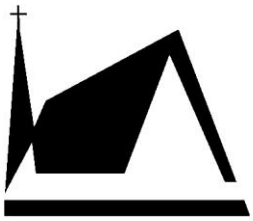
INFORMATION TECHNOLOGY POLICIES AND PROCEDURES HANDBOOK

Concordia Theological Seminary Fort Wayne

Revised December 20, 2019

Revision 2.3.1



Concordia Theological Seminary

Fort Wayne, Indiana

Contents

Concordia Theological Seminary
Fort Wayne, Indiana

Password Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	User Authorization, Identification & Authentication Policy
Related Procedures	
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	July 1, 2015
Next Review Date	February, 2020

Purpose

Passwords are the primary form of user authentication used to grant access to Concordia Theological Seminary's information systems. To ensure that passwords provide as much security as possible they must be carefully created and used. Without strict usage guidelines the potential exists that passwords will be created that are easy to break thus allowing easier illicit access to Concordia Theological Seminary's information systems, thereby compromising the security of those systems.

Scope

This Password Policy applies to all information systems and information system components of Concordia Theological Seminary. Specifically, it includes:

- Mainframes, servers, and other devices that provide centralized computing capabilities.
- SAN, NAS, and other devices that provide centralized storage capabilities.
- Desktops, laptops, smart phones, tablets, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- Firewalls, IDP sensors, and other devices that provide dedicated security capabilities.
- Cloud services, including but not limited to, infrastructure as a service, platform as a service, and/or software as a service.

Policy

1. Passwords must be constructed according to set length and complexity requirements. As such passwords must be at least eight (8) characters in length and must include at least three (3) of the following types of characters: upper case letters, lower case letters, numbers and special characters. While 8 is the minimum acceptable length of a password, you are encouraged to make it longer. It is generally harder to crack longer passwords than shorter ones.

2. Note that certain systems may have stricter criteria defined by the manufacturer or vendor. I.e. myclasses (misclases) enforces at least one of each of the 4 character types be used.)

3. Passwords will have both minimum and maximum lifespans. As such, passwords must be replaced at a maximum of 90 days and at a minimum of seven (7) Days.
4. Passwords may not be reused any more frequently than every five (5) password refreshes. Reuse includes the use of the exact same password or the use of the same root password with appended or pre-pended sequential characters.
5. Passwords are to be used and stored in a secure manner. As such, passwords are not to be written down or stored electronically unless stored in an encrypted, password-protected file with at least 256-bit AES security. Passwords are to be obscured during entry into information system login screens and are to be transmitted in an encrypted format.
6. Passwords are to be individually owned and kept confidential and are not to be shared under any circumstances. This includes, but is not limited to, coworkers, boss/supervisor, supervised persons / administrative assistant / secretary, family members, etc.
7. Users are required to reset their passwords upon first access.
8. Biometric security is an acceptable form of access for the defined systems. Examples of this are computer and Smart Phone Fingerprint Reader and Smart Phone facial recognition.
9. An exception may be made for accounts designated as service accounts (Procedure 3) or single-use stations (Procedure 4). Passwords for these accounts will not be changeable by the user, and may be allowed different lifespans. These accounts are not considered network user accounts, and are restricted to specified machines with limited or no network access.

Procedure 1

Password Vault. Programs should be reviewed and approved by IT. The following programs have been approved provided you are using 256-bit AES security or better.

- WinZip V 12.0 or later
- WinRAR V 4 or later

Password vaults should not be stored with a name indicating that it is a password repository.

Concordia Theological Seminary has reviewed and approved the use of LastPass.

- Requests for LastPass Enterprise access should be made to IT.
- LastPass allows for free personal vaults. Users are allowed to link their personal account to the enterprise account. Seminary account information **may not** be stored in a personal vault.
- Individuals should maintain a personal security score of 70% or higher. You can test your score by clicking on the Security Challenge link in LastPass.
- Master Passwords must have a score of 100%.

Procedure 2

In certain circumstances, you may need to allow somebody other than yourself access under your ID, (i.e. IT Help Desk tech troubleshooting an issue on your computer). In such circumstances, you should remain in attendance until control of your account is returned to you

Procedure 3

Service accounts with non-expiring passwords will have a fully random password consisting of a mix of upper & lower case, numbers and special characters with a length of at least 24 characters (or maximum allowed if system maximum is less than 24 characters).

Procedure 4

Single-use stations are workstations designated for a specified purpose, but used by multiple people. These computers will have limited or no network access, and where possible connect to a separate VLAN. These stations may be assigned an ID that is solely for the station use. The same ID can be used for multiple workstations of the same designation, but may not be used across different purposes. Examples designations are presentation computers, and classroom projection computers. Passwords must be changed at least annually, and must follow standard complexity rules. In cases where the workstation has access to network resources, the password must be changed on termination of any person with access.

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version	Change	Author	Date of Change
1.0	Initial Draft	Richard Woodard	4/17/2015
1.1	First Review	Richard Woodard	5/12/2015
1.2	Additions from previous policies. Policy adopted.	Richard Woodard	6/11/2015
1.3	Updated Non-Compliance to match newly adopted standards	Richard Woodard	09/29/2016
1.4	Updated Non-Compliance to match standard adopted October, 2016	Richard Woodard	12/7/2016

1.5	Add 9 – Exception for service and single-use accounts, and Procedure 4 for single-use workstation.	Richard Woodard	2/4/2019
1.5.1	Updated Storage Location	Richard Woodard	12/1/2019

Concordia Theological Seminary
Fort Wayne, Indiana

Acceptable Usage Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Data Protection Policy, Software Installation Policy
Related Procedures	
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	2/15/2016
Next Review Date	February, 2020

Purpose

Acceptable usage policies clearly indicate what information system users are and are not allowed to do. The potential exists that, without these policies, information system users could violate information security and avoid punitive actions by claiming to not know about any restrictions in place. This can make it extremely difficult to enforce the measures outlined in the policy and ultimately lead to a complete disregard of the policy.

Scope

This Acceptable Usage Policy applies to all users of all information systems that are the property of *Concordia Theological Seminary*. Specifically, it includes:

- All employees, whether employed on a full-time or part-time basis by *CTSFW*.
- All contractors and third parties that work on behalf of and are paid directly by *CTSFW*.
- All contractors and third parties that work on behalf of *CTSFW but* are paid directly by an alternate employer.
- All employees of partners and clients of *CTSFW* that access *CTSFW*'s non-public information systems.
- All volunteers and temporary users of CTSFW that access *CTSFW*'s information systems.

Policy

1. *CTSFW* will issue acceptable usage guidelines covering the following items:
    a. Computer and information system usage
    b. Software and data usage

c. Internet and e-mail usage

d. Telephone usage

e. Office equipment & materials usage

f. Social media

2. As a requirement of information system access, and as a component of security awareness training, all information system users, whether employees or third parties, will be required to provide signed acceptance of the acceptable usage guidelines. A copy of the signed document will be provided to the individual with the original being retained by the Human Resources department.

Procedure 1

Systems, including computers of all kinds, are the property of the seminary:

- Access to, and use of, systems and the components that form them may be monitored and controlled at all times.

Procedure 2

The software tools the seminary provides and the data they create and manipulate are the property of the seminary:

- Software is to be used for its intended purpose only. It is not to be copied, distributed, installed, or deleted without appropriate authorization. Such activities may be monitored and controlled at all times.
- Data is to be used for its intended purpose. It is not to be copied, distributed, edited, appended, or deleted without appropriate authorization. Such activities may be monitored and controlled at all times.

Procedure 3

Internet and e-mail usage must be restricted as both activities make use of public and unsecured networks:

- The Internet is to be used for business purposes only and usage will be logged at all times and may be monitored and controlled.
- E-mail is to be used for business purposes only and usage may be monitored and controlled at all times.

Procedure 4

The telephone system, including all telephones and fax machines, is the property of the seminary:

- The telephone system, including all analog and digital lines, is ordinarily to be used for business purposes only and may be monitored and controlled.

Procedure 5

The office materials, furnishings and supplies provided to employees are the property of the seminary and are to be used for business purposes only:

- Generic materials (those that do not imply consent of the seminary such as pens, blank paper, etc.) may be freely accessed but are not to be removed from those facilities without prior consent.
- Specific materials (those that imply consent of the seminary such as letterhead and stamps, etc.) must have restricted access and are not to be removed from the facilities without prior consent.

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version	Change	Author	Date of Change
1.0	Initial Draft	Richard Woodard	8/13/2015
1.1	Second Draft	Richard Woodard	10/1/2015
1.2	Accepted	Richard Woodard	2/11/2016
1.3	Change Non-Compliance to match new official standard	Richard Woodard	9/30/2016
1.4	Updated Non-Compliance to match standard adopted October, 2016	Richard Woodard	12/7/2016
1.4.1	Updated Storage Location	Richard Woodard	12/1/2019

Concordia Theological Seminary
Fort Wayne, Indiana

Clear Screen Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Physical and Environmental Security Policy, Password Policy, Clean Desk Policy, Security Awareness Training Policy
Related Procedures	
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	March 1, 2019
Next Review Date	February 2020

Purpose

The purpose of this Clear Screen Policy is to protect confidential, private and personally identifiable information. Prevent loss of information and data tampering by securing unattended workstations or data displays that may be publicly accessible.

Scope

This policy applies to all computer workstation and other data display devices of Concordia Theological Seminary, Fort Wayne (CTSFW).

This policy applies to all users of all information systems that are the property of CTSFW. Specifically, it includes:

- All CTSFW personnel, whether on a full-time or part-time basis.
- All contractors and third parties that work on behalf of and are paid directly by CTSFW.
- All contractors and third parties that work on behalf of CTSFW but are paid directly by an alternate employer.
- All employees of partners and clients of CTSFW that access CTSFW's non-public information systems.
- All volunteers and temporary users of CTSFW that access CTSFW's information systems.
- All students attending CTSFW.

Policy

1. Whenever any device capable of displaying data or accessing CTSFW systems is unattended for any period of time, it should be locked and password protected, logged off or powered down.

2. The use of screen saver, suspended mode and hibernation mode are acceptable provided proper network credentials are required to unlock on resumption.
3. The 10-minute screen lock group policy is only a precautionary measure, and is not considered sufficient for the purposes of this policy.

Procedure

- For Windows devices, Press Windows + L (⊞+L) on your keyboard to lock your screen.
- Close the lid on any laptop configured to sleep, hibernate or shut down on lid closure and require a password on resumption.

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version	Change	Author	Date of Change
1.0	Initial Draft	Richard Woodard	12/7/2016
1.1	Final Draft	Richard Woodard	2/5/2019
1.2	Accepted	Richard Woodard	2/22/2019
1.2.1	Updated Storage Location	Richard Woodard	12/1/2109

Concordia Theological Seminary
Fort Wayne, Indiana

Clean Desk Policy

Policy Owner	IT
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Clear Screen Policy, Data Protection Policy, Password Policy, Security Awareness Training Policy
Related Procedures	
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	10/1/2019
Next Review Date	10/1/2020

Purpose

A clean desk policy is an important tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or personnel leave their workstations. It is a critical component to reducing the risk of security breaches. This policy should also increase personnel's awareness about protecting sensitive information.

This policy establishes the minimum requirements for maintaining a "clean desk" where sensitive Private Information (PI) and Personally Identifiable Information (PII) about *Concordia Theological Seminary*'s (CTSFW) personnel, students, constituents, Intellectual Property (IP), and vendors is secure in locked areas and out of sight. A Clean Desk policy is an integral part of standard basic privacy controls.

Scope

This Clean Desk Policy applies to:

- All personnel, whether employed on a full-time or part-time basis (including student workers) by CTSFW.
- All contractors and third parties that work on behalf of and are paid directly by CTSFW.
- All contractors and third parties that work on behalf of CTSFW but are paid directly by an alternate employer.
- All employees of partners and clients of CTSFW that access CTSFW's non-public information systems.
- All volunteer workers that work on behalf of CTSFW.
- All student workers attending CTSFW.

This Clean Desk Policy applies to all data assets of *CTSFW*. Specifically, it includes:

- Intellectual Property (IP), whether owned by *CTSFW* or provided by a third party.
- Personally Identifiable Information (PII) for personnel, students, clients, constituents, or other third parties.
- Private or sensitive Information (PI) personnel, students, clients, constituents, or other third parties.
- Financial information for *CTSFW*, its employees, students, clients, constituents, or other third parties.
- Other non-public data or information assets deemed the property of *CTSFW*.
- Other public data or information assets deemed the property of *CTSFW*.

Policy

- All Personnel are required to ensure that all PI, PII, and IP in hardcopy or electronic form is secure.
- PI, PII, and IP may not be left unattended in a manner accessible by unauthorized persons.
- Documents containing PI, PII, and IP which is no longer required must be destroyed in a secure manner.

Procedure 1

Ensure PI, PII, and IP at workstations is secure.

- All sensitive information, PI, or PII in hardcopy or electronic form must be secure in work areas at the end of the day and when the area will be vacated for any period of time.
- Any PI, PII, or IP must be removed from the desk and locked in a drawer or cabinet when the desk is unoccupied and at the end of the day.
- Keys used for access to PI, PII, or IP must not be left at an unattended desk.
- Passwords may not be written and left near, on, or under a computer, nor may they be left written down in an accessible location.

Procedure 2

Keep electronic devices secure:

- Computer workstations must be locked when a workspace is unoccupied.
- Portable computing devices such as laptops and tables should be locked or secured when unattended.
- Mass storage devices such as CDROM, DBD, USB drives, External Drives, and portable storage devices must be secured and locked.

Procedure 3

PI, PII, and IP must be stored in a secure, locked location:

- File cabinets containing PI, PII, or IP must be kept closed and locked when not in use or when unattended.
- Safes and lockboxes containing PI, PII, or IP must be kept closed and locked with combinations fully scrambled when not in use or when unattended.

Procedure 4

PI, PII, and IP should not be left in publically accessible areas:

- Printouts containing PI, PII, or IP should be immediately removed from the printer.
- Whiteboards, blackboards and projectors containing PI, PII, or IP should be erased when no longer being used or when they will be unattended.
- Proper care should be taken that PI, PII, and IP are not projected or displayed in a manner or venue which is easily publically accessible.

Procedure 5

PI, PII, and IP must be properly disposed of when it is no longer required:

- PI, PII and IP must be immediately shredded or placed in the official shredder bins, or lockboxes designated for confidential document disposal.
- Electronic data should be erased in accordance with Data Protection Policy.

Procedure 6

Policy Compliance Measurement

- Verification will be made through various methods, including but not limited to, periodic walk-throughs, reporting tools, internal and external audits, and feedback to IT.

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in HR policies and procedures.

Revision History

Version	Change	Author	Date of Change
1.0	Initial Draft	Richard Woodard	9-13-2019
1.1	Final Draft	Richard Woodard	9-25-2019
1.2	Accepted	Richard Woodard	9/27/2019
1.2.1	Updated Storage Location	Richard Woodard	12/1/2019

Concordia Theological Seminary
Fort Wayne, Indiana

Anti-Virus Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Network Security Policy, Firewall Policy, Personal Device Acceptable Usage Policy, Hardware Sanitization Policy, Removable Media Acceptable Use Policy, Security Awareness Training Policy, Software Installation Policy
Related Procedures	N/A
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	October 15, 2016
Next Review Date	February, 2020

Purpose

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via email or instant messaging attachments, downloadable Internet files, files from removable media such as Flash drives / USB drives / thumb drives / jump drives / etc., diskettes, and CDs. Viruses are usually disguised as something else, so their presence is not always obvious to the computer user. A virus infection can be very costly to CTSFW in terms of lost data, lost staff productivity, and/or lost reputation.

As a result, one of the goals of CTSFW is to provide a computing network that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by CTSFW employees to help achieve effective virus detection and prevention.

Scope

This policy applies to all computers that are connected to CTSFW production network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both company-owned computers and personally-owned computers attached to CTSFW's network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

This policy applies to any full-time or part-time faculty or staff member, student workers, and contract or sub-contracted employee working for or on behalf of CTSFW.

