UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #09 (2022) Incident Response Policy

Policy Title:	Incident Response Policy
Policy Type:	Board of Visitors
Policy Number:	BOV UISP #09 (2022)
Approval Date:	Month, Day, Year
Responsible Office:	Office of Information Technology (OIT)
Responsible Executive:	Vice President for Operations and Chief Strategist for Institutional Effectiveness
Applies to:	All Norfolk State University (NSU) employees (classified, hourly, official representatives, and third-party vendors)

POLICY STATEMENT

The Incident Response policy addresses the scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance required to establish an acceptable level of incident response security controls at Norfolk State University. This includes, but is not limited to, any regulatory requirements that Norfolk State University is subject to, incident response best practices, and the requirements defined in this policy. The Incident Response Policy provides a consistent and effective approach to the management of information security incidents. It provides a framework by which NSU shall determine the scope and risk of an information security incident, respond appropriately to that incident, communicate the results and risks to all stakeholders, and reduce the likelihood of an incident from occurring or reoccurring.

This policy also meets the control requirements outlined in Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Information Security Policy SEC519 and Security Standard SEC501, Section 8.8 Incident Response Family, Controls IR-1 through IR-8, to include specific requirements for the Commonwealth of Virginia.

Table of Contents **Page Number**

UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #09 (2022) Incident Response Policy

DEFINITIONS

Chief Information Officer (CIO): Oversees the operation of NSU Information Technologies. Responsible for policies, procedures, and standards for assessing security risks, determining the appropriate security measures, and performing security audits.

Information Security Incident: A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices.

Data Custodian: Individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage.

Data Owner: The agency manager responsible for decisions regarding data and is responsible for evaluating and classifying sensitivity of the data, and any legal or regulatory requirements, and business needs.

Director of IT Security (DIS): The senior management designated by the CIO of NSU to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of information systems and data.

Encryption: The process or the means of converting original data to an unintelligible form so it cannot be read by unauthorized users.

Intrusion Detection Systems (IDS): An IPS detects an attack on a network or computer system. It uses signatures of known attack attempts to signal an alert. It also looks at deviations from the normal routine as indicators of an attack.

Intrusion Prevention Systems (IPS): An IPS prevents an attack on a network or computer system. It stops the attack from damaging or retrieving data and can block attacks in real time.

Keystroke Logging: Referred to as keylogging or keyboard capturing, it is the action of recording the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.

Office of Information Technology (OIT): The Office of Information Technology (OIT) manages the administrative and academic information technology resources for Norfolk State University.

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Sensitive Data: Any data of which the compromise, with respect to confidentiality, integrity, and/or availability, could adversely affect NSU interests, the conduct of NSU programs, or the privacy to which individuals are entitled.

NORFOLK STATE UNIVERSITY

UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #09 (2022) Incident Response Policy

CONTACT(S)

The Office of Information Technology officially interprets this policy. The Chief Information Officer is responsible for obtaining approval for any revisions as required by BOV Policy #1 (2014) *Creating and Maintaining Policies* through the appropriate governance structures. Questions regarding this policy should be directed to the Office of Information Technology.

STAKEHOLDER(S)

All NSU Faculty, Staff, Students, & Community

INCIDENT RESPONSE POLICY

OIT will review and update the Incident Response policy annually or more frequently if required to address changes.

A. INCIDENT RESPONSE

1. The Director of IT Security (DIS) shall or shall require its service provider document and implement threat detection practices that at a minimum include the following:

    a. Designates an individual responsible for threat detection program, including planning, development, acquisition, implementation, testing, training, and maintenance.

    b. Implements Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).

    c. Conducts IDS and IPS log reviews to detect new attack patterns as quickly as possible.

    d. Develops and implements required mitigation measures based on the results of IDS and IPS log reviews.

2. The DIS shall or shall require its service provider document and implement information security monitoring and logging practices that, at a minimum, include the following:

    a. Designation of individuals responsible for the development and implementation of information security logging capabilities, as well as detailed procedures for reviewing and administering the logs.

    b. Standards that specify the type of actions an IT system should take when a suspicious or apparent malicious activity occurs.

c. Prohibits the installation or use of unauthorized monitoring devices.

d. Prohibits the use of keystroke logging, except when required for security investigations and a documented business case outlining the need and residual risk has been approved in writing by the Agency Head (or designee).

3. The DIS or designee shall document information security incident handling practices and shall incorporate its service provider’s procedures for incident handling practices that, at a minimum, include the following:

   a. Designation of an Information Security Incident Response Team that includes personnel with appropriate expertise for responding to cyber-attacks.

   b. Controls to deter and defend against cyber-attacks to best minimize loss or theft of information and disruption of services.

   c. Proactive measures based on cyber-attacks to defend against new forms of cyber-attacks and zero-day exploits.

   d. Information security incident categorization and prioritization based on the immediate and potential adverse effect of the information security incident and the sensitivity of affected IT systems and data.

