University of New Hampshire

INFORMATION SECURITY INCIDENT RESPONSE PLAN

Responsible Executive/University Officer: Chief Information Officer
Responsible Office: Information Technology
OLPM Reference: NA
Authorized Distribution: Public Document
Status: APPROVED

1 OVERVIEW

Security incidents must be reported promptly through the proper University and/or University System channels and resolved by designated professionals in a manner that is consistent with University policies, applicable laws, and this plan.

This document establishes the procedures for identifying, reporting and responding to an information security event. It establishes the basic language to discuss such events, identifies roles and responsibilities involved in responding to and recovering from these events, and provides a process for handing these events from the time an event is detected to the final debriefing and closeout.

The objectives of the Incident Response Plan are to:

- Enable the University to respond to an information security incident without delay and in a controlled manner
- Enable assessment of mitigation measures that can be taken to protect information, assets and privacy and limit or prevent damage during an active incident
- Provide a framework that supports the protection and preservation of evidence in the event of illegal or criminal activity
- Ensure provision of timely notification of those who need to know, including but not limited to University management, Federal and/or State agencies, and business partners.
- Ensure that communications with the public/media are handled appropriately by designated University personnel
- Support completion of all required investigation, documentation, appropriate notifications, and remediation in a timely and organized manner
- Continuously improve the way the University handles information security events

2 SCOPE AND AUDIENCE

The Incident Response Plan should be followed when the following types of events occur:

- Any unauthorized access to University owned and/or controlled information and/or technology resources, including any potential data breach
- Any such incident involving a member of the University community, including but not limited to students, faculty, staff, guests, volunteers, partners and visitors
- Any such incident involving services provided by third parties to the University, such as contracted vendors, partner institutions, etc.

If it is not clear whether this plan applies to a particular situation, the UNH CIO, UNH ISO and/or USNH Legal Counsel can provide guidance on applicability.

The intended audience of this plan is all Information Technology, Academic Technology, and Research Computing employees, administrators of information technology resources located outside of those areas, and all supervisors/managers.

Users of UNH information technology resources should be familiar with the sections of this plan related to identifying and reporting information security incidents.

3 IDENTIFICATION OF INFORMATION SECURITY INCIDENTS

Information security incidents are events that have the potential compromise the confidentiality, integrity, or availability of University information and/or information technology resources.

When in doubt about whether to report something, report it.

Examples of Information Security Incidents

- Computer account(s) accessed by an unauthorized person
- Compromise of credentials resulting from malware infection, phishing attack, or improper disclosure of password(s) to an unauthorized person
- Device(s) infected with ransomware
- Unintentional or intentional disclosure of protected University data to an unauthorized person or people
- Evidence that someone tampered with a computer account (ex. account sending spam
- Unauthorized access to, alteration of, or activity within a University information system (Unexplained or unauthorized code changes, compromised/defaced website, etc.)
- Physical theft/breach (ex. broken doors to IT facilities, stolen computers, etc.)
- Stolen or lost laptop, tablet computer or smartphone
- Denial of Service Attack
- Notification of publicly posted University credentials
- Red Flags (as required by FTC Red Flags rule) or Identity Theft
- Risks or circumstances that are may or are likely to result in any of the above
- Notification from a cloud-computing vendor of a breach involving UNH data

If it is not clear whether a specific situation constitutes an information security incident, report it and UNH Information Security Services will make the determination.

4 INCIDENT REPORTING

Any member of the UNH community can report an information security concern or event to UNH Information Security Services (ISS).

It is the responsibility of all UNH users to report any event that might compromise information security to their direct manager and/or one of the groups in the Information Security Incident Reporting Escalation List (see below). Events, incidents, and potential breaches reported to UNH personnel by vendors must also be reported using this process.

4.1 How to Report an Incident

Note: UNH employees in non-management positions should attempt to report the incident to their manager or supervisor before reporting to any other entity. If the manager or supervisor is unavailable, report the incident as per the instructions below.

1. Call the UNH IT Service Desk
    a. The UNH IT Service Desk phone number is 603-862-4242.
    b. During the academic year, calls are answered from 7:30 AM to 10:00 PM.
    c. During the summer, calls are answered from 7:30 AM to 5:00 PM.
2. Inform the Service Desk tech that you are reporting an information security incident.
    a. The only information that should be provided to the Service Desk tech is your name, contact information, and if the incident you are reporting has life/safety implications.
    b. The Service Desk tech will request that you complete the Information Security Services support form and will provide you with the link to access the form.
    c. It is important that you contact the Service Desk and speak to someone in person even if you already have the link to the ISS support form.
3. The Service Desk will contact the Information Security Services team and alert them of the incident report.
4. A member of the ISS team will contact you to confirm receipt of the incident report and to request any additional details about the incident.

