Written Information Security Program

Version: 2.0
Issued: 11/28/2016

OBJECTIVE

Salem State University's (SSU) objective in the development and implementation of this comprehensive Written Information Security Program (WISP) is to create effective administrative, technical and physical safeguards for the protection of Confidential Information with which SSU conducts business transactions and with which SSU conducts business on behalf of its customers as a service provider. SSU will comply with any and all obligations to safeguard Confidential Information to prevent data breaches. The WISP sets forth SSU's procedures for evaluating its electronic and physical methods of accessing, collecting, storing, using, transmitting and protecting Confidential Information.

SSU will:

1) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Confidential Information;
2) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Confidential Information;
3) Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
4) Design and implement a WISP that puts safeguards in place to minimize those risks, consistent with Confidentiality Obligations which require SSU to safeguard Confidential Information to prevent data breaches; and
5) Regularly monitor the effectiveness of those safeguards.

PURPOSE

The purpose of the WISP is to:

a) Ensure the security and confidentiality of Confidential Information;
b) Protect against any anticipated threats or hazards to the security or integrity of such information;
c) Protect against any unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.
d) Ensure compliance with any and all "Confidentiality Obligations" which are defined as:
    - Any state or federal laws in effect or hereinafter enacted
    - Applicable industry standards such as the Payment Card Industry Data Security Standard (PCI DSS)
    - Client contractual obligations
    - Vendor contractual obligations
    - Partner contractual obligations
    - SSU defined Confidential Information

SCOPE

This WISP and associated policies, standards, guidelines, and procedures apply to all employees, vendors, part-time and temporary workers, service providers, and those employed by others to perform work on SSU premises, at hosted or outsourced sites, or who have been granted access to SSU information or systems. It also encompasses all systems/applications used by the afore-mentioned employees, vendors, and service providers.

The WISP is designed to encompass various aspects of the security of Confidential Information in electronic or written format, and in data transmission. For the purposes of this WISP, "Confidential Information" means any personal and business information that SSU must keep confidential.

Personal information means the first name and last name or first initial and last name of an individual with which SSU conducts business in combination with any one or more of the following data elements that relate to such an individual:

a) Social Security Number (US)
b) Driver's License, State or Federal Issued Identification Card Number or Passport; or
c) Financial Account Number, or Credit or Debit Card Number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; provided, however, that "Confidential Information" shall not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.
d) Medical Records Health Insurance Information and other Personal Health Information

Business information means information related to the business of SSU that is classified as confidential and information from SSU clients that is contractually agreed to as confidential including but not limited to:

a) Legal Documents
b) Intellectual Property
c) Client Information
d) Vendor Information
e) Partner Information

INFORMATION SECURITY OFFICER

The Information Security Officer will be responsible for:

a) Initial Implementation of the WISP;
b) Regular testing of the WISP's safeguards;
c) Evaluating the ability of each of SSU's third party service providers to implement and maintain appropriate security measures for Confidential Information to which we have permitted them access, consistent with Confidentiality Obligations which require SSU to safeguard Confidential Information to prevent data breaches; and requiring such third party service providers by contract to implement and maintain appropriate security measures and notify SSU of any security incident involving Confidential Information of which it becomes aware.
d) Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing the Confidential Information. The Information Security Officer shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review.
e) Ensuring new hire and an annual training session for those handling sensitive date be conducted via electronic means or in person for all owners, managers, employees and independent contractors, including temporary and contract employees who have access to Confidential Information on the elements of the WISP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with SSU's requirements for ensuring the protection of Confidential Information.
f) Executing the Incident Response Policy and corresponding procedures as required for Information Security incidents.

INTERNAL RISKS

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Confidential Information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately.

Protecting Against Internal Threats

1. Confidential Information Collection & Use, Access, Transmission, Storage & Disposal

SSU uses Confidential Information in personnel files, payment card transactions, benefits records, legal documents and other areas that process, transmit and/or store the information in electronic and/or hardcopy records. It is vital that the collection, use, transmission, storage and disposal of this Confidential Information is appropriately safeguarded and restricted so as to avoid any data breach.

a. Collection & Access to Confidential Information

The amount of Confidential Information collected by SSU should be limited to that amount reasonably necessary to accomplish SSU's legitimate business purposes, or necessary for SSU to comply with Confidentiality Obligations.

Access to any electronic records or to any hardcopy records containing Confidential Information shall be limited to those persons who are reasonably required to know such information in order to accomplish SSU's legitimate business purpose or to enable SSU to comply with other state, provincial or federal regulations.

