
- Reviews Policy annually to determine if security standards, policies, and procedures continue to be suitable, adequate and effective
- Coordinates and implements policy compliance throughout the institution's departments or campuses
- Oversees/coordinates training in support of the institution's security policies
- Ensures compliance with all federal, state, and university regulatory and PCI requirements
- Act as the Critical Incident Management Team lead

3.3.4.Legal Counsel

- Provide guidance on laws and regulations impacting information security

3.3.5.Internal Auditor

- Evaluate framework on sensitive information security based on laws, regulations, rules and other standards in which UWC and UWEX must operate
- Measure and assist with compliance of the institution's data protection system
- Increase the level of data protection awareness among management and staff
- Provide information for a data protection policy review
- Identify significant risks on information security and provide appropriate recommendations for their mitigation
- Conduct annual risk assessments of all policies and practices relating to protecting sensitive or restricted information

3.3.6.IT staff

- Implement security policies and procedures to prevent unauthorized access to confidential and sensitive information
- Where applicable, install and maintain perimeter firewalls to protect confidential and sensitive information
- Follow written procedures for the following: change control for system and software configuration, data retention and disposal, encryption, intrusion detection mechanism, anti-virus mechanism
- Coordinate information security activities with Information Security Officer and Central IT
- Identify security requirements that must be fulfilled before granting external party (including customer, vendor) access to the institution's information systems
- Secure third party confidentiality or non-disclosure agreement to ensure compliance with all appropriate security requirements.
- Change vendor-supplied default system passwords and other security parameters when deploying new systems.
- Regularly test security controls, limitations, network connections, and restrictions to ensure unauthorized access attempts are identified and prohibited.
- Use port scanner to detect any unwanted services running on the network or any port open in each system.

3.3.7.Supervisors

- Understand all the institution's policies regarding handling sensitive or restricted information and answer questions from employees on the subject
- Implement security policies and procedures
- Limit access to sensitive or restricted information to employees with a legitimate business need.
- Limit employee access to offsite storage facilities
- Conduct background checks upon employees before providing them access to personally identifiable information
- Remove employee access to sensitive or restricted information immediately following termination of employment, or transfer to another work group, department, or campus. Expire user accounts and collect access keys and identification cards as part of the employee check-out or exit process
- Ensure employees are following all institution's policies and procedures as part of employee's performance evaluation
- Consult the Chief Information Officer, Information Security Officer, Controller, Records Officer, Internal Auditor or Human Resources Managers if there is a question about sensitive or restricted information security

3.3.8.Employees

- Employees include management, supervisors, student interns, limited term employees, project employees, and volunteers
- Properly use the tools each computer system provides for maintaining the security of stored information
- Understand and follow the Organization-wide Information Security Policy
- Understand and accept responsibilities for identifying, transmitting, redistributing, storing or disposing of sensitive or restricted information
- Understand and comply with all applicable laws, rules and UW System's policies as well as this policy to keep sensitive or restricted information secured and confidential at all times
- Consult with their supervisor if there is a question about this policy
- Seek appropriate approvals if an exception to this policy is needed.
- Attend trainings when offered or familiarize themselves with all policies and procedures relating to handling sensitive or restricted information
- Attend trainings when offered to learn how to recognize security threats, suspicious activity and how to report or deal with security vulnerability problems
- Exercise diligence in preventing computer accounts from being used by unauthorized persons
- Notify their supervisor immediately if a potential security breach is suspected, such as a lost or stolen laptop, disclosure or leak of sensitive or restricted information
- Report the misuse or compromise of systems that handle, store or propagate sensitive, restricted or internal information to the Information Security Officer or the Chief Information Officer, Legal Counsel, Internal Auditor, and Human Resources Manager immediately so that all necessary steps can be taken in accordance with all applicable laws

3.3.9.Critical Incident Management Team (CIMT)

The CIMT has the responsibility for coordinating the institution's response to a breach in information security. Members of the CIMT will include the following:

- Information Security Officer (Team Lead)
- Chief Information Officer
- UW Police representative
- Legal Counsel representative
- Internal Auditor representative
- Human Resources representative
- Third Party Vendor representative (when applicable)

4. Handling Request for Sensitive Information

Unauthorized access could be the result of unintentional release of secure information to an untrusted environment. Other terms for this phenomenon include unintentional information disclosure, data leak and also data spill.