Definitions

Production Network – The segments of CTSFW's Local Area Network (LAN) that are designated specifically for faculty and staff. These segments have access to internal network resources such as servers and printers. Students and guests are denied access to the production network.

Guest / Student Network – The portions of CTSFW's LAN that are designated specifically for guests or students. These network segments are configured in such a way that they are given access to the Internet, and are denied access to all production network resources

Sophos Endpoint Security and Control – This is the anti-virus solution that is currently employed by CTSFW. Any mention of anti-virus software assumes this to be the product that is being used.

Virus – The word "virus" is often used in a general manner. For the purposes of this policy, this includes the following specific forms of malicious software: Rootkit, Spyware, Trojan, Worm and Virus.

Policy

1. Currently, CTSFW uses Sophos Endpoint Security and Control for its anti-virus software, and has enough licensed copies to install it on all CTSFW-owned computers. Installation of this software is the responsibility of the IT Department.
2. All computers attached to CTSFW's production network must have standard, supported anti-virus software installed. This software must be active, scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.
3. Any activities with the intention to create and/or distribute malicious programs onto the CTSFW network (e.g. viruses, worms, Trojan horses, email bombs, etc.) are strictly prohibited.
4. If a user covered by this policy receives what he/she believes to be a virus or suspects that a computer is infected with a virus, the virus must be reported to the IT department immediately at 260-452-3178. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.
5. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IT department.
6. Any virus-infected computer will be removed from the network until it is verified as virus-free.
7. No employee shall make any attempt to remove, disable, suspend, override, modify, bypass, or inhibit the operation of the anti-virus software.

Procedures

1. Always run the standard anti-virus software that is provided and installed by the IT department of CTSFW.
2. Never open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source.
3. Never open any files or macros attached to an email from a known source (even a co-worker) if you were not expecting a specific attachment from that source.

4. Be suspicious of email messages containing links to unknown websites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.
5. Files with the following filename extensions are blocked by the email system: .ADE, .ADP, .BAT, .CHM, .CMD, .COM, .CPL, .EXE, .HTA, .INS, .ISP, .JAR, .JSE, .LIB, .LNK, .MDE, .MSC, .MSP, .MST, .PIF, .SCR, .SCT, .SHB, .SYS, .VB, .VBE, .VBS, .VXD, .WSC, .WSF, .WSH. If you need to send a file with this extension for business purposes, please contact the IT Department to discuss options of accomplishing this.
6. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
7. Avoid direct portable drive (e.g. thumb drive, USB drive, memory stick, etc.) sharing with read/write access. Always scan a portable drive for viruses before using it.
8. If instructed to delete email messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.
9. Back up critical data and systems configurations on a regular basis and store backups in a safe place.

The following activities are the responsibility of CTSFW departments and employees:

1. Departments must ensure that all departmentally-managed computers have virus protection that is in keeping with the standards set out in this policy.
2. All employees are responsible for taking reasonable measures to protect against virus infection.
3. Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the CTSFW network without the express consent of the IT department.

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version Number	Version Name	Author	Date

1.1	First Draft	Jason Iwen	9/23/2016
1.2	Adopted	Richard Woodard	9/29/2016
1.3	Updated Non-Compliance to match standard adopted October, 2016	Richard Woodard	12/7/2016
1.3.1	Updates Storage Location	Richard Woodard	12/1/2019

Concordia Theological Seminary
Fort Wayne, Indiana

Firewall Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Network Security Policy, Password Policy, Removable Media Acceptable Use Policy, Security Awareness Training Policy
Related Procedures	See procedures for policies listed above
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	October 15, 2016
Next Review Date	February 2020

Purpose

Concordia Theological Seminary (CTSFW) operates perimeter firewalls between the Internet and its private internal networks in order to create a secure operating environment for CTSFW's computer and network resources. A firewall is just one element of a layered approach to network security. The purpose of this Firewall Policy is to describe how the Sophos firewall will filter Internet traffic in order to mitigate risks and losses associated with security threats, while maintaining appropriate levels of access for business users.

The Firewall Policy is subordinate to CTSFW's general Security Policy, as well as any governing laws or regulations.

Scope

This Firewall Policy refers specifically to the Sophos firewall. As stated in the Purpose section, the general role of this firewall is to create a secure operating environment for CTSFW's computer and network resources. With that in mind, the firewall will (at minimum) perform the following security services:

- Access control between the trusted internal network and untrusted external networks.
- Block unwanted traffic as determined by the firewall rule set.
- Hide vulnerable internal systems from the Internet.
- Hide information, such as system names, network topologies, and internal user IDs, from the Internet.

- Log traffic to and from the internal network.
- Provide robust authentication.
- Provide virtual private network (VPN) connectivity using two-factor authentication.

All faculty, staff, student workers, students, volunteers, contractors and sub-contractors of CTSFW are subject to this policy and required to abide by it.

Policy

The approach adopted to define firewall rule sets is that all services will be denied by the firewall unless expressly permitted. Describing in detail what traffic is allowed would be counterproductive for two reasons. First, the policy would quickly become too lengthy to be considered useful. At the time of this writing, the firewall contains 171 rules that define what sorts of traffic should be allowed. (And this does not include other configuration details that control other types of connections that are not addressed directly in the rulebase.) Secondly, describing in detail what is allowed would mean that any request for new traffic to be allowed would require a change to this policy, which would then need to be approved by the IT Policies and Procedures Committee. For these reasons, we will state in general terms that the following types of traffic are allowed:

- Outbound – All Internet traffic to hosts and services outside of CTSFW that have not been identified as malicious or illegal and/or unethical. (The firewall has the capability to block websites based on category. We currently block websites in the "Nudity" category.)
- Inbound – Only Internet traffic from outside CTSFW that supports the business mission of CTSFW. The primary example of this is external visitors to websites that we host on campus (such as my.ctsfw.edu).

The IT Department is responsible for implementing and maintaining CTSFW firewalls, as well as for enforcing and updating this policy. Logon access to the firewall will be restricted to IT Staff. Firewall administrators will access the firewall using their Active Directory credentials via LDAP. Password construction for those accounts is controlled through CTSFW's Password Policy.

Any questions or concerns regarding the Sophos firewall should be directed to Jason Iwen, Director of IT/Chief Information Officer: jason.iwen@ctsfw.edu or 260-452-3175.

Relevant Procedures

- CTSFW faculty, staff and students may request changes to the firewall's configuration in order to allow previously disallowed traffic. These requests should be made via the helpdesk system, stating the reason for the request, and any pertinent information, such as IP address(es), host name(s) and port(s). All requests will be assessed to determine if they fall within the parameters of acceptable risk. Approval is not guaranteed as associated risks may be deemed too high. If this is the case, an explanation will be provided to the original requestor and alternative solutions will be explored.

- CTSFW faculty and staff may request access from the Internet for services located on the internal CTSFW network. Typically, this remote access is handled via a secure, encrypted virtual private network (VPN) connection. The VPN currently configured by the firewall is an SSL VPN, and requires two-factor authentication. Requests for VPN access should be made through the helpdesk system. VPN access will only be configured on computers owned by CTSFW.
- From time to time, outside vendors, contractors, or other entities may require secure, short-term, remote access to CTSFW's internal network. If such a need arises, the department working with the third-party should make a request through the helpdesk system including full justification. Approval is not guaranteed.
- Files with the following filename extensions are blocked by the firewall: exe, msi, com, bat, vbx, hta, inf, jse, wsh, vbs, vbe, lnk, chm, pif, reg, scr, cmd, dll. Exceptions can be made on a per-domain basis (i.e. www.microsoft.com). If you need to download a file with one of these extensions from a domain that is not already allowed, please contact the IT Department to discuss options of accomplishing this.
- Turnaround time for the above stated firewall reconfiguration and network access requests is approximately 3 business days from the receipt of the request form.
- Firewall logs will be downloaded from the firewall on a quarterly basis. Once downloaded, they will be placed in the IT Staff share, which is backed up daily.
- Logs will be reviewed on an as-needed basis.

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version Number	Version Name	Author	Date
1.1	First Draft	Jason Iwen	9/23/2016

1.2	Adopted	Richard Woodard	9/29/2016
1.3	Updated Non-Compliance to match standard adopted October, 2016	Richard Woodard	12/7/2016
1.3.1	Updated Storage Location	Richard Woodard	12/1/2019

Concordia Theological Seminary
Fort Wayne, Indiana

Network Security Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Systems Monitoring & Auditing Policy, IT Password Policy, Account Management Policy, Systems Maintenance Policy, Anti-Virus Policy, Firewall Policy, IT Information Security Incident Management Policy, IT Information Security Incident Reporting Policy, User Authorization, Identification and Authentication Policy, Removable Media Acceptable Use Policy, Hardware Sanitation Policy, Security Awareness Training Policy, Software Installation Policy
Related Procedures	See above policies
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	October 15, 2016
Next Review Date	February 2020

Purpose

To provide a secure and reliable information network for Concordia Theological Seminary (CTSFW).

Scope

The Network Security Policy applies to all users of all information system that are the property of CTSFW. Specifically, it includes:

- All employees, whether employed on a full-time or part-time basis (including student workers) by CTSFW.
- All contractors and third parties that work on behalf of and are paid directly by CTSFW.
- All contractors and third parties that work on behalf of CTSFW but are paid directly by an alternate employer.
- All employees of partners and clients of CTSFW that access CTSFW's non-public information systems.
- All volunteer workers that work on behalf of CTSFW.
- All students attending CTSFW.

Policy

Network operation at CTSFW is ordinarily governed by the policies mentioned in the "Related Policies" section at the beginning of this policy. For circumstances not covered by the aforementioned policies, decisions will be made by the IT Director/Network Administrator in accordance with PCI/FERPA standards and regulations, as well as all applicable laws.

Procedures

Relevant procedures can be found in the related policy documents. Procedures not covered by the aforementioned policies should be researched and reviewed in accordance with PCI/FERPA standards and regulations, as well as all applicable laws.

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version Number	Version Name	Author	Date
1.1	First Draft	Jason Iwen	9/28/2016
1.2	Adopted	Richard Woodard	9/29/2016
1.3	Updated Non-Compliance to match standard adopted October, 2016	Richard Woodard	12/7/2016
1.3.1	Updated Storage Location	Richard Woodard	12/1/2019

Concordia Theological Seminary
Fort Wayne, Indiana

Security Awareness Training Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Antivirus Policy, Hardware Sanitation Policy, Removable Media Acceptable Use Policy, Clear Screen Policy, Clean Desk Policy, Firewall Policy, Network Security Policy, User Authorization, Identification & Authentication Policy, Account Management Policy, Data Protection Policy, Physical Access Control Policy, Information Security Incident Reporting Policy
Related Procedures	See Procedures of related Policies
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	December 16, 2019
Next Review Date	July, 2020

Purpose

The quality and integrity of CTSFW's security awareness training ensures that the workforce members, including management of CTSFW's information systems, understand the security implications of their actions and increase the likelihood that information system security will not be breached, either intentionally or unintentionally, through technical measures (such as hacking) or non-technical measures (such as Social Engineering). Without such training, information systems users have an increased likelihood of breaching security and have lower individual culpability should they breach security.

Scope

The Security Awareness Training Policy applies to all users of CTSFW information systems or personnel with campus access, including all temporary or contract workers, or anyone granted access to CTSFW system. Specifically, it includes:

- All CTSFW personnel, whether on a full-time or part-time basis.
- All contractors and third parties that work on behalf of and are paid directly by CTSFW.
- All contractors and third parties that work on behalf of CTSFW but are paid directly by an alternate employer.
- All employees of partners and clients of CTSFW that access CTSFW's non-public information systems.
- All volunteers and temporary users of CTSFW that access CTSFW's information systems.
- All students attending CTSFW.

Definitions

- Personnel – Any worker including Faculty, Ordained Staff, or staff. Unless otherwise noted this also extends to volunteer, student, and contract workers.

- A Phish or Phishing is a social engineering attack, generally involving spoofing of emails for the purpose of gaining private or personal information such as user credentials, and financial information.
- Social engineering is the art of manipulating, influencing, or deceiving you in order to gain control over your computer system. They may use the phone, email, mail or direct contact to gain illegal access.
- Penetration Testing is a method of testing computer systems and organizations security by attempting to circumvent security functions within certain constraints.

Governing Laws & Regulations

Guidance	Section
ISO/IEC 27001:2013	A.9 (A.9.1, A.9.2, A.9.3, A.9.4)
NIST SP 800-53 v4	AC-1~AC-25
FERPA 34 CFR	99

Policy Statements

1. All personnel of CTSFW are required to participate in security awareness training within 30 days of starting work and thereafter on an annual basis. Training modules track module progress of security awareness training, a completion status indicates that they have completed training, understand the purpose of the training and the specific procedures taught, and that they intend to abide by CTSFW's security policies.
2. All personnel of CTSFW that work as administrators or hold other positions with significant and relevant security operations responsibilities are required to participate in security operations training 30 days of starting work or the deployment of a new or significantly updated/revised information system and thereafter on an annual basis. Training modules track module progress of security awareness training, a completion status indicates that they have completed training, understand the purpose of the training and the specific procedures taught, and that they intend to abide by CTSFW's security policies.
3. Security Training will be ongoing at CTSFW; personnel will be kept up to date on new improvements or threats to watch out for. They can be distributed by email, posters, Blue News, or meetings.

Relevant Procedures

Procedure 1

- CTSFW provides training through KnowBe4, a professional security training and testing company. All seminary personnel will be given access to a KnowBe4 account, which provides training and tracks progress. This training is provided on hire, and must be completed within 30 days.

- This training program should address the following:

- *The creation and maintenance of appropriate passwords, including the need to maintain password confidentiality.*
- *Detecting, avoiding, and responding to viruses and other malware.*
- *Detecting, avoiding, and responding to Identity Theft.*
- *Detecting, avoiding, and responding to Social Engineering.*
- *Appropriate usage of network resources including the Internet and email.*
- *Appropriate usage of systems, including the servers, personal and portable computers, and external media devices.*
- *Appropriate usage of software including copyright and file sharing restrictions.*
- *Appropriate usage of data including entry, editing, and distribution restrictions and the use of encryption capabilities, where deployed.*
- *Appropriate physical security measures to ensure the protection of facilities, assets, and personnel.*
- *Appropriate reporting, including the reporting of abuse, policy violations and suspicious activities.*

Procedure 2

- To maintain awareness and measure the effectiveness of training, the program provides ongoing monthly testing. Each defined CTSFW user of KnowBe4 will receive at least one test Phishing email every month. The user's response to this email is tracked, and they are informed if they fell for the hook.

- When the functionality is reliably available, those who fail the phish test will be enrolled in a brief supplemental training session, generally a short spot-the-phish.

Procedure 3

CTSFW may also use physical and remote penetration testing, to verify security.

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.

- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.

- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version ID	Date of Change	Author	Rationale
1.0	12/1/2019	Richard Woodard	New
1.1	12/9/2019	Richard Woodard	Accepted by committee

Concordia Theological Seminary
Fort Wayne, Indiana

User Authorization, Identification & Authentication Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	IT Password Policy, Acceptable Use Policy, Network Security Policy, Administrative Rights Policy, Access Control Policy, Account Management Policy, Security Awareness Training Policy
Related Procedures	List other related enterprise procedures both within or external to this
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	9/1/2015
Next Review Date	August 2020

Purpose

The use of authorization, identification and authentication controls ensures that only known users make use of information systems. Without authorization, identification and authentication controls, the potential exists that information systems could be accessed illicitly and that the security of those information systems be compromised.

Scope

This User Authorization, Identification & Authentication Policy applies to all users of all information systems that are the property of *Concordia Theological Seminary, Fort Wayne (CTSFW)*. Specifically, it includes:

- All personnel, whether employed on a full-time or part-time basis (including student workers) by *CTSFW*.
- All contractors and third parties that work on behalf of and are paid directly by *CTSFW*.
- All contractors and third parties that work on behalf of *CTSFW* but are paid directly by an alternate employer.
- All employees of partners and clients of *CTSFW* that access *CTSFW*'s non-public information systems.
- All volunteer workers that work on behalf of *CTSFW*.
- All students attending CTSFW.