If you need to report an incident outside the UNH IT Service Desk business hours, call UNH Police Dispatch at 603-862-1427 and inform the dispatcher that you need to report an information security incident and are requesting that they alert the UNH Information Security Officer.

If you become aware that the incident is more serious or broader than what you originally reported, submit another notification to the person or department that confirmed receipt of your incident report.

Detailed procedures for first level support teams on how to handle intake of information security incidents can be found in the *Operational Procedures for First Level Support Teams Handling Information Security Incident Reports* that is available from ISS.

5 INCIDENT RESPONSE

Once an incident has been reported to UNH Information Security Services (ISS), ISS serves as the primary point of contact and coordination for the duration of the incident except in situations where ISS determines the specifics of the incident warrant law enforcement involvement.

Once a determination has been made that an incident has occurred, investigation of the incident and/or forensic analysis related to the incident must be initiated by and coordinated through UNH Information Security Services. Additional investigation, evidence collection, forensic analyses, and/or incident remediation by individuals outside of UNH ISS is prohibited, unless directed by the UNH ISS Incident Coordinator.

Note: This does not preclude system, application, and database administrators from taking investigatory actions to determine if an anomalous event is in actuality an incident. However, if these actions indicate that an incident has occurred, regardless of perceived severity, it must be reported to ISS and all investigatory activity must stop until officially requested by the Incident Coordinator.

Note: In events, incidents, and potential/confirmed breaches involving UNH data stored, accessed, managed, or otherwise used by a vendor application, ISS may opt to immediately involve UNH Procurement Services and USNH Legal Counsel to provide guidance and to determine if there is also a breach of contract that needs to be pursued. Additionally, in incidents involving vendors, UNH may have limited ability to initiate, monitor, guide, or otherwise influence or control the investigation, mitigation, remediation, and any notification resulting from the incident.

Step 1: Assign Incident Coordinator

The UNH ISO or other designated ISS staff member assigns an Incident Coordinator who will be the primary point of contact for the duration of the response and recovery effort. The Incident Coordinator's name and contact information will be provided to the incident reporter and other relevant parties from the reporting department.

Step 2: Assess Incident Risk and Assign Classification

The Incident Coordinator, in conjunction with the ISS team and any other appropriate personnel, reviews the known details of the incident and determines the incident's initial risk classification according to the Information Security Incident Risk Classification Matrix.

Information Security Incident Risk Classification Matrix

Critical	Major	Minor
Wide-scale malware infection or tangible threat of infection	Isolated malware infection or tangible threat of infection involving more than 10 user devices	Malware infection of less than 10 devices (as part of a single event)
Multiple devices infected with ransomware with potential for wide-spread infection via network access	Multiple devices infected with ransomware	Single device infected with ransomware
Compromise of: • business critical system or application • Financial processing system or application • System or application that stores, processes, accesses, or manages Restricted data (includes vendor hosted applications)	Compromise of: • any information system or application not listed under the Critical category • Vendor hosted applications that do not use, access, store or manage Restricted data	
Compromise, breach, or potential exposure of Restricted data	Compromise, breach, or potential exposure of Sensitive data	
Intrusion detection system flags an unauthorized user penetration or access	Intrusion detection system flags potential unauthorized user penetration or access	
Confirmed compromise of high risk user credentials	Confirmed compromise of VIP or Elevated Concern user credentials	Confirmed compromise user credentials
Large-scale unauthorized exposure of user credentials	Exposure of user credentials (more than 1 but does not rise to the level of large-scale) Potential (but not confirmed) large-scale exposure of user credentials	Exposure of a single user's credentials Notification of user credentials posted publicly
Unauthorized physical access to the data center	Unauthorized physical access to an IT-managed area where physical controls are in place	

Theft or loss of physical computing equipment used to store, access, process, or manage Sensitive or Restricted data	Theft or loss of an unencrypted end-point	Theft or loss of an encrypted end point

Incidents classified as Minor are managed and remediated according to specific processes, procedures, and guidelines available from ISS. Most minor incidents do not require the involvement of ISS and can be managed and remediated per standard processes.

Incidents classified as Critical or Major, continue to Step 3.

Step 3: Assemble the Incident Response Team

Under the guidance of the Information Security Officer (ISO), the Incident Coordinator will assemble an Incident Response Team (IRT) who will be responsible for mitigation, investigation, and remediation of the incident. The make-up of this team will vary depending on the classification of the incident, the type of incident, and the information systems and data impacted by the incident.

When appropriate, the ISO and/or the Incident Coordinator will consult with the CIO, USNH Legal Counsel, the UNH Police Department, UNH leadership/administration, individual college administrators, Communications and Public Affairs (CPA), and other departments or groups in order to establish an IRT appropriate to respond to the specific incident.