Disclosure of sensitive information is prohibited. All employees must follow the procedures below to safeguard sensitive information:

4.1. When responding to a request for access to confidential information, employees should follow the provisions of the open records law and confidentiality requirements that dictate the handling of confidential or restricted information, including personally identifiable information.

4.2. Never give out personal identifying information without fully confirming the source and circumstances.

4.3. Exceptions to these procedures must be authorized by the Chief Information Officer.

4.4. Personally identifiable information (including, but not limited to, the student's social security number/ID number, class schedule, course titles, or meeting times/places, and academic transcript information (grades, credits attempted/earned, GPA, etc.) cannot be released without one of the following:
- Student's prior, written consent
- Written request by certain authorized agencies of the Federal Government (Comptroller General, H.E.W., Education Department) and State of Wisconsin educational authorities
- Authorized request from UW Colleges personnel identified as having a legitimate educational interest
- Authorized request from organizations providing financial aid to the student who is the subject of the request
- Authorized request from accrediting agencies
- Judicial subpoena
- Approval from the Campus Dean or Student Services Director in the event of an emergency when the knowledge of the information, in fact, is necessary to protect the health or safety of the student or other person(s)

4.5. Provide access to enable an authorized UWC or UWEX employee to perform the general and specific job duties outlined in his/her position description.

5. Safeguard Sensitive Personal Information

All employees are responsible for the protection of any sensitive information in their custody. The improper disclosure of sensitive information can cause harm and embarrassment to students, faculty, staff and the University. Breaches of certain sensitive information are subject to fines and/or criminal penalties.

All employees must protect sensitive information in its many forms such as electronic, printed, voice, microfiche, etc. Below are a few guidelines that will help in the protection of sensitive information.

5.1. General Safeguards

5.1.1. Do not collect sensitive or restricted information such as Social Security Number (SSN) unless there is a legitimate business need for it. Create a unique identifier that does not use SSN. If you collect, use, store, disclose or transmit sensitive or restricted information such as SSNs, contact the Chief Information Officer for written approval or authorization.

5.1.2. Make sure the information is acquired in a safe manner. Based on method of acquisition (such as telephone call, fax, in-person, or internet) determine appropriate safeguard measures as dictated by the organization's policies and standards and/or policies or regulations to which the organization is subject. Do not collect personal identity information including restricted information and passwords via email.

5.1.3. Do not publicly display sensitive or restricted information or leave sensitive or restricted information unattended. Protect printed sensitive data. Store paper documents, files, CDs, floppy disks, zip drives, tapes, and backups that contain personally identifying information in a locked room or a locked file cabinet whenever an employee is not actively working on them. Do not leave sensitive data unattended on a copier, FAX or printer. Logout or lockout computers when you will be leaving them unattended.

5.1.4. Keep a clean and organized desk and file cabinet.

5.1.5. Shred paper copies of sensitive or restricted information when it is no longer needed. Select shredders that are PCI-DSS compliant.

5.1.6. Adhere to applicable written records retention policies, "opt-out" laws, and Wisconsin privacy laws as well as other federal and state laws relating to sensitive or restricted data.

5.2. General Information Technology (IT) Safeguards

5.2.1. Do not use the institution's website(s) to collect personally identifiable information without the user's consent. Assure that any such websites are compliant with the institutions policies for web application security.

5.2.2. Avoid copying or downloading sensitive data from the University's administrative systems to workstation, Web server, laptop, mobile devices, etc. unless absolutely required. Ensure you have permission from your supervisor and that your IT department has installed additional security controls prior to downloading. Consider removing the confidential portion of the information if this is possible (e.g., SSN).

5.2.3. If sensitive information is to be shipped by outside carriers or contractors, encrypt it and prepare an inventory before shipping.

5.2.4. Servers containing sensitive information must be housed in a secure location and operated only by authorized personnel.

5.2.5. Maintaining copies of sensitive information is strongly discouraged and requires approval by the CIO.

5.2.6. Sensitive information should be transmitted across the network in a secure manner (i.e., to secure web servers using encryption with passwords transmitted via secure socket layer, etc.) Do not send sensitive information via email, text, chat sessions, or any other electronic means of communication.