B. INCIDENT RESPONSE TRAINING

1. The DIS or designee shall provide incident response training to users consistent with assigned roles and responsibilities:

   a. After being assigned an incident response role or responsibilities.

   b. When required by information system changes.

   c. On an annual basis or more frequently if required to address an environmental change thereafter.

C. INCIDENT RESPONSE TESTING AND EXERCISES

1. The DIS or designee shall test and/or exercise the incident response capability on an annual basis or more frequently if required to address an environmental change using

organization-defined tests to determine the incident response effectiveness and document the results.

2. The DIS or designee shall coordinate incident response testing with organizational elements responsible for related plans (i.e., Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, etc.).

D. INCIDENT HANDLING

1. The DIS or designee shall:

   a. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

   b. Coordinate incident handling activities with contingency planning activities.

   c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implement the resulting changes accordingly.

   d. Implement and coordinate incident handling capability for insider threats across all sensitive components or elements of the organization.

   e. Correlate incident information and individual incident responses to achieve an NSU-wide perspective on incident awareness and response.

   f. Identify immediate mitigation procedures, including specific instructions, based on information security incident categorization level, on whether or not to shut down or disconnect affected IT systems.

   g. Establish procedures for information security incident investigation, preservation of evidence, and forensic analysis.

2. The DIS shall adhere to the following requirements where electronic records or IT infrastructure are involved. Also, where non-electronic records are involved or implied, the following are advisory in nature, but are strongly recommended:

   a. Identify and document all NSU systems, processes, and logical or physical data storage locations (whether held by NSU or a third party) that contain personal or medical information.

      i. Personal information means the first name or first initial with the last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth of Virginia (COV) when the data elements are neither encrypted nor redacted:

1. Social security number.

2. Driver’s license number or state identification card number issued in lieu of a driver’s license number.

3. Financial account number, or credit card or debit card number, combined with any required security code, access code, or password that would permit access to a resident’s financial accounts.

ii. Medical information means the first name or first initial with the last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth when the data elements are neither encrypted nor redacted:

1. Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

2. An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

b. “Redact” for personal information means alteration or truncation of data such that no more than the following are accessible as part of the personal information:

i. Five digits of a social security number.

ii. The last four digits of a driver’s license number, state identification card number, or account number.

c. “Redact” for medical information means alteration or truncation of data such that no information regarding the following is accessible as part of the medical information:

i. An individual’s medical history.

   ii. Mental or physical condition.

   iii. Medical treatment or diagnosis.

   iv. No more than four digits of a health insurance policy number, subscriber number.

   v. Other unique identifiers.

d. Include provisions in any third-party contracts requiring that the third party and third-party subcontractors:

   i. Provide immediate notification to NSU of suspected breaches.

   ii. Allow NSU to both participate in the investigation of incidents and exercise control over decisions regarding external reporting.

e. Provide appropriate notice to affected individuals upon the unauthorized release of unencrypted and/or un-redacted personal information or medical information by any mechanism, including, but not limited to:

   i. Theft or loss of digital media, including laptops, desktops, tablets, CDs, DVDs, tapes, USB drives, SD cards, etc.

   ii. Theft or loss of physical hardcopy.

   iii. Security compromise of any system containing personal or medical information (i.e., social security numbers, credit card numbers, medical records, insurance policy numbers, laboratory findings, pharmaceutical regimens, medical or mental diagnosis, medical claims history, medical appeals records, etc.).

f. NSU shall disclose the breach of the system's security if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key.

g. If a Data Custodian is the entity involved in the data breach, they must alert the Data Owner so that the Data Owner can notify the affected individuals.

h. In the case of a computer (i.e., public kiosk, individually owned, or NSU resource) found to be infected with malware that exposes data to unauthorized access, individuals that may have had their information exposed due to use of that computer must be alerted in accordance with data breach rules. NSU shall notify the CIO when notification of affected individuals has been completed.

i. Provide notification that consists of:

- i. A general description of what occurred and when.
- ii. The type of Personally Identifiable Information (PII) that was involved.
- iii. What actions have been taken to protect the individual's personal information from further unauthorized access.
- iv. A telephone number that the person may call for further information and assistance if one exists.
- v. What actions NSU recommends that the individual take. The actions recommended should include monitoring their credit report and reviewing their account statements (i.e., credit report, medical insurance Explanation of Benefits (EOB), etc.).

j. Provide this notification by one or more of the following methodologies:

- i. Electronic notice.
- ii. Written notice to the last known postal address in the records of the individual or entity.
- iii. Telephone Notice.
- iv. Substitute Notice - under certain circumstance substitute notices will be allowed pursuant to ITRM Information Security Standard (SEC501), Section 8, Incident Response Handling (Pg. 96).

k. NSU shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated below.