Access to Confidential Information collected, used, transmitted or stored by SSU shall be limited to active employees requiring such Confidential Information for the purpose of accomplishing a legitimate SSU business purpose.

Terminated employees must return all records containing Confidential Information in any form that may at the time of such termination be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.). A terminated employee's physical and electronic access to Confidential Information must be immediately blocked. Such terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to SSU's premises or information. Moreover, such terminated employee's remote electronic access to Confidential Information must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated.

b. Electronic Access and Transmission

Electronic access includes accessing Confidential Information through use of computers and laptops generally by way of email or file sharing and electronic document storage and possession. Lastly, it also includes access via mobile devices such as smartphones, tablets, thumb drives and similar storage devices.

Electronic access to Confidential Information shall be restricted to active users and active user accounts only. Electronic access to user identification after multiple unsuccessful attempts to gain access must be blocked. Current employees' user ID's and passwords must be changed periodically as outlined by IT system requirements and must never consist of vendor supplied, default passwords. Access to electronically stored Confidential Information shall be electronically limited to those employees having a unique log-in ID; and re-log-in shall be required when a computer has been inactive for a period of time as defined by IT system configuration requirements.

Electronic communication of any nature must not include Personally Identifiable Information unless the information is:

(a) Encrypted when transmitted over an open public network, for example the Internet
(b) Transmitted over SSU's secure VPN for remote access
(c) Faxed over a private direct fax line and the faxed documents are safeguarded and treated as hardcopy Confidential Information by the receiver

Alternatively, Confidential Information may be emailed externally if it is encrypted using SSU provided encryption tools. If there is no capability to send Confidential Information as encrypted data, a secure alternate means of delivery must be used. To the extent reasonable, any Confidential Information

emailed, should not be printed. If it is printed, this data should be safeguarded as hardcopy Confidential Information.

c. Hard Copy Access and Transmission and Transport

To the extent employees must access Confidential Information to accomplish a legitimate business purpose; such access must be limited to necessary SSU personnel only. Each department accessing such Confidential Information must develop internal controls to ensure that requests for disclosure of Confidential Information are legitimate. For example, in lieu of providing an employee's social security number, an employee's unique SSU employee number should be substituted.

Employees are prohibited from keeping open files containing Confidential Information on their desks when they are not at their desks during the day. All Confidential Information in hardcopy form or on removable electronic media must be secured in a locked office, cabinet or storage facility during non-business hours.

To the extent any electronic or hardcopy records must be shared with any internal or external party, and such information includes in part, Confidential Information that the internal or external party does not have authorization to access, such Confidential Information must be redacted prior to sharing.

For example, if Human Resources must provide a copy of an employee's records to a department manager, all Confidential Information within the file must be redacted whether the records are in hardcopy or electronic form.

d. Storage of Confidential Information

Each department shall develop rules (in consideration of the business needs of that department) that ensure that reasonable restrictions upon access to electronic or hardcopy records containing Confidential Information are in place, including a written procedure that sets forth the manner in which access to such records is to be restricted; and each department must store such records and data in locked facilities, secure storage areas or locked containers. In any event, no Confidential Information should ever be kept in any unlocked or unsecure storage facility, including unlocked cabinets or unlocked offices. Confidential information should also never be left at unsecure copy machines or fax machine locations where unauthorized individuals could gain access.

In no event should Confidential Information be stored on any SSU mobile device or laptop computer's encrypted local drive.

Hardcopy or electronic media with Confidential Information should never be taken out of its secure storage to an off-site location unless there is a legitimate SSU business purpose and the data is appropriately safeguarded at all times. For example, it is not acceptable to leave Confidential Information about employees in files in an employee's unsecure, unoccupied car, or store Confidential Information at an employee's residence. Should the need to arise to remove electronic Confidential Information from its secure location an encrypted laptop or appropriate media must be used.

e. Disposal of Confidential Information

Any hardcopy Confidential Information should be destroyed when there is no longer a legitimate SSU business purpose to the storage of such documents by use of an office-grade cross-cut shredder or by disposal of such documents in marked contracted document shredding receptacles in the office as provided by a contracted document shredding service provider. No Confidential Information should ever be disposed of in normal trash or in recycling bins or any other public means of disposal.

Paper or electronic records (including records stored on hard drives or other electronic media) containing Confidential Information shall be disposed of only in a manner that complies with all Confidentiality Obligations. IT will manage the disposal of Confidential Information in electronic format including on network equipment, servers, workstations, laptops, mobile devices owned by SSU. IT will consult with business units regarding the disposal on Confidential Information in hardcopy format to determine the most appropriate and secure manner of disposal to meet all Confidentiality Obligations.

