Office of Compliance and Ethics
UNIVERSITY of WEST FLORIDA

Payment Card Industry Data Security Standards (PCI/DSS) Policies

Wireless access point sweep Policy

On a quarterly basis ITS shall perform a scan for unauthorized wireless access points. The method used will at minimum detect and identify:

- WLAN cards inserted into systems
- Portable wireless devices connected to systems
- Wireless devices attached to open network ports

PCI DSS Security Policy

This policy pertains to full-time, part-time employees, temporary employees and personnel, and contractors and consultants who are 'resident' on UWF property or otherwise have access to UWF cardholder data environment.

This Policy shall be reviewed once a year by the PCI DSS delegate from Financial Services and/or Compliance and Ethics and/or a PCI DSS delegate from Information Technology Services.

The usage of technologies which can access or affect the cardholder environment are governed by this policy.

The only technology allowed to access the cardholder environment are local or remote (in the case of a vendor or business partner) desktop workstations or laptops using hard-wired network connections or a wireless network but only a specifically configured secure virtual private network. The workstations shall employ automatic disconnects of remote-access after 15 minutes of inactivity. Vendor and business partner access shall be managed by approved personnel and will have access privileges rescinded upon termination of use.

Technologies explicitly not allowed to access the cardholder environment are:

- ✗ Open or public (non VPN) Wireless technologies
- ✗ Removable electronic media
- ✗ Laptops
- ✗ Tablets
- ✗ PDAs (Personal Digital Assistants)
- ✗ Smartphones

Exceptions to any of the above technology must be approved in writing (employing the "Request for Significant Change to a Payment Process" form) by a PCI DSS delegate from either Financial Services, Compliance and Ethics, or Information Technology Services.

Reviewed September, 2018

In addition, while accessing and or connected to the cardholder environment the authorized employees shall not attempt and wherever reasonable and possible be prevented via security controls applied to their workstations from doing any of the following:

- ✗ Check personal mail
- ✗ Visit any website not directly associated and pertinent to the maintenance or actions being performed
- ✗ Make Internet or Intranet connections to any resources not explicitly necessary for maintenance or business actions

Approved Personnel Policy

Of the approved technologies, authentication will be asserted through Domain accounts (Microsoft Active Directory).

The PCI DSS delegates from Financial Services, Compliance and Ethics, and ITS shall maintain a list of approved personnel and their devices and the Network locations of these devices.

Information Security Policy

Approved personnel shall adhere to UWF established Information Security Policies and Procedures.

An approved ITS SIRT (Security Incident Response Team) member will be responsible for establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all security related situations in accordance with established SIRT procedures.

A formal security awareness program to make all personnel aware of the importance of cardholder data security shall be established and maintained by ITS and the Compliance Office.

A procedure will be maintained and implemented to manage service providers as outlined in the " Service Providers with Access to Card Holder Data" policy found on the Compliance and Ethics PCI DSS website (https://uwf.edu/offices/compliance-and-ethics/pci-dss-compliance/pci-dss-forms-and-resources/).

Inspection of Devices for Tampering

Approved personnel are required to periodically inspect device surfaces to detect tampering (ex. addition of card skimmers to devices), or substitution (ex. checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). Procedures and best practices will be made available via the Compliance and Ethics PCI D S S Compliance web resource, which will include guidance on:

- Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices
- Understanding to not install, replace, or return devices without verification
- Being aware of suspicious behavior around devices (ex. attempts by unknown persons to unplug or open devices)
- Reporting all suspicious behavior to appropriate personnel (ex. a manager or security officer)
- Reporting tampering or substitution of devices

Incident Response Plan

In the case of a security incident, such as the discovery of a rogue access point or break- in/infection of a system, the SIRT team member assigned PCI DSS duties will follow the established UWF IT Security Incident Process.

What is an Incident?

An IT security incident is attempted or actual:

- Unauthorized access, use, disclosure, modification, or destruction of information
- Interference with information technology operation
- Violation of explicit or implied acceptable use policy or of the Information Security and Privacy Policy

Examples include:

- Compromised user accounts
- Computer system intrusion
- Ransomware infection
- Unauthorized access to, or use of, systems, software, or data
- Unauthorized changes to systems, software, or data
- Loss or theft of equipment used to store or work with sensitive university data
- Denial-of-service attack
- Interference with the intended use of IT resources

Why Report an Incident?

- ITS can help you resolve the incident and recover your account/assets
- It is UWF policy to report IT security incidents; see Information Security and Privacy Policy

Overview of IT Security Incident Response and Reporting

Information Technology (IT) Security Incident Response and Reporting is tied to the principal University goal for information security: preserving the confidentiality, integrity and availability of enterprise information assets. An effective IT Security Incident Response program provides a means of dealing with unexpected circumstances in such a way as to minimize impact to the University. It also provides management with sufficient information on which to base an appropriate course of action. A systematic IT Security Incident Response program utilizing a formal methodology offers several benefits to the University such as:

- Providing a structured, logical approach to use in situations that are usually chaotic
- Increasing the efficiency of dealing with an incident, which reduces the impact to the University from both financial and human resources (HR) perspectives
- Providing evidence of due diligence and forethought that may become significant should legal and liability issues arise following an incident. This is particularly true when dealing with disclosure regulations and compliance with laws

Departmental Responsibilities for Reporting and Responding to an IT Security Incident

Reporting of IT Security Incidents

There are many different kinds of IT Security Incidents and different departments will become involved in the remediation of the incidents. It is the responsibility of the department to report an incident to the appropriate department. Anything considered criminal activity should be reported to the UWF Police. Employee misconduct, both criminal and otherwise should also be reported to Human Resources. ***Incidents of a technical nature usually deriving from an external source should be reported to the IT Security Team (itsecurity@uwf.edu)***. All University data, regardless of the format or medium of the record (paper, electronic data/ voice/ video/ image, microfilm, etc.), should be classified into one of three sensitivity levels categories:

- Level 1 - Protected
- Level 2 - Private
- Level 3 - Public

The data classification level of information involved in an incident is an important component in the process of timely risk mitigation in the response process.

Types of IT Security Incidents Reported to the UWF Police

- Electronic transmission/storage of child pornography
- Electronic transmission of threats to the physical safety of human beings, animals or physical assets
- Harassment and other criminal offenses involving individual user accounts
- Loss or theft of computing device(s)
- Use of UWF computing resources in the commission of fraudulent activity against the University, individual, or outside entity
- Incidents involving a breach of Criminal Justice Information Services (CJIS) information

Types of IT Security Incidents Reported to Human Resources (Employees/Faculty) or Office of Student Affairs (Students)

- Commercial use of IT resources that is not pre-approved
- Advertisements for personal gain on uwf.edu websites
- Use of IT resources that interferes with the performance of an employee's job
- Use of IT resources that result in an incremental cost to the University

Questions/ Concerns:
Matt Packard, CCEP
Chief Compliance Officer
850.857.6070 | mpackard@uwf.edu

Reviewed September, 2018