NSCS Information Security Standard 1: Definitions and Related Law, Policies, and References

1.1 Definitions

Availability - Ensuring that information is ready and suitable for use.

Central Identity Provider – a single Identity and Access Management system which often involves both single-sign-on architectures and access control systems.

Certificate, also Digital Certificate - An electronic document used to bind together a public key with an identity.

Chief Information Officer (CIO) – The senior officer responsible for Information Technology strategy, oversight, and systems required to support the College goals and objectives.

Chief Information Security Officer (CISO) - The person appointed by the President under Policy 7003 to oversee the Information Security Program, typically the College CIO or College Vice President for Information Technology.

Cloud Computing Service - The utilization of servers or information technology services of any type that are not hosted by the NSCS. Cloud Services are comprised of different methods of delivery, including Software as a Service (Saas), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS).

Confidentiality - Ensuring that information is not disclosed to unauthorized individuals.

Credential – A token of access to Information or Physical Assets, which may include but not be limited to ID Cards and username/password combinations.

CUI – Confidential Unclassified Information as defined in NIST 800-171 which is equivalent to NSCS High and Medium risk data.

Data - Unstructured information without added organization, interpretation or analysis.

Data Owner – The Nebraska State College System.

Data Steward – Person within NSCS who has administrative control and is officially designated as accountable for a specific information asset dataset. This person has ultimate responsibility for classifying, controlling and protecting the data.

Data User – Any faculty, staff, student or third-party provider who is authorized by the Data Owner to access Information Assets.

Electronic Communication - The exchange of data on systems provided by NSCS including but not limited to email systems, voice mail, telephone systems, phone lines, modems, computers, software, networks, electronic bulletin boards, Internet access, intranets and facsimile machines.

IaaS (Infrastructure as a Service): - Cloud computing service which provides infrastructure such as hardware, virtual servers, and operating systems.

Incident - An action or condition that violates IT Security policy, potentially compromises information confidentiality, integrity or availability.

Information Security Program – The collection of Standards, and associated College Procedures and Plans, designed to protect enterprise communications, systems and assets from both internal and external threats. Governed by NSCS Policy 7003.

Integrity of Data - Ensuring accuracy, completeness, and consistency.

ISP – Information Security Program.

Multi-factor Authentication -- Multi-factor authentication is an authentication method in which a Credential is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence. Two-factor authentication is a type, or subset, of multi-factor authentication.

NeSIS/NeBIS – Nebraska Student Information System and Business Information System respectively. These systems are collaboratively operated with the University of Nebraska and are the systems of record for student and human resources/finance information respectively.

PaaS (Platform as a Service) - Cloud computing service that provides a platform on which the customer can develop and run applications.

Phishing - The attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes indirectly money) by masquerading as a trustworthy entity in an electronic communication.

PKI Authentication – Public Key Infrastructure authentication of an account using an asymmetric encryption key Credential

Removable or Transportable Media - Includes but is not limited to paper forms, reports, cassettes, CDs, USB tokens, flash drives, hard drives and zip drives.

SaaS (Software as a Service) - An application hosted, maintained, and updated by the cloud service vendor and available to users over the Internet.

Security Staff - NSCS employees who have information security listed as part of their official duties.

Sensitive Information – NSCS data in the High or Medium risk category.

Service (System) Account -- an account that a computer service or application uses to run and access resources. A service account could also be an account that is used for a scheduled task (sometimes referred to as a batch job account), or an account that is used in a script that runs outside of a specific user's context.

System Office Information Security Officer (SOISO) - Is the Vice Chancellor for Facilities & Information Technology.

Technology Resources – Technology Resources include, and are not limited to: all NSCS owned, operated, leased, outsourced, or contracted computing, networking, telephone and information resources; all NSCS electronic information including data, voice and video; all NSCS data, voice, and

video networks; all NSCS application systems and software used to conduct campus business; and all NSCS assets connected to the networks. Employees are to refer to Information Security Standard 15: Bring Your Own Device (BYOD) regarding use of personal devices for work related functions beyond the guidelines indicated in the AUP (Standard 5). Intellectual Property Rights are governed by the SCEA agreement.

User – Anyone that is authorized and has been granted access to NSCS computer resources.

VLAN – A Virtual Local Area Network (VLAN) is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire.

Vulnerability – Condition which allows people, property, resources and systems to be susceptible to harm, degradation, or destruction.

1.2 Related Law, Policies, and References

State Law and Regulation

- Nebraska State Security Breach Notification Law: Neb. Rev. Stat. 7-801 to 87-808 shall be known and may be cited as the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006. https://nebraskalegislature.gov/laws/statutes.php?statute=87-801
- Nebraska State Social Security Number Law: Neb. Rev. Stat. 48-237 https://nebraskalegislature.gov/laws/statutes.php?statute=48-237
- Nebraska Information Technology Commission, NITC 8-802 – Incident Response Plan - https://nitc.nebraska.gov/standards/8-802.pdf

Related NSCS Board Policies

- Board Policy 2070 – Records of the System
- Board Policy 3650 – Student Records
- Board Policy 5008 – Employee Use of Technology Resources
- Board Policy 7004 - Federal Personal Information Security Programs
- Board Policy 7008 - Risk Management
- Board Policy 7015 - Contracts; Limitations, Exemptions
- Board Policy 8064 - Capital Construction and Information Technology; Bids

References

- NIST 800-171 https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
- NIST Special Publication 800-61r2 - https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
- University of Nebraska Policy ITS-05 -- https://its.nebraska.edu/-/media/unca/docs/offices-and-policies/policies/policies/its-05-data-classification-and-storage-policy.pdf?la=en

Revision History

April/14/2019: Initial submission by PCSS
May/8/2019: Initial review by SOISO/CISOs
July/8/2019: Second review by SOISO/CISOs
July/25/2019: Third review by SOISO
Sept/30/2019: Fourth review by SOISO/CISOs using campus feedback