- i. Hold the release of notification immediately following verification of unauthorized data disclosure only if law enforcement is notified and determines and advises NSU that the notice would impede a criminal or civil investigation, or homeland security or national security. Notice shall be made without unreasonable delay after NSU determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

E. INCIDENT MONITORING

1. The DIS or designee shall track and document information system security incidents.

2. The DIS shall monitor IT system event logs in real-time, correlate the information with other automated tools, identify suspicious activities, and provide alert notifications.

F. INCIDENT REPORTING

1. The DIS or designee shall:

    a. Require personnel to report suspected security incidents to OIT Security within 24 hours from when the occurrence was discovered or should have been discovered.

    b. Report security incident information to designated authorities (The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable laws, directives, policies, regulations, standards, and guidance).

    c. Report information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate NSU officials.

    d. Provide quarterly summary reports of IDS and IPS events to Commonwealth Security.

    e. Establish a process for reporting IT security incidents to the DIS. All NSU customers and partners are encouraged to report all information security incidents.

    f. Report information security incidents only through channels that have not been compromised.

G. INCIDENT RESPONSE ASSISTANCE

1. The DIS or designee shall provide incident response support resources, integral to OIT's incident response capability, which offers advice and assistance to users of the information system to handle and report security incidents.

2. The DIS or designee shall:

   a. Establish a direct, cooperative relationship between its incident response capability and external providers of information system protection capability.

   b. Identify NSU incident response team members to the external providers.

H. INCIDENT RESPONSE PLAN

1. The DIS or designee shall:

   a. Develop an incident response plan that:

      i. Provides NSU with a roadmap for implementing its incident response capability.

      ii. Describes the structure and organization of the incident response capability.

      iii. Provides a high-level approach for how the incident response capability fits into NSU.

      iv. Meets the unique requirements of NSU, which relate to mission, size, structure, and functions.

      v. Defines reportable incidents.

      vi. Provides metrics for measuring the incident response capability within NSU.

      vii. Defines the resources and management support needed to maintain and mature an incident response capability effectively.

      viii. Is reviewed and approved by designated officials within NSU.

b. Distribute copies of the incident response plan to NSU-defined list of incident response personnel (identified by name and/or by role) and appropriate elements.

c. Review the incident response plan at least once a year.

d. Updates the incident response plan to address system/NSU changes or problems encountered during plan implementation, execution, or testing.

e. Communicate incident response plan changes to the NSU-defined list of incident response personnel (identified by name and/or by role) and NSU elements.

f. Protects the incident response plan from unauthorized disclosure and modification.

EDUCATION AND COMPLIANCE

A. SECURITY POLICY TRAINING

Security policy training is intended to educate NSU employees who have a role in IT system security and to help foster an understanding of how NSU security policies protect the University employees, students, systems, and data.

1. NSU employees, who manage, administer, operate, or design IT systems, must receive role-based security training commensurate with their role. Personnel with assigned security roles and responsibilities will be trained:

    a. Before authorizing access to the information system or performing assigned duties.

    b. When required by policy changes.

    c. As practical and necessary thereafter.

2. OIT will educate and train all stakeholders and appropriate audiences on the policy's content using virtual or face-to-face engagements.

B. POLICY COMPLIANCE AND VIOLATIONS

1. OIT measures compliance with information security policies and standards through processes that include but are not limited to monitoring and audits.

2. Violations of this policy will be addressed in accordance with relevant NSU and Commonwealth of Virginia policies, including NSU Policy 32-01 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined individually by the appropriate executive or designee.

PUBLICATION

This policy shall be widely published and distributed to the NSU community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

1. Communicate the policy in writing, electronic or otherwise, to the NSU community within 14 days of approval.

2. Submit the policy for inclusion in the online Policy Library within 14 days of approval.

3. Educate and train all stakeholders and appropriate audiences on the policy’s content, as necessary. Failure to meet the publication requirements does not invalidate this policy.

REVIEW SCHEDULE

- Next Scheduled Review: Month, Day, Year
- Approval by, date: Month, Day, Year
- Revision History: *New Policy*
- Supersedes policies: *New Policy*

RELATED DOCUMENTS

1. ITRM Information Security Policy (SEC519): https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

2. ITRM Information Security Standard (SEC501): https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

3. ITRM Information Security Standard (SEC514): https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

4. Virginia Department of Human Resources Management Policy 1.75, Use of Electronic Communications and Social Media: https://hr.dmas.virginia.gov/media/1243/dhrm-policy-175-use-of-electronics-and-social-media.pdf