Policy

1. Prior to being granted access to an information system, each user must be provided with formal authorization by an appropriate official (i.e., the owner of the information system, the custodian of the data housed within the information system or a designee of these

individuals). This authorization will be based on definitive and verifiable identification of the user and will be logged by the authorizing official. The current accept policy is to submit authorization requests and return approvals in the IT Help Desk system at http://helpdesk.ctsfw.edu.

2. Once authorization has been granted, the user will be provided with a unique information system identifier. Examples of identifiers include user ids and employee numbers. Additionally, the user will be provided with a unique information system authenticator that is tied to the assigned identifier. Examples of authenticators include passwords and tokens. Identifiers and authenticators will be delivered to the authorized user in such a manner as to ensure they are received only by the authorized user. To minimize risk, identifiers and authenticators for critical information systems will not be provided together.
3. Should an information system user's account be disabled for any reason, the user's identifier and authenticator will also be disabled, where applicable.

Procedure 1

Identify users via external identity verification methods prior to the issuance of accounts:

- As part of the on-boarding process, student or employee identity should be verified through the use of government-issued identification documents that include the following information:
    - *Full name.*
    - *Signature.*
    - *Photograph.*

Procedure 2

Each system user is to be provided with an identifier and an authenticator such that they can uniquely and individually access the system:

- Identifiers must be unique to the individual but can be common across systems.
- User identifiers (User IDs) should be constructed in one of the following manners:
    - *First name initial and last name.*
    - *Last name, first name initial and middle name initial*
    - *Last name and first name initial*
    - *First name and last name.*
    - *First name, underscore and last name.*
    - *First name, period and last name.*
    - *Seminary Email Address*
- Authenticators must be unique to each individual and to each system; however, a master authenticator may be used to access individual system authenticators (a single sign-on system).

Procedure 3

The identifiers and authenticators associated with each account must be distributed in such a manner as to ensure they are delivered only to the personnel to whom they are assigned:

- Identifiers are to be distributed in a manner that ensures delivery will not be inhibited.
- Authenticators are to be distributed in a manner that protects their secrecy and ensures that delivery will not be inhibited.

Procedure 4

Once a system account is no longer required, it must be disabled to prevent its use and archived to provide for potential future investigation:

- Where account access is still required by any person, identifiers and authenticators will be reset.
- Where account access is no longer required, identifiers and authenticators will be deleted along with the account.

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version	Change	Author	Date of Change
1.0	Initial Draft	Richard Woodard	4/17/2015
1.1	First Review	Richard Woodard	7/9/2015
1.2	Accepted	Richard Woodard	8/13/2015
1.3	Change Non-Compliance to match new official standard	Richard Woodard	9/30/2016

1.4	Updated Non-Compliance to match standard adopted October, 2016	Richard Woodard	12/7/2016
1.5	Updated Storage Location and Related Policies	Richard Woodard	12/1/2019

Concordia Theological Seminary
Fort Wayne, Indiana

Administrative Rights Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Network Security Policy, Acceptable Usage Policy, Account Management Policy, Software Installation Policy
Related Procedures	See procedures for policies listed above
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	December 16, 2019
Next Review Date	July 2020

Purpose

The granting of administrative rights to an employee of CTSFW over an individual desktop, laptop, or other end-user device is a privilege only awarded to individuals who require this level of access and control in order to do their jobs effectively. The goal of this policy is to describe the circumstances under which administrative rights can be granted as well as the terms and conditions upon which this privilege will be granted.

Scope

This policy applies to all information systems and information system components of Concordia Theological Seminary. Specifically, it includes:

- Mainframes, servers and other devices that provide centralized computing capabilities.
- SAN, NAS and other devices that provide centralized storage capabilities.
- Desktops, laptops, tablets, phones and other devices that provide distributed computing capabilities.
- Routers, switches, access points and other devices that provide network capabilities.
- Firewalls, IDP sensors and other devices that provide dedicated security capabilities.
- Third-party Systems

Policy Statements

The granting of administrative rights allows the individual to change the configuration settings of a given machine and install software on that machine. As a result, these rights can expose the CTSFW network to malware and other security exploits. In addition, incorrect configuration of machines can lead to performance problems, potentially resulting in machine downtime, lost productivity, and higher support costs.

Given the serious consequences of mishandling or abuse of administrative rights, these rights will only be granted under the condition that they are essential for the performance of the grantee's job. Such conditions could include the following:

- The ability to download and install specific types of software or configure system settings is mandated in the individual's job description.
- An administrative rights access level is required for a necessary software title to run on a given machine. Company-owned and supported titles to which this applies include:
    - Blackbaud RE
    - Blackbaud FE/SIS/EE
- Sufficient levels of IT support do not exist due to time-of-day, geographical, or expertise constraints.

Note: Members of the IT Department are not automatically granted administrative rights based on their membership in the IT Department alone.

If you do not have administrative rights, then you will need to apply and gain approval for administrative rights if you believe it is required by your job. To apply for administrative rights, please use the Administrative Rights Application Form located at the end of this policy document. The designated authorities of the IT Department reserve the right to deny the application if it does not represent a clear business need or if the applicant has a documented history of security policy violation.

Relevant Procedures

Procedure 1

To apply for administrative access, open a ticket with the IT Helpdesk by sending an email to helpdesk@ctsfw.edu including the form at the bottom of this policy

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version ID	Date of Change	Author	Rationale
1.0	12/1/2019	Richard Woodard	New
1.1	12/9/2019	Richard Woodard	Accepted

Concordia Theological Seminary
Fort Wayne, Indiana

Administrative Rights Application Form

Employee Name	
Employee Job Title	
Employee Department	
Employee Phone/Email	
Supervisor	
Date of Application	

Please provide the following information:

Identity of machine for which administrative rights are being requested.
Reason that administrative rights are required.

Supervisor Approval

I approve the request for administrative rights as outlined above.

_____
Supervisor Name

_____ _____
Supervisor Signature Date

IT Approval

This section is for IT Department administrative purposes only.

The request has been: ___ Approved ___ Denied

If the request has been denied, please document the reason for denial.

If the request has been approved, please document the following information:

Planned Activation Date	
Actual Activation Date	
Policy Read and Signed	

_____
IT Authority Name

_____ _____
IT Authority Signature Date

Concordia Theological Seminary
Fort Wayne, Indiana

Technology Move/Add/Change Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Network Security Policy, Physical Access Control Policy, Acceptable Usage Policy, User Authorization, Identification & Authentication Policy, Account Management Policy, Physical and Environmental Security Policy, Access Control Policy, Software Installation Policy
Related Procedures	See Procedures of related Policies
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	December 16, 2019
Next Review Date	July, 2020

Purpose

This policy provides guidelines for end users to request a move, add, or change to their desktop computing environments. The goal of this policy is:

1. To mitigate the risk associated with unauthorized changes;
2. To minimize disruption to the business, IT department, and end users;
3. To maintain consistent expectations.

A Move/Add/Change request must be submitted to IT Helpdesk helpdesk@ctsfw.edu for the completion of any of the following:

- Move desktop system (e.g. PC, telephone) or peripheral (e.g. printer) to another location.
- Add/disable an employee account (e.g. network, email, voicemail).
- Add/remove a service to/from an existing employee account.
- Add a new employee desktop system.
- Add/remove/change software or hardware to/from an existing desktop system.
- Change an employee's name or other personally identifiable information in the system.

Scope

Desktop Move/Add/Change Policy applies to all information systems and information system components of CTSFW, all users of all information systems that are the property of *CTSFW*. Specifically, it includes:

- Mainframes, servers and other devices that provide centralized computing capabilities.
- SAN, NAS and other devices that provide centralized storage capabilities.
- Desktops, laptops, tablets, phones and other devices that provide distributed computing capabilities.
- Routers, switches, access points and other devices that provide network capabilities.
- Firewalls, IDP sensors and other devices that provide dedicated security capabilities.
- Third-party Systems
- All personnel, whether employed on a full-time or part-time basis by CTSFW.
- All contractors and third parties that work on behalf of CTSFW and are paid directly by CTSFW.
- All contractors and third parties that work on behalf of CTSFW but are paid directly by an alternate employer.
- All employees of partners and clients of CTSFW that access CTSFW's non-public information systems.
- All volunteers and users of CTSFW that access CTSFW's information systems.
- All CTSFW Student workers.

Governing Laws & Regulations

Guidance	Section
ISO27001:2013	A.16.1
NIST SP 800-53 v4	AU-6, IR-1, IR-6, CA-2, CA-7, PL-4, SA-5, SA-11, SI-2, SI-5, IR-4, IR-10, AU-7, AU-8, AU-9, AU-11
FERPA 34 CFR	99

Policy Statements

Management must ensure that their direct reports understand the scope and implications of this policy and make a copy readily available.

Although any employee may submit an M/A/C request for their desktop environment, all requests must be approved by a direct manager before submission to the IT department. For the addition of a new employee account, HR approval is required.

All move, add, or change requests must be received a minimum of 3 business days in advance of the requested action date. However, to ensure that your preferred action date can be met, it is recommended that you submit your request as far in advance as possible. In order to minimize

disruptions and maintain efficiency, all regular moves, adds, and/or changes will be scheduled to take place during the following time periods:

- Monday through Friday, 8:30 A.M. to 4:00 P.M. except holidays.

While all approved moves, adds, and/or changes will be carried out in as timely a manner as possible, they may be delayed in the event of an IT-related problem or emergency.

In the event of an emergency request, advance notification is not required. These will be handled on a case-by-case basis. Details of the actual execution of the request will be forwarded to the request contact within an hour of receipt of the request.

Most moves, adds, or changes involve system downtime for the user. Outage windows will be minimized whenever possible. If a window is to exceed the estimated time, affected users will be notified in advance.

Non-Compliance

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version ID	Date of Change	Author	Rationale
1.0	12/1/2019	Richard Woodard	New
1.1	12/9/2019	Richard Woodard	Accepted

Concordia Theological Seminary
Fort Wayne, Indiana

Software Installation Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Acceptable Usage Policy, Anti-Virus Policy, Network Security Policy, Administrative Rights Policy
Related Procedures	See procedures for policies listed above
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	December 16, 2019
Next Review Date	July, 2020

Purpose

The goal of the IT department is to provide stable technology solutions that both perform well and appropriately address business needs. A lack of standards regarding what software titles can be installed on company end-user devices, including desktop and laptop machines, can hinder provision of excellent service to all end users and departments.

The purpose of this Software Installation Policy is to address all relevant issues pertaining to appropriate software installation and deployment on CTSFW end-user computing devices.

This policy is a living document and may be amended at any time. Any questions regarding this policy should be directed to the IT Helpdesk.

Scope

This policy applies to all software, servers, desktops, and laptop computers owned and operated by CTSFW and all users of such systems.

Governing Laws & Regulations

Guidance	Section
ISO27001:2013	A.11 (A.11.1, A.11.2)
NIST SP 800-53 v4	PE-2~PE-6, MA-5, PE-8, CP-2, CP-6, CP-7, PE-1, CP-8, PE-19~PE-16, MA-2~MA-6, AC-19, AC-20, MP-5, PE-17, MP-6, MA-2, MP-5
U.S. Copyright Act of 1976	17 U.S.C. § 107 through 122

Policy Statements

1. Workstations and laptops come preinstalled with a base set of programs including, but not limited to:
   - Windows 10 Enterprise
   - Microsoft Office 2013 and 2016, all components and language packs
   - Google Chrome
   - Google Drive Filestream
   - Firefox
   - Adobe Acrobat Reader
   - Sophos Endpoint
   - Mitel Connect

   Other supported software titles, available upon request, include:
   - Adobe (All suites (Acrobat, Photoshop, Illustrator, etc.) and versions)
   - Blackbaud Raiser's Edge
   - Blackbaud SIS/Education Edge
   - PaperSave
   - Notepad++
   - WinZip
   - WinRar
   - Paint.net
   - Any Software located in the "Install from Network" section of "Add/Remove programs"

2. Other software titles are available upon request and approved on a case-by-case basis.
   Adobe (All suites and versions)
   LogMeIn Central
   Visual Studio
3. The IT department expressly forbids installation of the following software without express approval:
   - Privately owned software
   - Internet downloads
   - Any title not listed in this policy
4. The IT department expressly forbids installation of the following software
   - Pirated copies of any software titles
   - Any software not installed according to the procedures set out in this policy

5. Approval must be obtained from a direct supervisor (or designate) as well as the IT Department to have software installed on your device. This includes all software titles listed above, currently unlisted titles, and privately owned and licensed titles. The IT department reserves the right to reject any software installation request for any reason.
6. Software titles are to be installed on company-owned end-user devices by IT Staff or Student Workers, or under their direct supervision, unless permission is obtained for the end user to personally install.
7. All software installed on CTSFW systems (including all commercial and shareware products) must be used in compliance with all applicable licenses, notices, contracts, and agreements. The IT department reserves the right to uninstall any unapproved software from a company-owned machine.

8. The IT department reserves the right to monitor software installation and usage on CTSFW's end-user computing devices. The IT department will conduct periodic audits to ensure compliance with this Software Installation Policy. Unannounced, random spot audits may be conducted as well. During such audits, scanning and elimination of computer viruses may also be performed. Other unsanctioned software may also be uninstalled at this time.

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version ID	Date of Change	Author	Rationale
1.0	12/1/2019	Richard Woodard	New
1.1	12/9/2019	Richard Woodard	Accepted

Concordia Theological Seminary
Fort Wayne, Indiana

Access Control Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	User Authorization, Identification & Authentication Policy, IT Password Policy, Account Management Policy, Physical Access Control Policy
Related Procedures	See Procedures of related Policies.
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary website (www.ctsfw.edu). The latest version will be printed annually at the start of the fiscal year and the physical copy stored in Information Technology. At time of employment, the employee will be referred to the online copy and given signature acceptance form.
Effective Date	December 16, 2019
Next Review Date	July, 2020

Purpose

The purpose of this policy is to ensure users have the appropriate access levels specifically authorized to them to access information on systems and applications.

Scope

This Access Control Policy applies to all business processes and data, information systems and components, personnel, and physical areas of CTSFW.

Definitions

Personnel – All faculty, staff, students, volunteers, contractor and sub-contractors of CTSFW.

Governing Laws & Regulations & Standards

Guidance	Section
ISO/IEC 27001:2013	A.9 (A.9.1, A.9.2, A.9.3, A.9.4)
NIST SP 800-53 v4	AC-1~AC-25
FERPA 34 CFR	99

Policy Statements

Business Requirements of Access Control:

- This access control policy must be developed and reviewed regularly (i.e. annually) based on CTSFW security requirements.
    - CTSFW will employ a role-based access method.
- Users will only receive access to networks and network systems specifically authorized to them.
    - CTSFW will follow the principle of least privilege.

User Access Management:

- A formal user registration and de-registration process must be developed and initiated to allow assignment of rights.
    - CTSFW will employ use of automated mechanisms to enhance this process.
- A formal user provisioning process must be in place. This process will allow for the assignment or revocation of access rights for all users to all systems and services.
- Privileged access rights will be allocated in a highly controlled and restricted process. Their usage will also be controlled.
    - Inactivity logout will be enabled after a pre-determined time period.
- Secret authentication information allocation will be managed through a formal process.
- Asset owners must conduct regular reviews of users' access rights and use of accounts.
- Upon termination of employment, an employee's or external party's user access rights will be revoked.
    - If there is a change to a contract or agreement, then the access will be adjusted appropriately.
    - CTSFW will employ automated processes here to remove temporary and emergency accounts after a determined amount of time. A similar automated process will exist for disabling inactive accounts.
        - CTSFW will also terminate any accounts of high-risk users.

User Responsibilities:

- Users must follow CTSFW's procedures surrounding secret authentication information usage.

System and Application Access Control:

- User access to all information and application systems will be restricted based on CTSFW's access control standards.
    - According to the access control policy, access to systems and applications will be restricted with a secure log-on process.
        - A limit of successive incorrect logons (e.g. six times) will be enforced and an automatic account lock will be enabled.

- Time and date of logons and account changes will be appropriately recorded and monitored.

