College of Southern Nevada

Information Security Program

January 2018

CSN
COLLEGE OF
SOUTHERN NEVADA

Contents

Introduction

The College of Southern Nevada (CSN) is responsible for taking all reasonable and appropriate steps for the protection of the confidentiality, integrity, availability, and privacy of information in its custody, whether in electronic or physical form. The preservation and integrity of the information are key to ensure the availability and security of the data. This includes physical security as well as business continuity and disaster recovery plans. CSN recognizes that confidentiality and privacy, integrity, and availability of information are components of a comprehensive information security program. This document identifies the program objectives, roles and responsibilities, and oversight of the CSN Information Security Program.

The Information Security Program in conjunction with provisions of the Nevada System of Higher Education Board of Regents Handbook and institutional policies and procedures, provide a general framework for information security. The purpose of the Information Security Program is to establish a college-wide approach to the protection of the confidentiality, integrity, availability, and privacy of information in its custody, regardless of format.

This living document will evolve over time to ensure that we strive to provide the highest of protection.

Plan Objectives

- Provide administrative, physical, and technical safeguards to ensure compliance with applicable federal and state laws, regulations, and policies.
- Conform to the standards set forth by the Nevada System of Higher Education (NSHE).
- Safeguard against anticipated threats to the security or integrity of protected information.
- Prevent and protect against the unauthorized access to, and unlawful processing or disclosure of, protected information.

Information Security Program Coordination

CSN shall establish a coordinated approach to the protection of information resources and depositories of protected information that are under its custody by establishing appropriate and reasonable administrative, technical and physical safeguards that include all individuals, units, or others that administer, install, maintain, or make use of CSN’s computing resources and other depositories of information. The CSN Information Security Officer (ISSO) will be responsible for the development, maintenance, and yearly review of the Program, in collaboration with the following councils, and committees:

- NSHE Information Security Officers Council
- All departmental record management custodians

Roles and Responsibilities

Information Systems Security Officer

The Information Security Officer (ISSO) provides management and oversight to the day-to-day implementation of information security policies and strategies. The ISSO works closely with the Chief Information Officer (CIO) of the Office of Technology Services (OTS), as well as all campus departments and divisions. Kevin Uren, Director of Infrastructure Services, serves as CSN's ISSO.

The ISSO assist campus departments and divisions to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of protected information. The ISSO also assists in evaluating the effectiveness of the current safeguards for controlling these risks, designing and implementing mitigating solutions, and regularly monitoring and testing the effectiveness of the program.

NSHE Information Security Officers Council

The NSHE Information Security Officers Council is comprised of security professionals at the institutions within the Nevada System of Higher Education; the Council provides oversight and guidance in the establishment of unified security standards across all institutions.

Records Retention and Disposition

"NSHE adopted, effective July 1, 2016, a comprehensive Records Retention and Disposition Schedule ("Schedule") that was developed specifically to address the universities' and colleges' particularized records, documents, etc. The Schedule can be found in the Regent's Procedures and Guidelines Manual, Chapter 18. The retention and destruction of all messages, documents, records, etc. at CSN should follow the Schedule. Many or most of such messages, documents, or records now are electronically created and maintained; the Schedule applies to both paper and electronic versions."

CSN Information Systems & Electronic Resources Acceptable Use Policy can be located via the following link:

https://www.csn.edu/sites/default/files/documents/information_systems_and_eletronic_resources_acceptable_use_policy.pdf

The NSHE Records Retention and Disposition Schedule can be referenced via the following link:

https://www.csn.edu/sites/default/files/documents/pgmch18recordsretentionanddispositionschedule.pdf

The NSHE Information Security Officers Council has prepared a proposed data classification related to content for consideration of the Nevada System of Higher Education System Administration Office.

Information Security Risk Management

Prioritization

Prioritization of our efforts is based on the number of users impacted. This would include centralized systems that are used campus-wide, administrative systems, and the campus wired/wireless data network. Departmental systems or single-use systems would follow in order of magnitude.

Approach

Assessing internal and external risks is a primary responsibility of the ISSO. Working with members of the college community regularly scheduled risk assessments are performed and serve to determine the health of the existing solutions and system enhancements to address the ever-changing digital security threat landscape.

Priority emphasis in the application of risks identification is assigned to the following areas:

- Personally Identifiable Information (PII)
- Hardware and Software Environment
- Physical Security of the Data

Personally Identifiable Information (PII)

As outlined in Records Retention & Disposition section, each data custodian or designee will conduct periodic reviews to determine if the current security needs are adequate to protect the information outlined in the NSHE standard.