5.3. Perimeter Safeguards

5.3.1. Ensure LAN file servers are protected against unauthorized access.

5.3.2. Ensure access to data centers/server rooms have a physical barrier to protect from unauthorized access. Consider the following:

- Natural barriers like landscape and terrain, fencing type and construction, wall and ceiling construction at high risk areas
- Card controlled entry gates
- Staffed reception, door and window locations and corresponding security devices
- Surveillance and vigilance by employees
- Parking areas including entrance/exit and access to facility
- Frequency of patrols and security checks

5.3.3. Adequate entry controls in place to allow only authorized personnel into various areas within the organization such as:

- Closed circuit television
- Electronic locking devices such as card access, electromagnetic locks
- ID badges
- Alarm systems and anti-intrusion devices
- Key control management and accountability
- Levels of access and authorization
- Other types of access controls including sign-in/sign-out logs

5.3.4. Offices or rooms that house information processing services should have approved locks,as well as have lockable cabinets or safes. Put files away and lock file cabinets and office doors when staff are away from offices and workstations.

5.3.5. Ensure the facility is protected against external and environmental threats such as fire, flood, tornado, and other forms of natural or man-made disaster.

5.3.6. Implement appropriate access controls to the building and to the rooms where sensitive information is kept. Develop guidelines for working in secure areas. Full documentation of all security incidents and violations must be generated, reviewed, and maintained.

5.3.7. Prevent unauthorized personnel from accessing areas where sensitive or restricted information is housed. Identify delivery areas, loading docks, and other areas where unauthorized persons may enter the premises to avoid unauthorized access.

5.4. Equipment Safeguards

5.4.1. Protect equipment to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

5.4.2. Protect equipment from power failures and other disruptions caused by failures in utility provider infrastructure. Utilize permanence of power supplies, such as a multiple power feeds, Uninterruptible Power Supply (UPS), and backup generators if possible.

5.4.3. Protect power and telecommunications cable carrying data or supporting information services from interception or damage. Additional security controls should be in place for sensitive or critical information.

5.4.4. Maintain equipment to ensure high availability, integrity, and quality of service. This includes following supplier's recommended service intervals and specifications. Maintain logs of all suspected or actual faults and all preventive and corrective measures.

5.4.5. Ensure appropriate controls are implemented when equipment is sent off premises or used outside of the premises.

5.4.6. All equipment that contains storage media must be checked to ensure any sensitive information or licensed software is physically destroyed or securely over-written prior to disposal or reuse.

5.4.7. No property may be taken off-site without prior authorization.

5.5. General Electronic/Computer Safeguards

5.5.1. Do not store sensitive or restricted information on any computer with an internet connection unless it's essential for conducting official business and the information is encrypted.

5.5.2. Do not send sensitive or restricted information to third parties over public networks (such as the internet or an email account) unless the information is encrypted or the site is encrypted by a validated certificate (closed padlock in status bar in browser window)

5.5.3. Do not download or copy sensitive information to personal/home computer.

5.5.4. Do not install any unnecessary, unfamiliar, or untested software.

5.5.5. Do not download entertainment programs, applets and images from unreliable and/or unknown sources.

5.5.6. Secure all workstations, laptops, and portable devices. Regularly scan/run up-to-date anti-virus and anti-spyware programs on individual computers, servers and portable devices.

5.5.7. Keep operating systems and Internet browsers updated with the latest security patches.

5.5.8. Ensure use of strong passwords on all workstations, laptops, servers, and portable devices.

5.5.9. Control/limit access to computers that are logged into central servers storing sensitive information (i.e. authenticated logins and screen savers, locked offices, etc.).

5.5.10. Do not access sensitive information resources that are stored on central servers unless there is an official need to access the information and with proper approval.

5.5.11. Do not respond to email-based requests for PII such as 'phishing' attempts.

5.5.12. Prevent unauthorized use of computers that process institution's business.

5.5.13. Avoid using public Internet kiosks or other people's computers to access institution's data.

5.5.14. Take precautions about file sharing. Do not use peer-to-peer file sharing software.

5.6. Mobile Storage Media Safeguards

5.6.1. Do not store sensitive information on mobile computing devices or mobile storage media. If sensitive information must be stored on a mobile device, contact your IT professionals for assistance to ensure proper security settings are in place.

5.6.2. Do not take sensitive information home.

5.6.3. If personal information has been stored on mobile devices, contact your IT professionals to ensure proper disposition of the data.

5.6.4. Take precautions to mitigate wireless networking risks.

5.6.5. Mobile devices must be stored in a secure place. Never leave any of these devices visible in a car, at a hotel luggage stand, or packed in checked luggage unless directed to by airport security.