- Network and information systems sessions should remain locked for a predetermined time or until the user reestablishes access through an established authentication procedure.
- CTSFW will establish appropriate restrictions around remote access, wireless access, and mobile devices.

- Password management systems will be interactive and mandate strong passwords.
- Any use of utility programs capable of overriding system and application controls will be highly controlled and restricted, if necessary.
- Any access to program source code will be strictly prohibited.
- CTSFW will control the flow of information between interconnected systems to ensure secure transfers through measures like encrypted tunnels.
    - When an automated flow control decision is not possible or available, CTSFW will initiate a human review.
- The CTSFW will enact separation of duties to decrease abuse of privileges.
- Access by external information systems will be regulated.
- CTSFW will ensure information sharing process follows appropriate access levels of sharing partners.
    - CTSFW will designate individuals allowed to post information on publicly available systems.
- CTSFW will implement appropriate data mining prevention controls.

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version ID	Date of Change	Author	Rationale

1.0	12/1/2019	Richard Woodard	New
1.1	12/9/2019	Richard Woodard	Accepted

Concordia Theological Seminary
Fort Wayne, Indiana

Account Management Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	IT Password Policy, User Authorization Identification and Authentication Policy, IT Information Security Incident Management Policy, Security Awareness Training Policy
Related Procedures	See procedures of Related Policies.
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	October 1, 2015
Next Review Date	August 2020

Purpose

Information system accounts are the only legitimate method by which *Concordia Theological Seminary's* information systems may be accessed. Without active account management, the potential exists that legitimate users can use these accounts for illegitimate purposes. Additionally, the potential exists that these accounts can be usurped and used illegitimately to access *Concordia Theological Seminary*'s information systems.

Scope

This Account Management Policy applies to all information systems and information system components of *Concordia Theological Seminary*. Specifically, it includes:

- Mainframes, servers and other devices that provide centralized computing capabilities.
- SAN, NAS and other devices that provide centralized storage capabilities.
- Desktops, laptops, tablets, phones and other devices that provide distributed computing capabilities.
- Routers, switches, access points and other devices that provide network capabilities.
- Firewalls, IDP sensors and other devices that provide dedicated security capabilities.
- Third-party Systems

Policy

1. All information system accounts will be actively managed by appropriate account administrators. Active management includes the acts of establishing, activating, modifying, disabling and removing accounts from information systems.
2. Information system accounts are to be constructed such that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with that account. Further, accounts shall be created such that no one account can authorize, perform, review and audit a single transaction to eliminate conflicts of interest where feasible.
3. Information system accounts are to be reviewed to identify accounts with inappropriate privileges (either too high or too low) on at least an annual basis. Should information system accounts be discovered with inappropriate privileges those privileges will be manually reset to the established level.
4. Information systems accounts are to be reviewed to identify inactive accounts. Should information system accounts that are associated with an employee or third party be discovered that have been inactive for *30 days*, the owners of the account will be notified of pending disablement. Should the account continue to remain inactive for *30 more days,* it will be manually disabled.
5. Login attempts to information systems will be restricted such that after *five (5)* failed attempts within a *five (5) minute interval*, they will be locked out. Lockout will be automatically lifted after *thirty (30) minutes* or may be manually lifted by an *identity-verified call to the IT Help Desk*.
6. Third-party systems using critical or personally identifiable information should comply to these standards when practicable.

Procedure 1

Create user accounts to optimize security:

- Accounts must be created with the minimal set of permissions (also known as least privilege) and functions (also known as job segregation) as required by the role. Accounts should be created with the following restrictions:
    - *System administrative access (install, configure, modify and patch system software).*
    - *Account administrative access (create, delete, modify accounts and permissions).*
    - *Review administrative access (review activities of other administrators).*
    - *Full content access (read, write, edit and delete data).*
    - *Limited content access (read, write and edit data).*
    - *Restricted content access (read and write data).*
    - *Minimal content access (read data).*

Procedure 2

Actively manage user accounts on information systems:

- Perform user account review with the data owners to ensure that users are provided with appropriate accounts and account permissions:
    - *Validate each system user's role within the organization.*
    - *Review system accounts and account permissions for each user.*
    - *Validate that each user's account and account permissions meets the requirements established by role.*
- Should account review determine that users have insufficient accounts or account permissions, the required accounts and/or permissions must be provided:
    - *Where accounts exist but permissions are insufficient, modify the account to include appropriate permissions as per the requirements of the positional role.*
    - *Where accounts do not exist, create accounts with appropriate permissions as per the requirements of the positional role.*
    - *Review created accounts and assigned permissions to ensure they meet the requirements of the role.*
- Should account review determine that users have inappropriate accounts or account permissions, those accounts and/or permissions must be rescinded:
    - *Eliminate extraneous permissions in allowed accounts.*
    - *Revoke access to, and eliminate permissions in extraneous accounts.*
    - *Review system logs to catalogue the activity of the account.*
    - *Upon completion of all review and investigation, permanently delete any extraneous accounts.*

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version	Change	Author	Date of Change
1.0	Initial Draft	Richard Woodard	6/8/2015

1.1	First Review	Richard Woodard	7/9/2015
1.2	Accepted	Richard Woodard	9/10/2015
1.3	Change Non-Compliance to match new official standard	Richard Woodard	9/30/2016
1.4	Updated Non-Compliance to match standard adopted October, 2016	Richard Woodard	12/7/2016
1.4.1	Updated Storage Location	Richard Woodard	12/1/2019

Concordia Theological Seminary
Fort Wayne, Indiana

Data Protection Policy

Policy Owner	IT
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Document Retention Policy(In Process), Acceptable Usage Policy, Clear Screen Policy, Clean Desk Policy, Network Security Policy, Removable Media Acceptable Use Policy, Security Awareness Training Policy, Hardware Sanitation Policy, Systems Maintenance Policy
Related Procedures	List other related enterprise procedures both within or external to this
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	11/15/2015
Next Review Date	August 2020

Purpose

Data protection mechanisms allow information to be provided a greater level of security than can be achieved with system-based protection mechanisms alone. Without data protection mechanisms the potential exists that *Concordia Theological Seminary*'s (CTSFW) information assets could be exposed to an unnecessarily high level of risk, particularly in circumstances where data is taken out of the information system.

Scope

This Data Protection Policy applies to all data assets of *CTSFW*. Specifically, it includes:

- Intellectual Property (IP), whether owned by *CTSFW* or provided by a third party.
- Personally Identifiable Information (PII) for personnel, students, clients or other third parties.
- Financial information for *CTSFW*, its personnel, students, clients or other third parties.
- Other non-public data or information assets deemed the property of *CTSFW*.
- Other public data or information assets deemed the property of *CTSFW*.

Policy

1. All privileged information, whether stored in system or out of system (via information media), will be protected by data protection mechanisms to ensure the highest levels of confidentiality, integrity and availability. Non-privileged information will be protected to ensure the highest levels of integrity and availability.
2. Only personnel that have previously been authorized are allowed to enter information into an information system. Inputs will be restricted according to granted permissions, though these restrictions may be lifted on a temporary basis based on pre-defined project responsibilities. In

such circumstances, additional authorization is required and must be granted before restrictions are lifted.

3. Where possible, information systems will check entered information for accuracy, completeness, validity, and authenticity. These checks will be performed as close to the point of information entry as possible and will attempt to ensure that data corruption does not occur or that entered information cannot be interpreted as system commands by the information system.
4. Information systems will be configured such that they prevent unauthorized and unintended information transfer. Further, information systems will protect the integrity and confidentiality of transmitted information using firewall protection from external threats, 2-factor authentication for any external or VPN connection, Windows/Network authentication and access control, encryption of any file containing IP or PII, and full drive encryption (such as SafeGuard/Bitlocker) on laptops that travel often when available. All access across non-secured networks will be done using encrypted communication and secure tunnels.

Procedure 1

Configure systems to store confidential and sensitive data in a secure manner:

- Where possible, data encryption should be used for all confidential data at rest.
- Data encryption solutions should be centrally managed with key escrow.

Procedure 2

Positively dispose of data that is no longer required:

- Use software or hardware delete functions to remove non-confidential data from systems once that data is no longer required.
- Use dedicated media wiping solutions to permanently remove confidential data from systems once that data is no longer required.

Procedure 3

Configure systems to transmit confidential and sensitive data in a secure manner:

- Where possible, encrypted tunnels should be used for all electronic data transmissions.
- Where encrypted tunnels cannot be used for electronic data transmissions, data should be directly encrypted prior to transmission.
- Data encrypted for external transmission should use at least 256-bit AES with a 16-character fully randomized encryption key. The longest possible key should be used, up to the recommended 64-character key.
- Message digest hashes should be created and supplied for all electronic data transmissions.

Procedure 4

Configure systems to restrict and validate data input:

- Data should only be input by those with appropriate accounts and account permissions.
- Data should only be input according to established syntax parameters.

- Inputted data should be checked for accuracy, authenticity, completeness and validity by the system.

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version	Change	Author	Date of Change
1.0	Initial Draft	Richard Woodard	8/13/2015
1.1	Approved(Provisional)	Richard Woodard	10/1/2015
1.2	Approved	Richard Woodard	11/12/2015
1.3	Change Non-Compliance to match new official standard	Richard Woodard	9/30/016
1.4	Updated Non-Compliance to match standard adopted October, 2016	Richard Woodard	12/7/2016
1.5	Semi-Annual review	Richard Woodard	12/8/2016
1.6	Updated Storage Location and Related Policies	Richard Woodard	12/1/2019

Concordia Theological Seminary
Fort Wayne, Indiana

Removable Media Acceptable Use Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Antivirus Policy, Hardware Sanitation Policy, Firewall Policy, Network Security Policy, Data Protection Policy, Physical Access Control Policy, Information Security Incident Reporting and Response Policy, Security Awareness Training Policy
Related Procedures	See Procedures of related Policies
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	December 16, 2019
Next Review Date	July, 2020

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to connect portable removable media to any infrastructure within CTSFW's internal network(s) or related technology resources. This removable media policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Portable USB-based memory sticks, also known as flash drives, or thumb drives, jump drives, or key drives.
- Memory cards in SD, Compact Flash, Memory Stick, or any related flash-based supplemental storage media.
- USB card readers that allow connectivity to a PC.
- Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support data storage function.
- PDAs, cell phone handsets, and smart phones with internal flash or hard drive-based memory that support data storage function.
- Digital cameras with internal or external memory support.
- Removable memory-based media, such as rewritable DVDs, CDs, and floppy disks.
- Any hardware that provides connectivity to USB devices through means such as wireless (Wi-Fi, WiMAX, irDA, Bluetooth, among others) or wired network access.

Scope

This policy applies to all CTSFW personnel, including full and part-time staff, contractors, freelancers, and other agents who utilize either company-owned or personally-owned removable media and/or USB-based technology to store, back up, relocate or access any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust CTSFW has built with its students and other constituents. Consequently, employment at CTSFW does not automatically guarantee the initial and ongoing ability to use these devices within the enterprise technology environment.

Definitions

- USB input device - Any equipment that is plugged into a computer's usb ports to provide input or controls to the computer. Common examples are: keyboard, mouse, trackball, touchpad, and joystick.
- Removable media - Any form of data storage that can be removed from the computer or device. See the classifications in the Purpose section above for a list of applicable devices.
- Major outlet – An established and reputable merchant or online merchant. Examples include Best Buy, Walmart, Staples, Office Depot, Newegg, or Amazon. Note that eBay does not qualify in this category, as products are supplied by un-vetted 3rd parties.
- Volatile Memory – Any form of computer memory whose contents are erased when power is lost. Memory listed as RAM, DRAM, SDRAM, SDR. DDR, GDDR, HBM, SRAM DIMM, SIMM, or SO-DIMM is considered volatile.
- Quarantine – Any removable media that has been exposed to devices outside the seminary network are considered suspect, and cannot be plugged into a seminary device without being sanitized. Such a device is referred to as in quarantine.

Policy Statements

1. **No removable media of unknown or suspect origin is to be inserted into a seminary-owned device.**
2. Removable media of known origin, and which have not been used outside seminary equipment may be plugged in or inserted regularly.
3. Removable media of unknown or suspect origin, or from a source outside CTSFW may be sanitized by IT to allow data to be used.
   - IT has established devices and quarantine computers to allow for sanitation of suspect media.
   - Bring any suspect media to the IT Helpdesk in B-18 to be sanitized.
4. Certain USB devices and other media can be considered as a trusted source and plugged into system. This list is limited to:
   - USB Input devices purchased NEW from a major outlet.
   - Media purchased NEW from a major outlet in sealed packaging.
   - Any volatile memory such as RAM or DIMM. Note, memory should only be installed by IT.
   - Installation media provided by a reputable software company.

5. As CTSFW has no control of 3rd-party network security, any media received from a source other than those listed above cannot be considered as trusted.
6. Public computers such as those located in the general areas of the library are considered suspect.

Access Control

1. IT reserves the right to refuse, by physical and non-physical means, the ability to connect removable media and USB devices to corporate and corporate-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts the seminary's systems, data, users, and constituents at risk.

2. Prior to initial use on the corporate network or related infrastructure, all USB-related hardware and related software must be authorized by IT.

3. End users who wish to connect such devices to non-corporate network infrastructure to gain access to enterprise data must employ, for their devices and related infrastructure, a company-approved personal firewall and any other security measure deemed necessary by the IT department. Enterprise data is not to be accessed on any hardware that fails to meet CTSFW's established enterprise IT security standards.

4. Any device not explicitly mentioned in the policy statements may **NOT** be connected to seminary infrastructure

Security

1. Personnel using removable media and USB-related devices and related software for data storage, back up, transfer, or any other action within CTSFW's technology infrastructure will, without exception, use secure data management procedures. A simple password is insufficient. See the CTSFW's password policy and data protection policy for additional background. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.

2. All USB-based devices that are used for business interests must be pre-approved by IT, and must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data. Any non-corporate computers used to synchronize with these devices will have installed whatever anti-virus and anti-malware software is deemed necessary by CTSFW's IT department, and must conform to all CTSFW IT Policies and Procedures.. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be used must be updated in accordance with existing company policy.

3. No seminary data on a removable media may be transferred to permanent storage of any non-seminary device. If it is necessary to use the data on a non-seminary device, it may not be saved onto any media other than the source removable media.

4. All removable media will be subject to quarantine upon return to the office before they can be fully utilized on enterprise infrastructure.

5. Passwords and other confidential data as defined by CTSFW's IT department are not to be stored on portable storage devices.
6. End users must apply new passwords every business/personal trip where company data is being utilized on USB-based memory devices.

7. Any USB-based memory device that is being used to store CTSFW data must adhere to the authentication requirements of CTSFW's IT department. In addition, all hardware security configurations (personal or company-owned) must be pre-approved by CTSFW's IT department before any enterprise data-carrying memory can be connected to it.

8. Personnel, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once their use is no longer required. See Hardware Sanitation Policy for detailed data wipe procedures.

Help & Support

1. CTSFW's IT department will support its sanctioned hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media. This applies even to devices already known to the IT department.

2. Personnel, contractors, and temporary staff will make no modifications of any kind to seminary-owned and installed hardware or software without the express approval of CTSFW's IT department. This includes, but is not limited to, reconfiguration of USB ports.

3. IT may restrict the use of Universal Plug and Play on any client PCs that it deems to be particularly sensitive. IT also reserves the right to disable this feature on PCs used by personnel in specific roles.

4. IT reserves the right to summarily ban the use of these devices at any time. IT need not provide a reason for doing so, as protection of confidential data is the highest and only priority.

5. IT reserves the right to physically disable USB ports to limit physical and virtual access.

6. IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.

Organizational Protocol

1. IT can and will establish audit trails in all situations it feels merited. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to CTSFW's networks may be monitored to record dates, times, duration of access, etc. in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains CTSFW's highest priority.

2. The end user agrees to immediately report to his/her manager and CTSFW's IT department any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc. See the Information Security Incident Reporting and Response Policy.

