University of Nebraska

December 19st, 2016

High Risk Data Definitions
and
Minimum Security Standards

Introduction

In April, 2016, on behalf of the Data Governance Council commissioned by University of Nebraska President, a working committee was formed with the primary purpose to protect the University of Nebraska (NU) and the Nebraska State College System's (NSCS) institutional data (includes, and is not limited to, information in paper, electronic, audio, and visual formats) while preserving the open, information-sharing mission of their academic cultures. The University of Nebraska and the State College System classify institutional data in accordance with legal, regulatory, administrative, and contractual requirements; intellectual property and ethical considerations; strategic or proprietary value; and/or operational use. The following outlines identified high risk data and minimum data security requirements to protect that data.

High Risk Data Definition

University of Nebraska data is classified as high-risk if:

- Protection of the data is required by law/regulation,
- Nebraska is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed or
- The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.

High-Risk Data

Social Security numbers:
- Employees
- Students
- Dependents
- Contractors (vendors)
- Social Security card **
- Dependent verification documents **
- Vendor W-9 form **
- Employee I-9 form **
- Employee W-4 form **

Credit card numbers:
- Purchasing cards
- Individual travel cards
- University settlement cards (e.g. travel agency)
- Individual travel receipts (if not redacted) **

Financial account numbers:
- Employee bank accounts
  - Payroll
  - Travel expenses

Vendor bank account numbers
Vendor ACH enrollment information **
Employee direct deposit enrollment **
Student checking/saving account routing and account numbers

Student ITIN (International Tax ID Number)

Driver's license numbers:
Qualification information for those required to drive vehicles
Driver's license copy for new employee **
Students - Collected on FASFA
Copy of driver's license may be stored in ImageNow/paper in gender change process

Passport and visa numbers:
Non-resident aliens
Passport and visa copies **

Immunization Data

- Immunization records
  - NeSIS – Immunization/dates
  - Attachments containing:
    - Name
    - Birth date
    - SSN
    - List of immunization
    - Date of immunization

** Scanned document images

Minimum Security Standards

Minimum security standards for University of Nebraska high risk data are categorized by three areas: endpoints, servers and applications. Any one of these areas containing high risk data as defined by this policy most conform to these minimum security requirements.

Endpoints

An endpoint is defined as any laptop, desktop, or mobile device.

1. Determine the risk level by reviewing the data, server and application risk classification examples and selecting the highest applicable risk designation across all. For example, an endpoint storing Low Risk data but storing High Risk data but utilized to access a High Risk application is designated as High Risk.

2. Follow the minimum security standards in the table below to safeguard your endpoints.

STANDARDS	RECURRING TASK	WHAT TO DO	HIGH RISK DATA
Patching	✓	Based on National Vulnerability Database (NVD) ratings, apply high severity security patches within 7 days of being published, medium severity within 14 days and low severity within 28 days. Use a currently supported OS version.	✓
Device Inventory		All devices used to access NeSIS or SAP data should be inventoried by the responsible technical office per University Memorandum 16 for the University, and appropriate guidelines for the State Colleges, and the inventory list provided to the campus CISOs.	✓
Whole Disk Encryption		Enable full disk encryption.	✓
Malware Protection		Install supported antivirus and malware protection.	✓
Backups		NeSIS and SAP data should not be stored on endpoint devices. Any saved data sets should be stored on approved University or State College storage.	✓
Configuration Management		Install University or State College provided endpoint management tools.	✓

Regulated Data Security controls		This standard does not replace applicable regulatory standards such as PCI DSS, HIPAA or export controls as identified in University or State College policy. Consult with the Information Security Officers for specific details.	✓
Firewall		Enable local firewall in default deny mode and permit minimum necessary services.	✓
Data Scans	✓	Require data discovery tools such as Identify Finder or other available tools to be ran periodically/annually on all endpoints that contain high risk data.	✓
Physical Endpoint Protection		Desktops, laptops and mobile devices should be secured against theft when not in use. Computer screens and mobile devices should be locked with a password when not in use. Install MDM (mobile device management) on mobile devices.	✓
Education	✓	Educate and provide an on-going awareness program on the importance of handling and securing high risk data. Provide annual or periodic re-certification of all interfaces that extract high risk data. Provide annual FERPA training provided to all NeSIS business staff who use and access high risk data.	✓

Servers

STANDARDS	RECURRING TASK	WHAT TO DO	HIGH RISK DATA
Patching	✓	Apply security patches within 14 days of being available from the vendor. Use a currently supported OS version.	✓
Inventory		All servers in the data flow path NeSIS or SAP data should be inventoried by the responsible technical office per University Memorandum 16 for the University, and appropriate guidelines for the State Colleges, and the inventory list provided to the campus CISOs.	✓
Firewall		All NeSIS and SAP servers will be behind a network firewall(s) and host based firewall(s) in default deny mode and permit minimum necessary services as approved by the Information Security Council.	✓
Credentials & Access Control	✓	Federation with University campus and State College authentication services is recommended. Review existing accounts and privileges periodically. Follow University and State College policy on password complexity for all accounts.	✓