5.7. Wireless devices safeguards

5.7.1. There must be a legitimate business justification to use a wireless device to connect to the institution's network or to transmit sensitive information.

5.7.2. All wireless and remote access security measures, including encryption, must be implemented by IT staff.

5.8. Contractors or service providers safeguards

5.8.1. Standardized contract language and due diligence processes that specifically address protection of sensitive information must be included in every agreement or contract with outside parties where such data is at risk.

5.8.2. Contractors or service providers must have a clear understanding of the expectation that their information security practices must be comparable to the institution's standards, that they must handle security issues in a similar manner, and that they must notify the institution if there is a problem or breach.

6. Sensitive Information Security Breach

In general, a sensitive information security breach incident may be defined as a deliberate electronic attack on communications or information processing systems. Whether initiated by a disgruntled employee, a malicious vendor, or a misguided hacker, deliberate attacks often cause damage and disruption to organization-wide information systems.

There are state and federal laws and regulations and various contracts that require UWC and UWEX to protect sensitive information from unauthorized access. UWC and UWEX must prepare for security incidents and protect key or sensitive information to minimize the impact an incident might have on business operations.

When a breach is suspected, the Information Security Breach Response Procedure must be followed.

7. Awareness, Training and Education

7.1. Basic Awareness and Education Training

- New employee training – Employee Handbook and the Appropriate Use policy are presented to new employee on the first day.
- Recurring training – All relevant policies, references and practices are discussed at staff meetings and materials are posted on appropriate UWC and UWEX websites.

- Online educational modules – posted on the uwex.uwc.edu website.
- Resources: Contact the Information Security Officer, Chief Information Officer, Controller, Records Officer, Internal Auditor, or Human Resources Managers, or the Office of General Counsel.

7.2. Information Incident Reporting Training

Knowledge needed	End Users of the Unit	Central IT Help Desk	Local/Unit IT staff	Management of the Unit
How to identify suspicious activity or events	Yes	Yes	Yes	Yes
How to preserve evidence	Yes	Yes	Yes	Yes
How to contact local IT staff in a timely manner	Yes			Yes
How to contact Central IT Help Desk in a timely manner (if local IT staff is not available)	Yes			Yes
How to prudently investigate suspicious activity of events to determine whether or not there is a reasonable belief that UWC or UWEX sensitive information may have been accessed by unauthorized persons		Yes	Yes	Yes
How to contact management of the unit regarding a possible information incident	Yes	Yes	Yes	
How to report a possible information incident in a timely manner via the Information Incident Reporting Procedure	May report incidents	Yes	Yes	May report incidents
How to assure that a possible information incident is reported in a timely manner				Yes

8. Glossary

Access – The ability or opportunity to gain knowledge of PII.

Awareness, Training, and Education – Includes (1) awareness programs for training that changes organizational attitudes toward realization of the importance of security and the adverse consequences of its failure; (2) a training purpose, which is to teach people the skills that will enable them to perform their jobs more effectively; and (3) education that is more in-depth than training, targeted for security professionals and those whose jobs require expertise in automated information security.

Computer Security Incident – An incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Control – The authority of the government agency that maintains information, or its successor in function, to regulate access to the information. Having control is a condition or state and not an event. Loss of control is also a condition or state which may or may not lead to an event (e.g., a Privacy Incident).

Institution Personnel – Includes UW Colleges central and campus employees, UW-Extension employees, independent consultants, or government contractors using or with access to UW Colleges or UW-Extension information resources.

Information Technology – Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive

Notice-Triggering Information – Specific items of personal information identified in Administrative Code. This information includes an individual's name in combination with Social Security Number, driver's license/Wisconsin Identification card number, health insurance information, medical information, or financial account number such as credit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Personally Identifiable Information – Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the U.S.

Examples of PII include: name, date of birth, mailing address, telephone number, Social Security Number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), Internet protocol addresses, biometric identifiers (e.g., fingerprints), photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual. See Privacy Impact Assessments, Official Guidance, DHS Privacy Office. Personal information refers to any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history.

Information Security Breach Incident – The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for an other than authorized purpose, have access or potential access to PII in usable form, whether physical or electronic. The term encompasses both suspected and confirmed incidents involving PII which raise a reasonable risk of harm.

.