-

The appropriate level of protection must be incorporated into operational systems throughout the development process. Especially in cases where the data is sensitive or requires protection because of the risk and magnitude of loss or harm that could result from improper operation, manipulation or disclosure.

- • = Section 5.3
- • =
  - o Protected (or FERPA) Information Handling Standard
  - o Restricted Information Handling Standard
  - o Confidential Information Handling Standard
  - o Vendor Cloud Service Security Standard
  - o Data Administration and Management Standard (future)
  - o System Acquisition, Development, and Maintenance Lifecycle Standard (future)

5.5.2 Protection of Confidentiality, Authenticity and Integrity of Information

USNH will protect the confidentiality, authenticity and integrity of information.

- • = Sections 5.1 and 5.3
- • =
  - o Protected (or FERPA) Information Handling Standard
  - o Restricted Information Handling Standard
  - o Confidential Information Handling Standard
  - o Data Administration and Management Standard (future)

5.5.3 Conducting IT Projects and Support Activities in a Secure Manner

Changes and updates to systems and data must be traceable to accountable individuals and source documents under a defined management process.

- • = 5.12
- • =
  - o System Acquisition, Development, and Maintenance Lifecycle Standard (future)
  - o Security Configuration Management Standard (future)

5.5.4 Maintaining Security of Application System Software and Dat9 446.11 Tm0 g0 G[(s)8(5)-3(.1)9(and)] TET4 g00

5.7.1.2 Password change schedules will be established and communicated to password holders at timely intervals.

- Already addressed in the USNH Password Policy

5.7.1.3 Employee-specific passwords shall be treated as sensitive, confidential information and shall not be shared. Employee-specific passwords also shall not be stored on-line or written down unless adequately secured from unauthorized viewing.

- Already addressed in the USNH Password Policy

5.7.1.4 Authorized users of computer systems will take reasonable and appropriate measures to prevent access to systems by unauthorized persons.

- Already addressed in the USNH Password Policy

5.7.1.5 All data on computers or electronic storage devices (including but not limited to desktop, laptop, server, or handheld devices) shall be wiped clean of files and data prior to transfer or surplus.

- = Section 5.12.7
- = Information Technology Resource Secure Disposal Standard (future)

5.7.1.6 Social Security Number (SSN) is a particularly sensitive data item for all constituents. Whenever the SSN is utilized and/or displayed, the following shall apply to mitigate its exposure to unauthorized access.

- = Section 5.3
- =
    - o Restricted Information Handling Standard
    - o Data Administration and Management Standard (future)

5.7.1.6.1 A SSN shall not be sent via e-mail unless encrypted or masked for all but the last four (or fewer) digits of the number.

- = Restricted Information Handling Standard

5.7.1.6.2 Shared electronic and paper reports shall have all but the last four (or fewer) digits of the SSN masked. In the limited cases where SSN is required for regulatory compliance related to employment, payroll processing, provision of benefits, and tax reporting, access to the information shall be limited to those with need to know.

- =
    - o Restricted Information Handling Standard
    - o Data Administration and Management Standard (future)

5.7.1.6.3 Paper and electronic documents containing a SSN shall be disposed of in a secure fashion.

inventory should be drawn up and maintained of the important assets associated with each information system. Each asset should be clearly identified and its ownership and security classification agreed [upon] and documented together with its current location.

- • = 5.5.4, 5.12.5
- • =
  - o Security Categorization Standard
  - o Information Technology Resource Inventory Management Standard (future)

5.10.3 Safeguarding Information Sensitivity. All USNH institutions, providers, managers and users of USNH IT resources will establish methods to identify, classify, and where necessary, restrict access to institutional data so as to recognize sensitivity, protect confidentiality or safeguard privacy as required by law, institutional policy or ethical considerations.

- • NP = Section 5.3, 5.5, 5.7, 5.8. 5.9
  - o Also revised USNH Information Classification Policy
- • =
  - o Access Management Standard
  - o Access to Password Protected Information Standard
  - o Confidential Information Handling Standard
  - o Cybersecurity Awareness and Training Standard
  - o Privileged Access Management Standard