Two-Factor Authentication		Require multi-factor authentication for all users and administrator access.	✓
Centralized Logging		All server logs in the data flow path NeSIS or SAP data should be collected and forwarded to the University's log aggregation tool. Logs will be retained according to University policy and regulatory compliance.	✓
Vulnerability Management	✓	Perform monthly vulnerability scans. Remediate severity 5 vulnerabilities within seven days, severity 4 vulnerabilities within 14 days, and severity 3 vulnerabilities within 28 days of availability. Internal mitigations are required for vulnerabilities that cannot be remediated.	✓
Malware Protection	✓	Servers must not be used for general web browsing or reading email.	✓
Physical protection		All NeSIS and SAP servers and any servers in the data flow path should be located in approved University or State College data centers.	✓
Security, Privacy & Legal Review		Request a Security, Privacy, and Legal review from the Information Security Council as part of the change control process for the NeSIS and SAP environments.	✓
Regulated data security controls		This standard does not replace applicable regulatory standards such as PII, PCI DSS, HIPAA, or export controls.	✓
Monitoring		All NeSIS and SAP systems should be monitored for uptime and data released to respective campuses and colleges for parsing and review.	✓
Data Scans	✓	Require data discovery tools such as Identify Finder or other available tools to be ran periodically/annually on all servers that contain high risk data.	✓
Education	✓	Educate and provide on-going Awareness Program on the importance of handling and securing high risk data. Provide annual or periodic re-certification of all interfaces that extract high risk data. Provide annual FERPA training provided to all NeSIS business staff who use and access high risk data.	✓

Applications

STANDARDS	RECURRING TASK	WHAT TO DO	HIGH RISK DATA
Patching	✓	Use a supported version of the application and apply patches provided by the vendor.	✓
Inventory	✓	Maintain a list of applications and data classifications. Review and update records quarterly.	✓
Firewall		All web applications should be secured behind a web application firewall. All application firewall rulesets should be audited and updated annually.	✓
Credentials & Access Control	✓	Federation with campus authentication services is recommended. Review existing accounts and privileges quarterly. Follow university or state college policy on password complexity for all accounts.	✓
Two-Factor Authentication		Require multi-factor authentication for all interactive user and administrator logins where applications are compatible with multi-factor authentication. This will includes access to high risk data within SAP and NeSIS applications and those external applications to the ERP systems.	✓
Centralized Logging		All application logs in the data flow path for NeSIS or SAP should be collected and forwarded to the University's log aggregation tool. Logs will be retained according to University policy and regulatory compliance.	✓
Website SSL		Obtain and use a TLS certificate on all websites. Sites that accept credentials or credit card information use an "extended validation" certificate. Obtain certificate from university Information Security department.	✓
Vulnerability Management	✓	Monthly application vulnerability scan performed by the university Information Security department. Remediate severity 5 vulnerabilities within seven days, severity 4 vulnerabilities within 14 days, and severity 3 vulnerabilities within 28 days of vendor approved availability.	✓
Secure Software Development		Include security as a design requirement. Review all code and correct identified security flaws before deployment. Use of static code analysis tools recommended.	✓
Security App Scan		All applications should be scanned for security vulnerabilities by the university Information Security department.	✓

Developer Training	✓	All developers are required to complete 10 of the 43 SANS training modules annually.	✓
Backups/Disaster Recover		All critical applications should be redundant and hosted in geographically dispersed locations.	✓
Dedicated Admin Workstation		Access administrative accounts only via the Full Tunnel VPN profile.	✓
Security, Privacy & Legal Review		Request a Security, Privacy, and Legal review from the Information Security Council as part of the change control process for the NeSIS and SAP environments.	✓
Regulated Data Security Controls-		This standard does not replace applicable regulatory standards such as PII, PCI DSS, HIPAA, or export controls.	✓
Education	✓	Educate and provide on-going Awareness Program on the importance of handling and securing high risk data. Provide annual or periodic re-certification of all interfaces that extract high risk data. Provide annual FERPA training provided to all NeSIS business staff who use and access high risk data.	✓

Definitions

Computing Equipment
Any University or State College desktop or portable device or system, or any non - university or non-state college desktop, portable device or system used to access university or state college - provided data or services

Masked number
- A credit card primary account number (PAN) has no more than the first six and the last four digits intact, and
- All other Prohibited or Restricted numbers have only the last four intact. See the entire DSS 3.1 Standard (if you are willing to agree to some terms).

NIST - Approved Encryption
National Institute of Standards and Technology (NIST) develops and promotes cryptographic standards that enable U.S. Government agencies and others to select cryptographic security functionality for protecting their data. Encryption which meets NIST - approved standards is suitable for use to protect data if the encryption keys are properly managed. In particular, secret cryptographic keys must not be stored or transmitted along with the data they protect. Cryptographic keys have the same data classification as the most sensitive data they protect. Payment Card Industry Data Security Standards the practices used by the credit card industry to protect cardholder data.

The Payment Card Industry Data Security Standards (PCI DSS)
PCI DSS requires all merchants to comprise an effective and appropriate security program for systems that store, process, or transmit card payment data.

Protected Health Information (PHI)
All individually identifiable information that relates to the health or health care of an individual and is protected under federal or state law. For questions about whether information is considered to be PHI, contact the University or State College Privacy Officer.

Qualified Machine
A computing device located in a secure University facility and with access control protections that meet the Payment Card Industry Data Security Standards.

Family Educational Rights and Privacy Act (FERPA)
Student Record Information maintained by the University or State Colleges and under jurisdiction of the Family Educational Rights and Privacy Act (FERPA) tenets. Student Records include University or State Colleges - held student academic transcripts and other related academic records (official and unofficial), and University - held records related to:

(i) academic advising,
(ii) health/disability,
(iii) academic probation and/or suspension,
(iv) conduct (including disciplinary actions), and
(v) directory information and other biographical and personal data maintained by the Office of the University Registrars and other University or State Colleges offices. Applications for student admission are considered to be Student Records at the point of enrollment to a University or State College campus.