3. CTSFW will not reimburse employees if they choose to purchase their own USB-based memory devices.
4. Any questions relating to this policy should be directed to the IT Helpdesk, at x3178 or helpdesk@ctsfw.edu

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version ID	Date of Change	Author	Rationale
1.0	12/1/2019	Richard Woodard	New
1.1	12/9/2019	Richard Woodard	Accepted

Concordia Theological Seminary
Fort Wayne, Indiana

Hardware Sanitization Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Antivirus Policy, Network Security Policy, Data Protection Policy, Physical Access Control Policy, Information Security Incident Reporting and Response Policy, Removable Media Acceptable Use Policy, Security Awareness Training Policy
Related Procedures	See Procedures of related Policies
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	December 16, 2019
Next Review Date	July, 2020

Purpose

The quality and integrity of CTSFW's hardware sanitization policy is the basis for sound decision-making. As a result, the purpose of this policy is to protect the intellectual property of CTSFW and the confidentiality of personal information. It defines standards and procedures for the pre-disposal data sanitization of CTSFW's hardware.

Scope

The policy applies to all hardware owned or leased by CTSFW and capable of storing CTSFW's intellectual property or information related to the privacy of CTSFW's employees, clients, or suppliers.

- Portable and notebook computers.
- Workstations and desktop computers.

The following devices and storage media are not specifically addressed by the terms of this policy, but must be sanitized accordingly:

- Servers should be backed up and sanitized in accordance with vendor recommendations. If the vendor has not provided recommendations, servers can be sanitized as workstations.
- Mobile devices, such as PDAs and smart phones, must be destroyed by crushing, incineration, shredding, or melting prior to disposal.
- Removable storage media such as flash memory devices, floppy disks, optical CD and DVD media, tape, and other long-term storage media must be destroyed by incineration, shredding, or melting prior to disposal.

Governing Laws & Regulations

Guidance	Section

ISO27001:2013	A.16.1
NIST SP 800-53 v4	AU-6, IR-1, IR-6, CA-2, CA-7, PL-4, SA-5, SA-11, SI-2, SI-5, IR-4, IR-10, AU-7, AU-8, AU-9, AU-11
NIST SP 800-88 V1	1, 2, 3, 4
FERPA 34 CFR	99

Policy Statements

1. Consult with the IT department prior to disposing of any computer equipment. Richard Woodard is the primary contact for sanitization issues. They will provide an approved sanitization tool and assistance in properly sanitizing the hardware. Richard Woodard or their designee must sign a certification that the equipment has been properly sanitized before it can be surplussed, transferred, or donated. Copies of all certification statements should be maintained by IT staff.
2. Sanitation will be conducted in accordance with NIST Special Publication 800-88, utilizing a minimum DOD 3-pass erasure.

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version ID	Date of Change	Author	Rationale
1.0	12/1/2019	Richard Woodard	New
1.1	12/9/2019	Richard Woodard	Accepted

Concordia Theological Seminary
Fort Wayne, Indiana

Personal Device Acceptable Use Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Antivirus Policy, Hardware Sanitation Policy
Related Procedures	
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	December 16, 2019
Next Review Date	July, 2020

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who are connecting a personally-owned device to CTSFW's corporate network for business purposes. This device policy applies, but is not limited to all devices and accompanying media (e.g. USB thumb and external hard drives) that fit the following classifications:

- Smartphones
- Other mobile/cellular phones
- Tablet computers
- Portable media devices
- PDAs
- Ultra-mobile PCs (UMPCs)
- Laptop/notebook computers, including home desktops
- Any personally-owned device capable of storing corporate data and connecting to a network

The policy applies to any hardware and related software that is not corporately owned or supplied, but could be used to access corporate resources. That is, devices those employees have acquired for personal use but also wish to use in the business environment.

The overriding goal of this policy is to protect the integrity of the confidential client and business data that resides within CTSFW's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a device or carried over an insecure network where it could potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to the company's public image. Therefore, all users employing a personally-owned device connected to CTSFW's

corporate network, and/or capable of backing up, storing, or otherwise accessing corporate data of any type, must adhere to company-defined processes for doing so.

Scope

This policy applies to all CTSFW personnel, including full and part-time faculty, staff, contractors, freelancers, volunteers, and other agents who use a personally-owned device to access, store, back up, or relocate any organization, constituent, or student-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust CTSFW has built with its students and other constituents. Consequently, employment at CTSFW does not automatically guarantee the initial or ongoing ability to use these devices to gain access to corporate networks and information.

Definitions

- Intellectual property (IP) refers to creations of the mind, such as inventions, literary and artistic works, designs and symbols, names, and images.
- Personally Identifiable Information (PII). The term "PII," refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
- Private or sensitive Information (PI) - Computer Definition Information that a user wishes to keep from public viewing. Credit card, social security and financial account numbers, along with passwords to websites and other venues, are commonly kept private.

Stipend Guidelines

CTSFW maintains a reimbursement stipend for personnel who use their own telephone/smartphone for CTSFW business. See the HR Personnel Handbook for further details.

Policy Statements

It is the responsibility of any personnel of CTSFW who uses a personal device to access business resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct CTSFW business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this requirement, the following rules must be observed:

General Policy

1. PI, PII, and IP may only be stored on CTSFW-owned devices.
2. Personal devices are allowed for Seminary Web Applications, Email, Phone Apps, and Remote Access.
3. Personal mobile devices may be connected the Seminary wireless for data and communication access.

Access Control

1. IT reserves the right to refuse, by physical and non-physical means, the ability to connect personal devices to corporate and corporate-connected infrastructure. IT will engage in such action if such equipment is being used in a way that puts the company's systems, data, users, and clients at risk.
2. Prior to initial use on the corporate network or related infrastructure, **all devices must be approved by IT.** Devices that are not approved may not be connected to corporate infrastructure. Contact the help desk at helpdesk@ctsfw.edu or x3178 and create a ticket for approval.
3. End users who wish to connect such devices to non-corporate network infrastructure to gain access to enterprise data **must employ,** for their devices and related infrastructure, security measures deemed necessary by the IT department. Enterprise data is not to be stored on or accessed from any hardware that fails to meet CTSFW's established enterprise IT security standards.
4. All personal devices attempting to connect to the corporate network through the Internet will be inspected using technology centrally managed by CTSFW's IT department. Devices that have not been previously approved by IT, are not in compliance with its security policies, or represent any threat to the seminary network or data will not be allowed to connect.

Security

Personnel using personally-owned devices and related software for network and data access will, without exception, use secure data management procedures. **All devices that are able to store data must be protected by a strong password;** a PIN is not sufficient. All data stored on the device must be encrypted using **strong encryption.** See CTSFW's Password Policy and Data Protection Policy for additional background. Personnel agree never to disclose their passwords to anyone, including family members, or store passwords on personally-owned devices if business work is conducted from home.

1. All users of personally-owned devices **must employ reasonable physical security measures.** End users are expected to secure all such devices whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data.
2. Any non-business computers used to synchronize with these devices will have installed **up-to-date anti-virus and anti-malware software deemed necessary** by CTSFW's IT department. See Antivirus Policy.
3. Passwords and other confidential data as defined by CTSFW's IT department are **not to be stored unencrypted** on mobile devices.
4. Any device that is being used to store CTSFW data must **adhere to the authentication requirements** of CTSFW's IT department. In addition, all hardware security configurations must be pre-approved by CTSFW's IT department before any enterprise data-carrying device can be connected to the corporate network.
5. IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. **Any attempt to contravene or bypass that security**

implementation will be deemed an intrusion attempt and will be dealt with in accordance with CTSFW's overarching security policy.

6. IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.
7. Personnel, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to **permanently erase company-specific data from such devices once its use is no longer required**. See Hardware Sanitation Policy for detailed data wipe procedures for eligible devices.
8. In the event of a lost or stolen device, it is incumbent on the user to report the incident to IT immediately.

Help & Support

1. Personal devices are not eligible for support for device-specific hardware or software from CTSFW's IT department. If the employee-owned device requires maintenance, the employee is responsible for taking the device to an employee-provided third.

Organizational Protocol

1. IT can and will establish audit trails, which will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to the corporate network, and the resulting reports may be used for investigation of possible breaches and/or misuse. **The end user agrees to and accepts that his or her access and/or connection to CTSFW's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity.** This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties.
2. The end user agrees t**o immediately report** to his/her manager and CTSFW's IT department **any incident or suspected incidents of unauthorized data access**, data loss, and/or disclosure of company resources, databases, networks, etc.

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version ID	Date of Change	Author	Rationale
1.0	12/1/2019	Richard Woodard	New
1.1	12/9/2019	Richard Woodard	Accepted

Concordia Theological Seminary
Fort Wayne, Indiana

Systems Maintenance Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Data Protection Policy
Related Procedures	
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	3/1/2016
Next Review Date	August 2020

Purpose

Information system maintenance is required to ensure that information systems are always operating optimally. Set maintenance processes are required to ensure that maintenance is conducted in the most secure manner possible. Without systems maintenance the potential exists that information systems will be unable to provide appropriate information security. Without maintenance processes the potential exists that the act of performing systems maintenance could, either directly or indirectly, compromise information system security.

Scope

This Systems Maintenance Policy applies to all information systems and information system components of *Concordia Theological Seminary, Fort Wayne*. Specifically, it includes:

- Mainframes, servers and other devices that provide centralized computing capabilities.
- SAN, NAS and other devices that provide centralized storage capabilities.
- Desktops, laptops and other devices that provide distributed computing capabilities.
- Routers, switches and other devices that provide network capabilities.
- Firewalls, IDP sensors and other devices that provide dedicated security capabilities.

Policy

1. Routine preventative and regular maintenance (including repairs) on information systems shall be scheduled with *two days'* notification to ensure business units have sufficient notice and that conflicts are avoided. Maintenance shall be performed in accordance with manufacturer/vendor specifications and/or organizational requirements.
2. Only pre-authorized personnel are allowed to perform information system maintenance. If maintenance personnel do not have sufficient facilities or information systems access authorization, they shall be accompanied at all times by personnel that do.

3. Remote maintenance must be authorized, actively monitored and audited upon completion. Remote maintenance must make use of appropriate risk mitigation techniques that include *suggest encrypted communications and strong authentication two-factor authentication*.
4. A maintenance log shall be maintained for all information system maintenance.

Procedure 1

Ensure appropriate notification prior to the initiation of scheduled security operations:

- Issue notification of maintenance requirements to affected users and solicit response. All notifications should include the following information:
  - *Nature of the work.*
  - *Reason for the work.*
  - *Scheduling of the work.*
- Issue maintenance plans to person performing maintenance functions and overview and solicit response. All works plans should include the following information:
  - *Tasks involved in the work.*
  - *Contact plans to be followed during the work.*
  - *Rollback plans in the event of failure of the work.*
- Provide update notifications throughout maintenance operations. Work plans will include a notification schedule that includes the following:
  - *The individuals to be notified.*
  - *The individuals to provide the notification.*
  - *The milestones at which notification will occur.*
  - *The method through which notification will occur.*

Procedure 2

System maintenance must be conducted in a manner that neither contravenes security while being performed nor degrades security once complete:

- Where remote maintenance is allowed additional security measures will be utilized. These will include:
  - *All active connections as well as the system being maintained will be actively monitored.*
  - *Remote maintenance will be performed over encrypted tunnels only.*
  - *Tunnels should be positively terminated upon completion of all work.*
- A maintenance log will be completed for all maintenance work. This will record:
  - *Affected system.*
  - *Date and time of scheduled maintenance.*
  - *Description of the work performed.*
  - *Listing of any equipment removed or replaced.*
  - *Name and organization of person performing the maintenance.*
  - *Identity verification mechanism used.*
  - *Name of escort.*

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version	Change	Author	Date of Change
1.0	First Draft	Richard Woodard	2/1/2016
1.1	Accepted	Richard Woodard	2/11/2016
1.2	Change Non-Compliance to match new official standard	Richard Woodard	9/30/2016
1.3	Updated Non-Compliance to match standard adopted October, 2016	Richard Woodard	12/7/2016
1.3.1	Updated Storage Location		

Concordia Theological Seminary
Fort Wayne, Indiana

Systems Monitoring & Auditing Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies & Procedures Committee
Related Policies	System Owner Authorization, Acceptable Usage, Privacy Policy, Account Management
Related Procedures	
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	3/15/2016
Next Review Date	August 2020

Purpose

System monitoring and auditing is used to determine if inappropriate actions, either intentional or unintentional, have occurred within an information system. System monitoring is used to look for these inappropriate actions in real time while system auditing looks for them after the fact. Without system monitoring and auditing it can be difficult, if not impossible, to determine when a failure of the information system security, or a breach of the information systems itself has occurred, the magnitude of the breach or failure, and the details of that breach or failure.

Scope

This Systems Monitoring & Auditing Policy applies to all information systems and information system components of Concordia Theological Seminary, Fort Wayne (CTSFW). Specifically, it includes:

- Mainframes, servers, and other devices that provide centralized computing capabilities.
- SAN, NAS, and other devices that provide centralized storage capabilities.
- Desktops, laptops, smart phones, tablets, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- Firewalls, IDP sensors, and other devices that provide dedicated security capabilities.
- Cloud services, including but not limited to, infrastructure as a service, platform as a service, and/or software as a service.

Policy

1. Information systems will be configured to record login/logout and all administrator activities into a log file. Additionally, information systems will be configured to notify administrative personnel in the event that inappropriate, unusual and/or suspicious activity is noted. Inappropriate, unusual, and/or suspicious activity will be fully investigated by appropriate administrative personnel and findings reported to appropriate security management personnel

2. Information systems are to be provided with sufficient primary (on-line) storage to retain 30 days' worth of log data and sufficient secondary (off-line) storage to retain 1 year's worth of data. If primary storage capacity is exceeded, the information system will be configured to overwrite oldest logs. In the event of other logging system failures, the information system will be configured to notify administrator.
3. System logs shall be manually reviewed as needed. Inappropriate, unusual, and/or suspicious activity will be fully investigated by appropriate administrative personnel and findings reported to appropriate security management personnel.
4. System logs are considered confidential information. As such all access to system logs and other system audit information requires prior authorization and strict authentication. Further, access to logs or other system audit information will be captured in the logs.
5. In the case of individual workstations, a spot-check of selected computer logs may be made for unusual and/or suspicious activity.

Procedure 1

Systems must be configured to generate logs and those logs must be configured to capture required information:

- Configure logging capabilities to capture, at a minimum, all system access events and all system administrative events. The following data points should be captured for each log event entry:
  - Date and time of the event.
  - Component of the system affected by the event (if logging at the system level rather than component level).
  - Identity information of the individual that triggered the event.
  - Information describing the outcome of the event.

Procedure 2

Logs are useful in the investigation of a previously discovered security incident and to discern previously undiscovered security incidents so periodic log review should be performed:

- Full logs generated for information systems should be reviewed as needed.
- Where sufficient resources for full log review do not exist, partial random log review should be performed:
  - A randomly determined subset of all systems should be reviewed.
  - A randomly determined subset of all log entries should be reviewed.
  - Random review should be structured such that every system or every log entry type should be reviewed periodically.

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version	Change	Author	Date of Change
1.0	Initial Draft	Richard Woodard	2/11/2016
1.1	Accepted	Jason Iwen	3/10/2016
1.2	Change Non-Compliance to match new official standard	Richard Woodard	9/30/2016
1.4	Updated Non-Compliance to match standard adopted October, 2016	Richard Woodard	12/7/2016
1.5			

Concordia Theological Seminary
Fort Wayne, Indiana

Physical and Environmental Security Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Physical Access Control Policy
Related Procedures	
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary website (www.ctsfw.edu). The latest version will be printed annually at the start of the fiscal year and the physical copy stored in Information Technology. At time of employment, the employee will be referred to the online copy and
Effective Date	February 1, 2019
Next Review Date	August, 2020

Purpose

The purpose of this policy is to ensure proper measures are in place to prevent unauthorized physical access or damage to Concordia Theological Seminary's (CTSFW) information and facilities.

Scope

This Physical and Environmental Security Policy applies to all business processes and data, information systems and components, personnel, and physical areas of CTSFW.