EXTERNAL RISKS

In addition to monitoring its internal risks, it is necessary for SSU to ensure it is protected from outside threats to access Confidential Information in its possession.

1. Electronic Safeguards

SSU employees that must transmit Confidential Information via laptops and desktop computers should never transmit such data on non-company computers as such devices increase the risk of an external threat to data security. Further, any such Confidential Information transmission cannot occur using electronic messaging such as email or instant messaging, through any social media sites, or through any other Internet channel that is not specifically approved by IT as an encrypted means to transmit Confidential Information.

When Confidential Information remote access transmissions are necessary to complete a legitimate business purpose, they should be conducted only using official SSU provided private network, VPN connections or encrypted internet protocols.

SSU maintains up-to-date firewall protection and operating system security patches, designed to maintain the integrity of the Confidential Information, installed on all systems processing Confidential Information. SSU maintains up-to-date versions of system security agent software which includes malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing Confidential Information. All employees with company-issued laptops or using desktops must ensure that they do not disable the automatic updating functions on such devices. All computer systems are to be monitored for unauthorized use.

SSU also requires each employee who uses university owned desktop, laptop, or mobile device to set up a unique password for entry into the business systems (if applicable) and onto the computer system itself (i.e. Windows password). These passwords must not be shared with anyone. In addition, SSU's system periodically notifies users that they must modify their passwords. All employees must abide by these requirements and ensure they appropriately update their passwords as required.

COMPLIANCE AND ENFORCEMENT

1. Distribution of the Written Information Security Program

A copy of the WISP must be distributed to each existing employee and all new hires who have any exposure to Confidential Information. Access to the WISP will be made easily available to all employees required to comply with the WISP. Each hiring manager must evaluate whether their direct reports have exposure to Confidential Information, and if so, ensure that they receive a copy of the WISP in electronic or hardcopy format, and certify their compliance with the WISP.

2. Training Regarding the Written Information Security Program

As noted above, each employee required to comply with the WISP because they handle Confidential data must complete mandatory training which will be distributed either in person or via electronic means to certify their compliance with the WISP. Each employee required to comply with the WISP will also undergo an annual retraining on the WISP.

3. Discipline for Violations of the Written Information Security Program

Any violation of the WISP shall result in immediate disciplinary action, up to and including termination. Employees are required to report any suspicious or unauthorized use of customer information to the parties noted below. Any manager receiving information regarding a potential violation of the WISP must take the following steps within twenty-four (24) hours:

i. Report the violation to the University Counsel;
ii. Consult with Human Resources as to what disciplinary action shall be taken against any employees violating the WISP; and
iii. In line with SSU's policy on disciplinary actions, ensure that the disciplinary action is appropriately documented in writing in the employee's personnel file.

Whenever there is an incident that requires notification under any Confidentiality Obligations, there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in SSU's security practices are required to improve the security of Confidential Information for which SSU is responsible.

All management and supervisory employees shall be responsible for the enforcement of, and compliance with, the WISP including necessary distribution to ensure employee knowledge, acceptance and compliance. All employees are under an obligation to comply with SSU policies, including all Information Security policies and procedures, and to follow any of SSU's additional reasonable and authorized instructions. Serious violations of the Written Security Information Program must be reported to each of the following persons:

Information Security Officer	Thomas Cesso, CISO	Phone: 978-542-2745 Email:tcesso@salemstate.edu
General Counsel	John Keenan, General Counsel & VP of Administration	Phone:978-542-6400 Email:jkeenan@salemstate.edu
AVP-Human Resources	Mark Quigley	Phone: 978-542-6078 Email: mquigley@salemstate.edu

Reporting of any lost or stolen SSU equipment or other documents containing Confidential Information must be immediately reported to the Information Security Office.

COMPLIANCE WITH LAWS

It is the policy of SSU to comply fully with all laws and regulations that govern its operations nationally, as well as in the various states, provinces and countries in which it conducts its businesses. Employees must conduct themselves accordingly.

COMPLIANCE AND DISCLOSURE

All employees are under a duty to comply with this Policy upon receipt, regardless of whether they sign any acknowledgement or participate in any training. Employees who fail to disclose reportable interests or relationships, who knowingly make a false report, or who fail to comply with SSU's policies shall be subject to disciplinary action up to and including dismissal.

REVISION HISTORY

This section contains comments on any revisions that were made to this document and the date they were made.

Version Number	Issued Date	Approval	Description of Changes
1.0	3/15/2016	Compass IT Compliance	Initial Draft
2.0	11/28/2016	John Keenan, General Counsel/VP for Administration Mark Quigley, AVP, Human Resources Thomas Cesso, CISO	First Issue