The ISSO will conduct regular reviews of the procedures, incidents, and root cause analysis. This will help to ensure that CSN is following the standards established by NSHE that helped to establish a standard in Nevada. The ISSO will develop written plans to ensure that communication of confidential information that could contain PII is encrypted in transit. Evaluating data loss prevention (DLP) options to ensure that data in transit is properly secured. The ISSO will also develop written policies and procedures on the proper handling of detection and response to actual or attempted attacks targeting CSN related resources.

As noted in section *"Records Retention and Disposition"* the NSHE Information Security Officers Council has prepared a data classification of content for consideration. Upon approval, this section will contain additional details related to the types and content in terms of risk and the need to encrypt in transit.

Hardware and Software Infrastructure

OTS will ensure that patches are tested and applied in a timely fashion to keep up with the threat landscape. This includes all servers and desktops that are under OTS control and includes operating systems, system software/applications, database management systems, and the networking infrastructure including switches, routers, firewalls, and wireless systems. OTS will also work with other departments throughout the college to develop guidelines to manage these systems to ensure that they are protected and patches applied if they are connected to the campus network.

Physical Security

Physical security including the electronic access control system is under the responsibility of the Facilities Management Department and monitored by CSN Campus Police. Physical access to data closets and data centers is granted by both lock/key as well as through proximity reader access. Many of these areas are collocated for both OTS and Facilities Management. Access reports are available for review by Facilities Management leadership and Campus Police and reviewed periodically by the ISSO for unauthorized access.

The ISSO will coordinate with other areas of the college to develop guidelines that cover physical security related to devices that reside outside of the primary data centers and data closets. Surveys shall be conducted of other identified physical security risks in an effort to mitigate the exposure of CSN to paper or electronic records that are stored in unsecured locations.

Disaster Recovery Plan

The ISSO will work to formalize a more detailed approach to Disaster Recovery as well as data protection, recovery point objective (RPO), recovery time objectives (RTO), and a business continuity plan to cover CSN's infrastructure and resources.

Information Security Incident Response Plan

CSN in conjunction with the Nevada System of Higher Education will be coordinating the development of a formal incident response plan. The plan shall be reviewed regularly to ensure compliance and to ensure that the proper response is initiated when a misuse of protected information or a form of cyber-attack has been validated.

NSHE has adopted the use of the NIST Cybersecurity framework and the Nevada Board of Regents will be voting to ratify this as the standard across all Nevada Higher Educational institutions. With this direction, the plan will be developed to adhere to the RS.RP-1 standard (Page 33 of the link provided https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf).

Nevada Law also identifies requirement for breach notification. The plan will be developed to adhere not only to the NIST standard but also standard 603A.220 of Nevada State Law (https://www.leg.state.nv.us/NRS/NRS-603A.html#NRS603ASec220).

Information Security Awareness and Education

OTS works with the Center for Academic & Professional Excellence (CAPE) department to manage employee training. Conducting this training during convocation or during semesters will afford coverage for new employee orientation as well as a refresher to those returning. The ISSO regularly reviews the content to ensure accuracy as well as provide updated content to reflect the current security landscape.

OTS also provides background on campus computers and labs with regular information related to security that students could leverage for their student and personal lives. OTS is active during October, Cyber Security Month, to extend additional information and education to CSN resources to increase awareness.

Management of Third Party Contractors and Service Providers

CSN's Facilities and Auxiliary departments will select/approve the use of service providers and justify the needs/access types those organizations will require. This may require OTS and ISSO review of the required needs and the safeguards proposed to ensure secure access in both directions. Once adequate safeguards are determined, access will then be processed and tracked accordingly in the help desk system.

Information Security Compliance

Institutional Compliance

Compliance and adherence to policies and procedures is the responsibility of all individuals provided access to and the ability to utilize systems. Users, which include but are not limited to faculty, staff, students, volunteers, contractors, or other CSN Information Systems must accept acknowledgement of the Acceptable Use Policy and associated responsibilities.

Evaluation and Revision of the Information Security Program

The Information Security Program will be evaluated and adjusted to reflect changing circumstances, including changes in the college's business practices, operations, or arrangements, or as a result of testing and monitoring the safeguards. These changes may also be a result of implementing proactive measures to anticipated changes in the security landscape. Substantive changes in business practices, operations, or arrangements will require a new assessment of risk for the area of change.

The input to proposed changes should include the following information:

1. Feedback from interested parties or data owners
2. Results from independent reviews
3. Status of preventative and corrective actions
4. Results of previous reviews
5. Information security policy compliance
6. Changes that could affect the college's approach to managing information security (e.g., contractual, regulatory, legal conditions, technical environment)
7. Trends related to threats and vulnerabilities
8. Reported information security incidents
9. Audit findings