Policy

Physical Access and Security:

- Physical security perimeters will be identified and will protect mission critical information or facilities.
- Appropriate entry controls will be implemented at secure access points to ensure only individuals with appropriate access levels are allowed access. These access points will be monitored.
    - CTSFW should develop, approve, and maintain a list of personnel with authorized access to the facility where information systems are physically located.
    - CTSFW should establish a process to review, approve, and issue credentials for facility access.
    - Information Technology shall remove individuals from the facility access list when access is no longer required.
    - CTSFW should maintain physical access audit logs for data center(s) and/or sensitive facilities entry/exit points.
- Security measures will be implemented for working in various identified safe spaces and delivery and loading spaces.

Environmental Security:

- Protection against natural disasters or other malicious attacks, as well as accidental incidents, will be determined and implemented.
- CTSFW should place power equipment and cabling in safe locations to prevent environmental and/or man-made damage and destruction.
- Applicable security measures will be implemented for offices, boardrooms, etc., including considerations for temperature, protection against water damage, and emergency lighting.

Equipment Security:

- Equipment will be handled and protected to ensure risks are reduced, preventing potential environmental threats and hazards.
- Redundancies and other supporting procedures will be put in place to protect from power failures and other disruptions, including ensuring power and telecommunications cabling carrying data will be properly protected.
- Equipment will be regularly maintained.
- Any removal of assets must be done with prior authorization from the appropriate party.
- Any offsite assets will be treated with the same security measures, with special consideration to risks of being off-premise.
- Disposal or re-use of equipment must be done after the removal of sensitive or critical data has been completed.
- Any unattended equipment must have applicable protection.
- Personnel are responsible for maintaining their personal workspaces and ensuring media or literature containing sensitive or critical information is properly stored and not in the open.

Guidance

Guidance	Section
ISO27001:2013	A.11 (A.11.1, A.11.2)
NIST SP 800-53 v4	PE-2~PE-6, MA-5, PE-8, CP-2, CP-6, CP-7, PE-1, CP-8, PE-19~PE-16, MA-2~MA-6, AC-19, AC-20, MP-5, PE-17, MP-6, MA-2, MP-5

Revision History

Ver.	Version Name	Authored by	Date
1.0	Initial draft	CISO Division of Information Security	9/25/2013
1.0	Final version – no changes from initial draft	CISO Division of Information Security	2/10/2014
2.0	Adapted for CTSFW	Richard Woodard	12/7/2016
2.1	Final Draft	Richard Woodard	2/5/2019

2.2	Accepted	Richard Woodard	2/22/2019
2.3	Updated Storage Location	Richard Woodard	12/1/2019

Concordia Theological Seminary
Fort Wayne, Indiana

Physical Access Control Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Physical and Environmental Security Policy, Hardware Sanitation Policy, Removable Media Acceptable Use Policy, Security Awareness Training Policy
Related Procedures	
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	March 1, 2019
Next Review Date	August 2020

Purpose

Physical access controls define who is allowed physical access to facilities that house information systems, to the information systems within those facilities and/or the display mechanisms associated with those information systems. Without physical access controls, the potential exists that information systems could be illegitimately physically accessed and the security of the information they house could be compromised.

Scope

This Physical Access Control Policy applies to all facilities of Concordia Theological Seminary, Fort Wayne (CTSFW) within which information systems or information system components are housed. Specifically, it includes:

- Data centers or other facilities for which the primary purpose is the housing of IT infrastructure.
- Data rooms or other facilities within shared purpose facilities for which one of the primary purposes is the housing of IT infrastructure.
- Switch and wiring closets or other facilities for which the primary purpose is not the housing of IT infrastructure.

Policy

1. Access to facilities, information systems and information system display mechanisms will be limited to authorized personnel only. Authorization will be demonstrated through the use of authorization credentials that have been issued by CTSFW.

2. Access to facilities will be controlled at defined access points through the use of locked doors or personnel review. Authorized personnel are required to authenticate themselves at these access points before physical access to facilities, information systems or information system display mechanisms is allowed. The delivery and removal of

information systems will also be controlled at these access points. No equipment will be allowed to enter or leave the facility without prior authorization and all deliveries and removals will be logged.

3. A list of authorized personnel will be established and maintained such that newly authorized personnel are immediately appended to the list and those personnel whose authorization has been revoked are immediately removed from the list. This list shall be reviewed and, where necessary, updated on an at least annual basis.
4. In the event that visitors need access to the facilities that house information systems or to the information systems themselves, those visitors must have prior authorization, must be positively identified, and must have their authorization verified before physical access is granted. Once access has been granted, visitors must be escorted and their activities monitored at all times.

Procedure 1

Authorize, identify and authenticate individuals that require physical access:

- Identify the roles that require both regular as well as occasional physical access and identify the individuals that fill these roles.
- Provide standing authorization and a permanent authenticator to individuals that require regular access.
- Require individuals that require occasional access to submit a request that must be approved prior to access being attempted or allowed.
- Authenticate individuals with regular access requirements through the use of their assigned permanent authenticator.
- Authenticate individuals with occasional access requirements through the use of a personal identification mechanism that includes name, signature and photograph.

Procedure 2

Verify that work to be performed has been pre-approved or meets emergency response procedures:

- Verify against standard Change Control procedures.
- Verify against standard Maintenance procedures (Insert policy name here).

Procedure 3

Make use of logs to document the coming and goings of people and equipment:

- Assign the responsibility for the maintenance of an access log that records personnel access. Record the following:
    - *Date and time of entry.*

- *Name of accessing individual and authentication mechanism.*
- *Name and title of authorizing individual.*
- *Reason for access.*
- *Date and time of departure.*

- Assign the responsibility for the maintenance of a delivery and removal log that records equipment that is delivered to or removed from facilities; Record the following:
  - *Date and time of delivery/removal.*
  - *Name and type of equipment to be delivered or removed.*
  - *Name and employer of the individual performing the delivery/removal and the authentication mechanism used.*
  - *Name and title of authorizing individual.*
  - *Reason for delivery/removal.*

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Version	Change	Author	Date of Change
1.0	Initial Draft	Richard Woodard	12/7/2016
1.1	Final Version	Richard Woodard	2/5/2019
1.2	Accepted	Richard Woodard	2/22/2019
1.2.1	Updated Storage Location	Richard Woodard	12/1/2019

Concordia Theological Seminary
Fort Wayne, Indiana

Information Security Incident Management Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Information Security Incident Reporting and Response Policy, IT Application Security Policy(In Process), Password Policy, IT Firewall Policy, IT Anti-Virus Policy, IT Network Security Policy, Data Privacy Policy, Data Protection Policy, Systems Monitoring Auditing Policy
Related Procedures	See procedures for policies listed above
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	November 1, 2016
Next Review Date	August 2020

Purpose

The purpose of this policy is to ensure proper and consistent recognition, management, and communication of security incidents and weaknesses through a formal process.

Scope

This Information Security Incident Management Policy applies to all personnel, business processes and data, information systems and components using CTSFW information technology resources or data, and to physical areas of CTSFW.

Definitions

Personnel – All users of all information system that are the property of CTSFW. Specifically, it includes:

- All faculty, staff and student workers, whether employed on a full-time or part-time basis by CTSFW.
- All contractors and third parties that work on behalf of and are paid directly by CTSFW.
- All contractors and third parties that work on behalf of CTSFW but are paid directly by an alternate employer.
- All employees of partners and clients of CTSFW that access CTSFW's non-public information systems.
- All volunteer workers that work on behalf of CTSFW.
- All students attending CTSFW.

Security Incident – Any real or suspected event that may adversely affect the security of CTSFW information or the systems that process, store, or transmit that information. Examples include:

- Unauthorized access to data, especially confidential data like a person's name and social security number
- Computer infected with malware such as a worm, virus, Trojan Horse, or botnet
- Reconnaissance activities such as scanning the network for security vulnerabilities
- Denial of Service attack
- Web site defacement
- Violation of a CTSFW security policy
- Security weakness such as an un-patched vulnerability

Personally identifiable information (PII) – The US government officially defines PII as "Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." Divulgence of student and family PII is subject to FERPA governance found online at http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferparegs.pdf . PII includes, but is not limited to :an individual's name; date of birth; address; telephone number; driver's license number or card or non-driver's identification number or card; social security number or card; place of employment; employee identification numbers or other personal identification numbers or cards; mother's maiden name; birth, death or marriage certificates; electronic identification numbers; electronic signatures; and any financial number, or password that can be used to access a person's financial resources, including, but not limited to, checking or savings accounts, credit or debit card information, demand deposit or medical information, or ones name in combination with a passport number.

Confidential Data - Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know.

Incident Manager – The person responsible for managing the response to a security incident as defined in the incident response summary table below.

Executive Incident Management Team - oversees the handling of security incidents involving confidential data (e.g., Personally Identifiable Information). This team has authority to make decisions related to the incident and to notify appropriate parties. The team consists of:

- VP in charge of the affected department
- Chief Information Officer (CIO)
- Information Security Specialist (ISS)
- CTSFW Legal Counsel
- Director of Seminary Relations

- Others as needed (i.e. Law Enforcement)

Policy

Incident response will be handled appropriately based on the type and severity of the incident in accordance with the Incident Response Summary Table below. The Incident Management Team will respond based on the Incident Severity and Response Time to **analyze** the incident, **contain** the breach, **eradicate** the vulnerability, **recover** data and follow-up with **Post-Incident Activity and reporting**.

Handling of security incidents involving confidential data will be overseen by an Executive Incident Management Team.

All individuals involved in investigating a security incident should maintain confidentiality, unless the Chief Information Officer authorizes information disclosure in advance.

Procedures

This Information Security Incident Management Policy applies to all business processes and data, information systems and components, personnel, and physical areas of CTSFW.

Security Incident Classification System

Security incidents will be classified according to incident categories and severity of incident in order to determine the appropriate response. A security incident classification scheme will be maintained by the Information Security Specialist (ISS) to describe security events and support incident tracking over time.

INCIDENT CATEGORIZATION SUMMARY			
	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations,	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations,	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational

authenticity. [44 U.S.C., SEC. 3542]	organizational assets, or individuals.	organizational assets, or individuals.	operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Incident Categories

The following categories will be used to describe IT security incidents at CTSFW. Several categories may apply to a single incident. The examples listed in each category are not meant to be exhaustive.

Confidential personal identity data exposure

Social Security Numbers with or without names

Credit Card information

Identity theft

Other

Criminal activity/investigation

Subpoena, search warrant, or other court order

Litigation hold request (aka e-Discovery)

Online theft, fraud

Threatening communication

Child pornography

Physical theft, break-in

Denial of Service

Single or distributed (DoS or DDoS)

Inbound or outbound

Digital Millennium Copyright Act (DMCA) violation

Official DMCA notification from copyright owner or legal representative

Illegal distribution of copyrighted or licensed material (movies, music, software, games)

Illegal possession of copyrighted or licensed material

Malicious code activity

Worm, virus, Trojan

Botnet

Keylogger

Rootkit

Policy violation

CTSFW policy violation

Violation of student code of conduct

Personnel action/investigation

Reconnaissance activity

Port scanning

Other vulnerability scanning

Unauthorized monitoring

Rogue server or service

Rogue file/FTP server for music, movies, pirated software, etc.

Phishing scam web server

Botnet controller

Spam source

Spam relay

Spam host

CTSFW computer on a block list

Spear Phishing

Scam e-mail specifically targeting a CTSFW e-mail addresses that tries to trick people into divulging private information

Unauthorized access

Abuse of access privileges

Unauthorized access to data

Unauthorized login attempts

Brute force password cracking attempts

Stolen password(s)

Un-patched vulnerability

Vulnerable operating system

Vulnerable application

Vulnerable web site/service

Weak or no password on an account

Web/BBS defacement

Defacement of web site

Inappropriate post to BBS, wiki, blog, etc.

Redirected web site

No Incident

When investigation of suspicious activity finds no evidence of a security incident

Incident Severity

The severity of incident is a subjective measure of its impact on or threat to the operation or integrity of the institution and its information. It determines the priority for handling the incident, who manages the incident, and the timing and extent of the response.

The following factors are considered in determining the severity of an incident:

Scope of impact – how many people, departments, or systems does it affect?

Criticality of the system or service – how important is it to the continuing operation of the institution? What would be the impact on the business, either functional or financial, if this system or service were unavailable or corrupted?

Sensitivity of the information stored on or accessed through the system or service – does it contain confidential data, such as Personally Identifiable Information or credit card information?

Probability of propagation – how likely is it that the malware or negative impact will spread or propagate to other systems, especially to other systems off campus?

Three levels of incident severity will be used to guide incident response: high, medium, and low.

High

The severity of a security incident will be considered "high" if any of the following conditions exist:

Threatens to have a significant adverse impact on a large number of systems and/or people (for example, the entire institution is affected)

Poses a potential large financial risk or legal liability to the Seminary

Threatens confidential data (for example, the compromise of a server that contains names with social security numbers or credit card information)

Adversely impacts an enterprise system or service critical to the operation of a major portion of the Seminary (for example, e-mail, student information system, financial information system, human resources information system, learning management system, Internet service, or a major portion of the campus network)

Poses a significant and immediate threat to human safety, such as a death-threat to an individual or group.

Has a high probability of propagating to many other systems on campus and/or off campus and causing significant damage or disruption

High severity incidents require an immediate response and focused, dedicated attention by the ISS and other appropriate Seminary officials and IT security staff until remediated. These incidents also have extensive notification and reporting requirements, as outlined in the Incident Response Summary Table below. A Post-Incident Report is required.

Medium

The severity of a security incident will be considered "medium" if any of the following conditions exist:

Adversely impacts a moderate number of systems and/or people, such as an individual department, unit, or building

Adversely impacts a non-critical enterprise system or service

Adversely impacts a departmental system or service, such as a departmental file server

Disrupts a building or departmental network

Has a moderate probability of propagating to other systems on campus and/or off campus and causing moderate damage or disruption

Medium severity incidents require a quick response by appropriate personnel (usually from the affected unit) who have primary responsibility for handling the incident. Notification requirements are outlined in the Incident Response Summary Table below. A Post-Incident Report is not required unless requested by the Chief Information Officer or other appropriate administrator.

Low

Low severity incidents have the following characteristics:

Adversely impacts a very small number of systems or individuals

Disrupts a very small number of network devices or segments

Has little or no risk of propagation or causes only minimal disruption or damage in their attempt to propagate

Since a single compromised system can "wake up" and negatively affect other systems at any time, appropriate personnel (usually the technical support staff responsible for the system) must respond as quickly as possible, no later than the next business day. Notification requirements are outlined in the Incident Response Summary Table In the. A Post-Incident Report is not required unless requested by the CIO.

Incident Response Summary Table

INCIDENT RESPONSE SUMMARY					
INCIDENT See Incident Categorization Summary above		**RESPONSE**			
Potential Impact	**Characteristics** Any condition met qualifies	**Response Time**	**Incident Manager**	**Who to Notify**	**Post-Incident Report Required**

High	Significant adverse impact on a large number of systems and/or people Potential large financial risk or legal liability to the Seminary Threatens confidential data Adversely impacts a critical enterprise system or service Significant and immediate threat to human safety High probability of propagating to a large number of other systems on or off campus and causing significant disruption	Immediate	Chief Information Officer , Information Security Specialist or Incident Management Team	Chief Information Officer Information Security Specialist Unit VP Department head Tech Support for affected system	Yes
Medium	Adversely impacts a moderate number of systems and/or people Adversely impacts a non-critical enterprise system or service Adversely impacts a departmental scale system or service Disrupts a building or departmental network Moderate risk of propagating and causing further disruption	4 Hours	Appointed by unit VP	Information Security Specialist Unit VP Department Head Tech Support for affected system	No, unless requested by CIO, ISS or other appropriate administrator
Low	Adversely impacts a very small number of non-critical individual systems, services, or people Disrupts a very small number of network devices or segments Little risk of propagation and further disruption	Next Day	Technical Support for affected system	Information Security Specialist Department Head Tech Support for affected system	No

Security Incident Reporting and Detection

Security Incident Reporting

All members of the Seminary community are responsible for promptly reporting suspected or known security incidents, including an observed or suspected security weakness in CTSFW systems or services, in accordance with CTSFW's IT Security Reporting and Response Policy.

All suspected high severity incidents, including those involving possible breaches of Personally Identifiable Information, must be reported directly to the Information Security Specialist (ISS) as quickly as possible by phone (preferred), email, or in person:

If the ISS is not available, contact CTSFW's Chief Information Officer (CIO)

All other suspected incidents must also be reported to any of the following:

Send email to infotech@CTSFW.edu

Contact the ISS

Contact the IT Helpdesk. Any incident that is not high severity may be reported first to department VP before reporting it to the people listed above.

Warning: If reporting a suspected security weakness or system vulnerability, do not attempt to confirm it by testing the weakness since that could be interpreted as a potential misuse of the system or cause damage to it.

When receiving a report of a suspected or confirmed security incident, the ISS or designee will gather as much of the following information as possible:

Name, affiliation, e-mail address, and phone number of person reporting the incident

Description of the suspected security incident

Information to help identify the source of the suspicious activity, like an IP address or an e-mail message with full headers.

Date(s) and time(s) of the suspicious activity, noting the time zone.

Evidence of suspicious activity (for example, full headers of an e-mail message suspected to be spam originating at CTSFW, appropriate log records, etc.)

In addition to documenting the initial report, the ISS or designee will:

Create an entry in the Seminary security incident tracking system (see “Incident Tracking and Reporting” below)

Initiate appropriate incident handling procedures

As appropriate, communicate with and provide feedback about the results to those reporting the incident once the incident has been handled and closed

Incident Detection

In addition to reports from the Seminary community of suspected or confirmed security incidents, anomalous events may be detected that indicate potential security incidents. Having mechanisms to detect anomalous events early and reliably helps minimize their impact. Detection can be very challenging since there are potentially so many different types of incidents and vectors for attack on a huge number and variety of systems and networks. Thus no one person, unit, or technology can possible monitor it all. Detection is therefore a collaborative effort among Seminary and departmental IT and security personnel.

Channels for detecting possible security incidents include:

E-mail sent to infotech@CTSFW.edu or helpdesk@ctsfw.edu

E-mail sent directly to the ISS

Phone call to the ISS

Automated botnet detection system

Network performance monitoring (e.g., noticing a congested network segment)

Notification from a copyright owner or representative sent to CTSFW's designated copyright agent

Court orders (for example, a subpoena or search warrant). All IT-related court orders should be directed to the CTSFW Legal Counsel.

A customer contacts the IT Help Desk

Monitoring security mailing lists and web sites for threat alerts (for example, the SANS Internet Storm Center — isc.sans.org)

Monitoring external sources of information about new vulnerabilities and exploits and about incidents occurring at other organizations

Employing passive detection techniques such as network flow analysis (top talkers, traffic volume thresholds, communication with known malicious sites, etc.); log file analysis (operating system, system services, databases, applications, network devices, etc.); intrusion detection/prevention systems, and monitoring alerts from security systems (firewalls, anti-virus protection, intrusion detection/prevention systems, wireless network management systems that detect rogue wireless access points, etc.)

Employing active detection techniques such as port scans looking for unusual services, vulnerability scans, manual monitoring of radio frequencies to detect unauthorized wireless access points, and file integrity verification that detects changes to important files

Incident Handling and Response

Security incident response will be typically handled through several stages: analysis, containment, eradication and recovery, and follow-up.

Analysis

Once a potential security incident is reported or anomalous activity detected, analysis must be performed to determine if it is indeed symptomatic of a security incident and to understand the nature of the incident for proper remediation.

Goals

Understand the nature and scope of the incident

Collect enough information about the incident so the response team can prioritize the next steps in handling the incident, which is normally containment

Determine if confidential data is involved in the incident

Components of security incident analysis

Collaboration with other professionals as needed (for example, a security analyst, network analyst, system administrator, and application manager working as a team to analyze the system exhibiting the anomalous behavior; consulting external sources like REN-ISAC, US-CERT, SANS, etc.)

Understanding normal system and network behavior so anomalous activity can be identified

Analysis and correlation of as many indicators as possible, such as monitoring network traffic to/from the host suspected of being compromised, network packet captures for more in-depth analysis, log file analysis, interviews with users and/or system administrators, etc.

Initial determination of the incident's scope (How many systems affected? Is it actively propagating? If so, how?)

Research of the specific malware or type of attack

Collection of additional data which may require permission from the Chief Information Officer (CIO) per CTSFW's IT Acceptable Usage Policy.

Procedures for Analysis

Detect security event

Analyze event data to determine if it is indicative of a security incident and get an initial impression of the nature and scope of the incident

Notify the ISS who may assist with the initial analysis of the event data. Other appropriate personnel may be notified at this point as well, like relevant IT support staff, or a supervisor or department head.

The ISS will record it in the Incident Tracking System

If there's a need to access personal data, like an individual's e-mail or files, in order to gather more information about the incident, first get approval from the CIO per CTSFW's IT Acceptable Usage Policy.

Determine if any confidential data was or might have been affected.

If the incident is of high or medium severity:

Image the hard drive, memory, and any other relevant media before performing analysis that might alter evidence. For hard drives, bit-by-bit copies are required in case deleted files need to be recovered. This is especially important for cases that involve confidential data, possible criminal investigation, or sensitive personnel actions.

Preserve the original media in a secure location and perform analysis on a copy of the data.

Take notes on all actions taken.

Perform additional forensics sufficient to characterize the incident (for example, analyze netflow data).

Containment

Once a security incident is confirmed, the next step is typically containment.

Goals

Stop potential loss of confidential data

Protect other computers and information on the campus network and Internet (for example, keep the malware from spreading to other computers on or off campus)

Prevent further damage to the compromised system and/or information

Identify the location and owner of the computer(s) so they can be engaged in containment, eradication, and recovery

Delaying containment

In some cases, containment may need to be delayed in order to monitor the attacker's activity, usually to collect more evidence. However, the risk of the compromised system being used to attack other systems or breach confidential data could lead to legal liabilities. Consult with the ISS and CTSFW Legal Counsel before deciding to delay containment.

Procedures for Containment

Identify the location and/or owner of the system(s) involved in the incident by checking any of the following:

Network ARP tables to map the IP address to a MAC address

DHCP logs for MAC address and hostname

"nbtscan" command to query host NetBIOS information

Current network access control system for registered student computers

"netsum" info

Network device management software

Log file management software

Determine if the computer needs to have its network access blocked. If so, this can be accomplished in several ways by the CTSFW network team:

At the switch port, router interface, campus border

Block the MAC address on all campus wireless networks (be sure to block it on all wireless networks, not just the residence halls, for example. Also block the wired network interface for the same computer if known).

Disable dial-up modem access

Disable VPN access

If the offending device is an unauthorized wireless access point, its connection to CTSFW's data network must be blocked or removed. This can be done either via the network switch port to which it is connected, or by physically locating the device and unplugging it.

An alternative to blocking all network access, if available, is to put the computer in a network quarantine that redirects its network traffic to a web server with instructions for the owner on how to proceed.

There may be cases when a specific protocol or UDP/TCP port needs to be blocked at the campus border or some other network interface in order to prevent propagation of the malware or to protect the campus from further attacks. Consult the CTSFW network team (infotech@CTSFW.edu) if considering this since they will have to implement it in campus firewalls or router Access Control Lists.

Notify the system administrator and/or user responsible for the system.

Isolate the affected computer(s) either by unplugging the network cable (preferred) or shutting down the computer. Unplugging the network cable and leaving it running is best since shutdown can alter or destroy evidence, like with memory-resident malware. For wireless computers, the wireless interface can be disabled while leaving the computer running.

Perform containment on the affected system(s) to keep it(them) from doing further damage to the computer or the data on it. This step depends on the nature of the compromise/malware, the need for preserving evidence (i.e., if you have to preserve evidence, don’t do anything to the computer until

images of RAM and the hard drive are captured), the urgency of restoring the service hosted on the affected systems, and the time and resources available.

Eradication and Recovery

Goals

Preserve evidence if it has not already been done

Perform additional analysis as needed to complete the investigation

Remove the components of the incident impacting the affected systems, such as deleting the malicious code or disabling a compromised user account.

Mitigate the attack vector so a similar incident does not occur (for example, patch the vulnerability used to compromise the system, apply standard system hardening procedures, adjust firewall rulesets, etc.)

Restore systems to normal operation

Procedures for Eradication and Recovery

Determine the full scope of the incident – how many systems did it affect and therefore need to be repaired?

Determine if any additional analysis is needed:

Determine if any of the affected systems still need to have memory, hard drive(s), or other media imaged to preserve evidence; make an image copy of the media, preserve the original and perform analysis on the copy.

Perform additional analysis, which may include:

Searching for malware by running an anti-virus scan and/or rootkit detection software, or looking for specific files known to be associated with current threats

Recover deleted files and file fragments

Perform a vulnerability scan

Check for unusual running processes and suspicious registry entries, especially ones that run on start-up

Determine open network ports and processes listening to those ports

Take a network packet capture and analyze the network traffic

Analyze network flow data

Analyze log files for unusual activity

Search for confidential data that may have been missed in the initial analysis

If eradication and recovery keeps the system or service out of operation beyond the length of time that can be tolerated by the institution, invoke business recovery and continuity procedures to restore the service until normal operations can be resumed.

Determine if a reformat/reinstall is required. **Compromises that allow remote control of the system, gain root/Administrator privileges, and/or install a backdoor require a complete, clean re-install of the system for eradication.**

The ISS in conjunction with SIRT will determine when a specific type of compromise requires reformat/reinstall

Reformatting the hard drive and re-installing from a backup tape prior to the compromise is acceptable, as is restoring from a clean image for those systems that use disk imaging technology like Symantec Ghost.

Note that reinstalling must occur without exposing the vulnerable system to the campus network and the Internet

If infected with malware and a reformat/reinstall is not required, remove the malware from the system. Running an anti-virus scan after updating virus definition/pattern file may suffice. Specific instructions for removing certain types of malware may also be found by searching the Internet.

If the incident involves an unauthorized wireless access point, locate the device and contact the person responsible for it to ensure that it ceases operation.

Mitigate the attack vector to prevent further instances. This may include:

Patching vulnerabilities in the operating system and all applications software

Changing passwords

Placing the system behind a firewall

Adjusting firewall rules

Updating or installing new security software (for example, anti-virus software or a host-based personal firewall)

Applying standard system security hardening techniques

Passing a security assessment

User training

Restore network access if the system was blocked during the containment phase.

Return the system to normal operations

Follow-up

Goals

Determine lessons learned and make recommendations to prevent subsequent similar incidents

Issue final reports

Archive evidence and documentation

Close out the incident

Procedures

The Incident Manager should confirm that all action items, investigations, analyses, and communications are completed

Hold a Post-Incident Review session, if required, to determine ways to improve CTSFW's management of security incidents and help prevent future incidents, not to assign blame.

It should be scheduled to occur within 2-3 weeks of the incident's remediation

Include the incident response team and relevant stakeholders

Appoint one person to record notes – successes, failures, recommendations, and action items

Cover the following areas in the review session:

Are there any open issues? In other words, is remediation of the incident complete?

What could have prevented the incident?

How effectively was the incident handled (response time, communication, following procedures, containing spread/damage, etc.)?

Recommend changes to policy, procedure, and security controls to prevent and more effectively handle future incidents.

Identify any needed follow-up tasks and assign those tasks to individuals

Evidence management — does any evidence need to be preserved longer? If so, for how long and by whom? Release or properly destroy any evidence that is no longer needed.

Complete a Post-Incident Report if required and submit it to the Chief Information Officer. Security incidents with a severity category of "high" must complete a post-incident report. The CIO may request a post-incident report for any security incident.

The CIO will review any recommendations and consider assigning resources to implement them.

Archive reports and other relevant documents and communications ("work product") according to CTSFW's Document Retention policy and procedures. This includes log files, timelines, recovered files, notes, network flow data, e-mails, etc.

Close out incident tickets in the incident tracking system

Collection and Preservation of Evidence

When a security incident involves legal action against a person or organization, or a personnel action against a CTSFW employee, evidence must be collected, preserved, and presented to conform to the rules for evidence specified in the relevant jurisdiction(s). The following procedures help ensure the strong evidence trail needed for admissibility (making sure it can be used in court) and weight of evidence (high quality and completeness).

When collecting evidence, follow all appropriate CTSFW policies and procedures, such as getting permission from the Chief Information Officer to access data in situations outlined in confidentiality and privacy sections of CTSFW IT Policies.

Document all actions taken in the collection and preservation of the evidence.

For data stored on electronic media, such as a hard disk drive, USB flash drive, CD, DVD, or RAM, make a mirror image or copy (depending on applicable requirements) of the media. For example, if forensics will require recovering deleted files or file fragments from a hard drive, a bit-by-bit mirror image of the drive is required since a file-by-file copy will not capture that data.

Have another person witness the imaging/copying process. If the incident involves a high profile or sensitive criminal case, have a law enforcement officer assist with the collection of the evidence, witness the imaging/copying process, and store the originals.

Log all actions taken during the imaging/copying process, including date, time, and location the image/copy was made, who performed the actions and who witnessed it, and the tools and programs used.

Label the original media and store it along with the log of the imaging/copying process in a secure location.

Perform all forensics work on the image or copy, not the original. Additional images or copies of the original can be made if needed (for example, if forensics analysis on the copy destroyed some evidence and you need to continue analysis on a fresh copy).

For paper-based documents, keep the original in a secure location and log the following:

- who found the document
- where it was found

- date and time it was found
- who witnessed the discovery

Incidents Involving Confidential Personally Identifiable Information
Incidents suspected of or known to involve confidential Personally Identifiable Information, such as names with social security numbers or credit card numbers, have special legal, policy, and notification requirements in addition to the normal incident handling procedures outlined in this document.

State of Indiana Law
The primary law framing response requirements for incidents involving Personally Identifiable Information is Indiana Code Article 24-4.9, Indiana's *Security Breach Notification Statute*, that became effective in July 1, 2006.

It provides Indiana residents with the right to know when a security breach has resulted in the exposure of their personal information.

A security breach is defined as an unauthorized acquisition of computerized data which compromises the security, confidentiality or integrity of personal information. Breaches that involve paper documents that were once maintained as computerized data are also covered by this law.

It defines "personal information" as: "a social security number or an individual's name in combination with any one or more of the following data elements: driver's license number, account number, a state identification card number, a credit card number, a financial account number, or a debit card number in combination with any required security code."

The Statute requires that a business notify:

Affected consumers following discovery of the breach. The disclosure must be made without unreasonable delay and must be provided to the affected persons by one of the following methods:

- mailed written notice
- telephone notification
- Facsimile (fax)
- electronic mail notice, if an email address is available

Consumer reporting agencies if more than 1,000 Indiana residents are to be notified. The contact information for the three nationwide consumer reporting agencies is as follows:

EQUIFAX
Equifax:
Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374

800-525-6285
security.dataadministration@equifax.com

EXPERIAN
Consumer Fraud Assistance
P.O. Box 9556
Allen, TX 75013
888-397-3742
businessrecordsvictimassistance@experian.com

TRANSUNION
Consumer Relations & Fraud Victim Assistance
1561 E. Orangethorpe Ave.
Fullerton, CA 92831
Tel: 800-372-8391 fax: 714-680-7290
FVAD@Transunion.com

The Attorney General's office. Failure to do so may result in penalties under the breach notification statute. Use our security breach reporting form. You can submit your breach notification to the Indiana Attorney General's Office by completing the printable Breach Notification Form and mailing or faxing the form to:
Identity Theft Unit—Data Breach
Attorney General of Indiana
Indiana Government Center South, 5th Floor
302 West Washington Street
Indianapolis, IN 46204
317-232-6201

Online Breach Notification Form can be found at:
http://www.in.gov/attorneygeneral/files/841375_1(1).PDF

Printable Breach Notification Form can be found at:
http://www.in.gov/attorneygeneral/files/Form_1079_Security_Breach_Reporting_Form_-_Print_Version.pdf

Exceptions:
The law also provides for substitute notice to consumers if the business demonstrates to the Attorney General that the cost of providing regular notice to Indiana residents would exceed $250,000 or that the affected class of Indiana residents exceeds 500,000. Where substitute notice is used, it must consist of all of the following, as applicable: conspicuous posting on the entity's web site, and notification to geographically relevant statewide media.

Executive Incident Management Team

Incident response in these cases will be overseen by an Executive Incident Management Team (EIMT) as mandated by CTSFW's Security Incident Reporting and Response Policy. An EIMT may also oversee the response to other high-severity incidents, but the primary purpose is to deal with incidents involving Personally Identifiable Information.

The purpose of the EIMT is to provide executive guidance to the response process to insure: a) an appropriate, timely, and legal response, b) to make decisions related to the incident, and c) to notify appropriate parties.

The team consists of:

Senior administrator (VP) for the affected department

Chief Information Officer (CIO)

Information Security Specialist (ISS)

Representative from CTSFW Legal Counsel

Director of Seminary Relations

Others as needed (for example, Police for criminal incidents, or the data steward of the affected data)

The CIO will convene the EIMT at the appropriate time per the procedure that follows.

Credit Card Information

If the PII threatened in the incident includes credit card information, all normal procedures for handling a suspected breach of confidential data must be followed, in addition to:

Include the CFO or a representative on the Executive Incident Management Team (EIMT)

Promptly notify the affected payment brands (VISA, MasterCard, Discover, etc.), as required by the Payment Card Industry Data Security Standards, security control 12.9.1

The EIMT should consider notifying the acquiring bank that processes financial transactions for CTSFW

Procedure for handling a breach of confidential personal identity data

If the ISS determines that confidential data has been or may have been breached, the ISS will immediately notify the CIO.

The ISS will oversee additional forensics analysis to gather as much information as possible about what happened, being sure to properly protect evidence.

If after analysis the CIO and ISS have definitive evidence that the confidential data was not breached, then no further special action is required and normal incident response procedures may continue.

However, the security of this system and the need to store confidential data on it should be carefully assessed.

If there is a possibility that confidential data involving Personally Identifiable Information was breached, the CIO will convene the EIMT as quickly as possible to review the evidence and determine if a breach of confidential personal identity data occurred or is “reasonably likely” to have occurred (wording of the state notification law).

If the EIMT determines that personal identities are not at risk, no further special action is required and normal incident management procedures may continue.

If the EIMT determines that personal identities are at risk, the EIMT oversees the response, addressing the following issues:

Determine if the affected individuals need to be notified and the appropriate method for notification (Senate Bill 196 has stipulations)

Determine who will draft and sign the notification

Assign someone to collect victim mailing addresses and to distribute notifications

Determine the point of contact for inquiries from the victims, media, and other interested parties and the type of assistance to offer. In determining the type of assistance appropriate to the situation, consider assistance such as:

Providing personal assistance in getting free credit protection,

Establishing a toll-free phone number for victims to call for assistance, and/or

Establishing an informational website.

Determine the need for a news release and timing in relation to the communication with victims. The news release will be drafted by the Director of Seminary Relations or designee and reviewed by the EIMT.

Determine if all national consumer credit agencies need to be notified (required by Indiana law if notifying more than 1,000 consumers) and if so, who will notify them and what information will be provided

Discuss how the incident could have been prevented and steps to take to prevent similar incidents in the future

If potential victims do need to be notified, the CIO or designee(s) should notify the following people as quickly as possible:

Office of the President

Board of Regents

The ISS will convene a Post-Incident Review Session with key stakeholders from the EIMT and others as needed

The ISS will draft a confidential Post-Incident Report (see "Post Incident Report" below) to be reviewed by appropriate members of EIMT for accuracy and submitted to the CIO and VP(s) in the affected department(s).

Deciding Whether or Not to Notify Victims

If confidential data resides on a compromised computer, it is not always obvious whether the data were accessed and therefore whether potential victims need to be notified. EDUCAUSE provides the following questions to consider when deciding whether confidential data was breached (from the University of California Office of the President):

Is the information in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing unencrypted notice-triggering information?

Is there evidence that information has been downloaded, copied, or otherwise accessed, for example: an ftp log that contains the name of a file containing notice triggering information?

Was a privileged (e.g. root or administrator) or non-privileged account, one with access to privileged information, compromised?

Was one system or multiple systems compromised?

Is the identity of the attacker known or unknown? If known was the attacker a disgruntled insider or an unaffiliated third party? Were multiple attackers involved?

Are there indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported?

Did the unauthorized person have access to the information for an extended period of time?

What was the time between compromise start and compromise discovery?

Did the compromise indicate a directed attack, such as a pattern showing the machine itself was targeted versus an automated attack?

Did the attack appear to seek and collect the information?

Did the attack appear to include tampering with records (e.g., changing grades)?

Did the attacker attempt to cover up their activity?

Did the attacker release information about the nature or scope of the attack?

Was the information encrypted and would the encryption method effectively prevent the information from being accessed.

What is the potential damage to individuals if notification is not given?

What is the potential damage to institutional credibility in the case of notification?

What is the potential damage to institutional credibility in the case of failure to notify?

Incident Tracking and Reports

Incident Tracking System

The ISS will maintain an incident tracking system and record the following information about all reported security incidents:

Incident ID number assigned by the ISS in the form YYYY-XXX where "YYYY" is the year in which the incident occurred and "XXX" is a unique number that roughly corresponds to the sequential order of occurrence of the incident that year. For example, 2016-13 would be the 13th incident that occurred in 2016.

Incident category(ies), severity, and description

Identity of the affected system(s) – IP address, domain name, MAC address

Whether the system contains confidential data

Location of the affected system(s) – building and department

Contact information – usually the departmental security contact, appropriate system administrator, or VP

Dates and times – first notice, when contact notified, blocking/unblocking

Recovery action taken

All IT security incidents or suspected incidents (i.e., reports of suspicious activity that upon investigation are determined not to be a security incident) will be recorded in the incident tracking system.

The incident tracking system should be used to identify trends or outbreaks that may require changes to security controls and/or policies to reduce the risk of future occurrences.

The incident tracking data is considered confidential and should therefore be encrypted when stored or transmitted and disclosed only to authorized individuals. The confidentiality of reports derived from the incident tracking data will be determined on a case-by-case basis by the ISS and/or the CIO.

Annual Report

In January each year, the ISS will summarize the incidents for the previous calendar year and provide a

report to the CIO. The security incident data may also be used for other reports as needed. This report will be marked as confidential.

Post-Incident Report

Individual security incidents may require completion of a Post-Incident Report. Incidents with a severity category of "high" must submit one, and the CIO may request one for any security incident. Normally, the incident manager will complete the post-incident report.

The CIO will review any recommendations in the report and determine additional follow up actions.

Post-incident reports must be submitted to the CIO, be marked as confidential, and use IT Security Post Incident Report.DOCX document on the IT Staff Share Drive.

Guidance

Guidance	Section
ISO27001:2013	A.16.1
NIST SP 800-53 v4	AU-6, IR-1, IR-6, CA-2, CA-7, PL-4, SA-5, SA-11, SI-2, SI-5, IR-4, IR-10, AU-7, AU-8, AU-9, AU-11

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Change	Version	Author	Date of Change
1.0	Initial Draft	Richard Woodard	9/25/2016
1.1	Provisionally accepted - Accepted	Richard Woodard	9/29/2016 – 10/20/2016
1.2	Updated Non-Compliance to match standard adopted October, 2016	Richard Woodard	12/7/2016
1.2.1	Updated Storage Location	Richard Woodard	12/1/2019

Concordia Theological Seminary
Fort Wayne, Indiana

Information Security Incident Reporting and Response Policy

Policy Owner	Information Technology
Policy Approver(s)	IT Policies and Procedures Committee
Related Policies	Information Security Incident Management Policy, IT Application Security Policy(In Process), Password Policy, IT Firewall Policy, IT Anti-Virus Policy, IT Network Security Policy, Data Privacy Policy, Hardware Sanitization Policy, Data Protection Policy, Removable Media Acceptable Use Policy, Systems Monitoring and Auditing Policy, Security Awareness Training Policy
Related Procedures	See procedures for policies listed above
Storage Location	The latest version will be kept as a digital copy in the Information Technology section of the Seminary community website (myctsfw.force.com/cc/s/information-technology). A paper copy will be kept at the IT Helpdesk in B-18.
Effective Date	October 15, 2016
Next Review Date	August 2020

Purpose

The purpose of this policy is to ensure proper recognition, management, and communication of security events and weaknesses through a formal process. It governs the actions required for reporting or responding to security incidents involving CTSFW information and/or information technology resources to ensure effective and consistent reporting and handling of such events.

Scope

This Information Security Incident Management Policy applies to all personnel, business processes and data, information systems and components using CTSFW information technology resources or data, and to physical areas of CTSFW.

Definitions

Personnel – All faculty, staff, students, volunteers, contractor and sub-contractors of CTSFW.

Security Incident – Any real or suspected event that may adversely affect the security of CTSFW information or the systems that process, store, or transmit that information. Examples include:

- Unauthorized access to data, especially confidential data like a person's name and social security number
- Computer infected with malware such as a worm, virus, Trojan Horse, or botnet
- Reconnaissance activities such as scanning the network for security vulnerabilities
- Denial of Service attack
- Web site defacement
- Violation of a CTSFW security policy
- Security weakness such as an un-patched vulnerability

Personally identifiable information (PII) – The US government officially defines PII as "Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." Divulgence of student and family PII is subject to FERPA governance found online at http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferparegs.pdf . PII includes, but is not limited to:an individual's name; date of birth; address; telephone number; driver's license number or card or non-driver's identification number or card; social security number or card; place of employment; employee identification numbers or other personal identification numbers or cards; mother's maiden name; birth, death or marriage certificates; electronic identification numbers; electronic signatures; and any financial number, or password that can be used to access a person's financial resources, including, but not limited to, checking or savings accounts, credit or debit card information, demand deposit or medical information, or ones name in combination with a passport number.

Incident Manager – The person responsible for managing the response to a security incident as defined in the incident response summary table below.

Executive Incident Management Team - oversees the handling of security incidents involving confidential data (e.g., personally identifiable information). This team has authority to make decisions related to the incident and to notify appropriate parties. The team consists of:

VP in charge of the affected department

Chief Information Officer

Information Security Specialist

CTSFW Legal Counsel

Director of Seminary Relations

Others as needed (i.e. Law Enforcement)

Policy

All members of the Seminary community are responsible for reporting known or suspected information or information technology security incidents. All security incidents at CTSFW must be promptly reported to CTSFW's Information Technology Department and other appropriate authority(ies) as outlined below.

Incident response will be handled appropriately based on the type and severity of the incident in accordance with the Incident Response Summary Table below. Handling of security incidents involving confidential data will be overseen by an Executive Incident Management Team.

All individuals involved in investigating a security incident should maintain confidentiality, unless the Chief Information Officer authorizes information disclosure in advance.

Procedures

Security incidents are to be reported to the appropriate person(s) as outlined in the "Who to Notify" section of the Incident Response Summary table below. Once reported, the Incident Management Team will respond based on the Incident Severity and Response Time, using the Information Security Incident Management Policy processes to **analyze** the incident, **contain** the breach, **eradicate** the vulnerability, **recover** data and follow-up with **Post-Incident Activity and reporting**.

1. **Reporting Security incidents**
   Any member of the CTSFW community who suspects the occurrence of a security incident must report incidents through the following channels:
   a. All suspected high severity events as defined in Procedure 2.a below, including those involving possible breaches of personally identifiable information, must be reported directly to the Information Security Specialist (ISS) as quickly as possible by phone, e-mail, or in person. If the ISS cannot be reached, contact the Chief Information Officer (CIO).
   b. All other suspected incidents must also be reported to the ISS. These incidents may be first reported to Information Technology Help Desk, or the Department head or VP who can then contact the ISS. Reports should be made by sending email to infotech@ctsfw.edu or by notifying the ISS by phone, email, or in person.
   c. For detailed information about reporting IT security incidents, see the CTSFW Information Security Incident Management Procedures.
2. **Responding to Security Incidents**
   a. **Incident Severity**
   Incident response will be managed based on the level of severity of the incident. The level of severity is a measure of its impact on or threat to the operation or integrity of the institution and its information. It determines the priority for handling the incident, who manages the incident, and the timing and extent of the response. Three levels of incident severity are used to guide incident response: high, medium, and low.

i. High
The severity of a security incident will be considered "high " if any of the following conditions exist:
1. Threatens to have a significant adverse impact on a large number of systems and/or people (for example, the entire institution is affected)
2. Poses a potential large financial risk or legal liability to the Seminary
3. Threatens confidential data (for example, the compromise of a server that contains names with social security numbers or credit card information)
4. Adversely impacts an enterprise system or service critical to the operation of a major portion of the Seminary (for example, e-mail, SIS, RE, Moodle, Internet service, Phone systems or a major portion of the campus network)
5. Poses a significant and immediate threat to human safety, such as a death-threat to an individual or group
6. Has a high probability of propagating to many other systems on campus and/or off campus and causing significant damage or disruption

ii. Medium
The severity of a security incident will be considered "medium" if any of the following conditions exist:
1. Adversely impacts a moderate number of systems and/or people, such as an individual department or building
2. Adversely impacts a non-critical enterprise system or service
3. Adversely impacts a departmental system or service, such as a departmental file server
4. Disrupts a building or departmental network
5. Has a moderate probability of propagating to other systems on campus and/or off campus and causing moderate damage or disruption

iii. Low
Low severity incidents have the following characteristics:
1. Adversely impacts a very small number of systems or individuals
2. Disrupts a very small number of network devices or segments
3. Has little or no risk of propagation or causes only minimal disruption or damage in their attempt to propagate

b. **Incident Response Summary Table**
The following table summarizes the handling of IT security incidents based on incident severity, including response time, the responsible incident managers, and notification and reporting requirements. Detailed procedures for incident response and management are further defined in the CTSFW Information Security Incident Management Procedures.

INCIDENT RESPONSE SUMMARY					
INCIDENT See Incident Categorization Summary above		**RESPONSE**			
Potential Impact	**Characteristics** Any condition met qualifies	**Response Time**	**Incident Manager**	**Who to Notify**	**Post-Incident Report Required**
High	• Significant adverse impact on a large number of systems and/or people • Potential large financial risk or legal liability to the University • Threatens confidential data • Adversely impacts a critical enterprise system or service • Significant and immediate threat to human safety • High probability of propagating to a large number of other systems on or off campus and causing significant disruption	Immediate	Chief Information Officer , Information Security Specialist or Incident Management Team	• Chief Information Officer • Information Security Specialist • Unit VP • Department head • Tech Support for affected system	Yes

Medium	• Adversely impacts a moderate number of systems and/or people • Adversely impacts a non-critical enterprise system or service • Adversely impacts a departmental scale system or service • Disrupts a building or departmental network • Moderate risk of propagating and causing further disruption	4 Hours	Appointed by unit VP	• Information Security Specialist • Unit VP • Department Head • Tech Support for affected system	No, unless requested by CIO, ISS or other appropriate administrator
Low	• Adversely impacts a very small number of non-critical individual systems, services, or people • Disrupts a very small number of network devices or segments • Little risk of propagation and further disruption	Next Day	Technical Support for affected system	• Information Security Specialist • Department Head • Tech Support for affected system	No

Guidance

Guidance	Section
ISO27001:2013	A.16.1
NIST SP 800-53 v4	AU-6, IR-1, IR-6, CA-2, CA-7, PL-4, SA-5, SA-11, SI-2, SI-5, IR-4, IR-10, AU-7, AU-8, AU-9, AU-11, 800-88
FERPA 34 CFR	99

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook. If

the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.

- Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the CTSFW Personnel Handbook.
- In the case of a student, the breach will also be remanded to the Dean of Students.

Revision History

Change	Version	Author	Date of Change
1.0	Initial Draft	Richard Woodard	9/25/2016
1.1	Provisionally Accepted	Richard Woodard	9/25/2016
1.4	Updated Non-Compliance to match standard adopted October, 2016	Richard Woodard	12/7/2016
1.4.1	Updated Storage Location	Richard Woodard	12/1/2019