Step 4: Mitigate the Potential for Additional Loss/Damage

The IRT determines if the incident is an active incident with ongoing impact. If the determination is made that the incident is ongoing, strategies to mitigate additional loss, damage, or exposure are identified, discussed, agreed, and implemented. The classification and specific details of the incident will determine the measures appropriate for mitigation, which may include:

- Firewall ports may need to be blocked until the source of an attack is known
- Systems may need to be shut down or taken off-line until they can be protected without disrupting services
- Protocols may need to be disabled temporarily
- Access to all users, storage, applications, subnets, etc. may need to be disabled until the extent of any compromise is understood
- 24x7 guard may need to be provided for physical access control
- Network access may need to be blocked or restricted to prevent additional intrusion or the spread of malware

With sign-off by the CIO or ISO, the IRT is empowered to take whatever action is deemed necessary, including the use of extraordinary measures, to mitigate the impact of or prevent further damage from an active information security incident.

In lieu of CIO or ISO approval, Service Owners can authorize the IRT to block access to the applications or systems under their purview or to take these applications or systems offline.

Note: Restoration of service/access and remediation activities cannot commence without the explicit approval of the Incident Coordinator on behalf of the IRT or at the direction of the CIO or ISO. Service Owners do not have the authority to authorize these activities.

Step 5: Investigate the Incident

If the IRT determines the incident is not an active incident, or, once steps have been taken to prevent further loss/damage and/or to mitigate the impact of the incident, the IRT investigates the incident.

During the investigation, the IRT will determine the following, wherever possible:

- How the incident occurred
- Whether or not the incident resulted in the exposure or potential exposure of restricted data
- If there are other systems, data, or services that might have been impacted or that may be at risk because of the incident
- If the incident involved criminal activity
- What steps need to be taken to recover from the incident

At any point in the investigation, the IRT may determine, based on the type and classification of the incident and the specific details of the loss or damage, thatit is necessary to involve other UNH departments to participate or assist in the investigation and subsequent remediation of the incident. These additional resources may or may not become part of the overall IRT and fall into two categories:

- Incident Handlers:
  - UNH IT Resources – to assist in investigation activities related to specific systems, databases, devices, and/or networks
  - Non-IT UNH Resources - to assist in investigation activities related to systems, infrastructure, and devices managed and administered outside of IT
- Subject Matter Experts:
  - UNH Communications and Public Affairs – to provide guidance on and assistance with notifications to the UNH community and other entities, to handle any contact with the press
  - USNH General Counsel – to provide legal guidance and support
  - UNH HIPAA Compliance Officer – to advise on any incident involving Protected Health Information
  - UNH Procurement – to advise on and assist with incidents involving contracted vendors
  - UNH Data Stewards – to advise on and assist with incidents involving restricted or sensitive data loss/exposure

In the event that the IRT's investigation uncovers criminal activity, the Incident Coordinator or the ISO will notify the UNH Police Department or other law enforcement agencies who may take over investigation of the incident. Processes and procedures related to information security incidents that have criminal components will be dictated by the relevant law enforcement agency investigating the incident.

Step 6: Define and Implement Remediation Plan

As the IRT investigates the incident, necessary remediation/mitigation activities will also be identified and must be documented, agreed, and organized into a Remediation Plan. These activities will vary depending on the type and scale of the incident and may include:

- Patching vulnerabilities in the impacted infrastructure components and identifying similar infrastructure components that might share that vulnerability in order to apply preventive patches
- Securing the accounts of compromised users
- Rolling back application code to pre-compromise backups
- Implementing additional security controls on impacted devices, systems, or networks
- Improving business processes to reduce the risk of recurrence
- Revising policies and procedures to reduce the risk of recurrence or the impact from similar future incidents
- Documenting the acceptance of risk in situations where the vulnerability or circumstance that enabled the incident to occur cannot be mitigated or remediated

In most cases, the activities outlined in the remediation plan will require assistance from Incident Handlers who are not part of the core IRT. When participation of Incident Handlers is required for remediation, the Incident Coordinator will monitor and coordinate these resources and the activities they need to perform.

6 INCIDENT CLOSE-OUT

Incident Documentation

The type of documentation required depends on the classification of the Incident.

- Incidents classified as Critical require a completed Incident Report, a Remediation Plan (which may or may not be documented separately from the Incident Report), an Incident Debrief write-up, and a tracking ticket in the ITSM ticketing system.
- Incidents classified as Major require an Incident Report and a tracking ticket in the ITSM ticketing system
- Incidents classified as Minor are only documented in a tracking ticket within the ITSM system.
- Additional documentation may be produced as needed, regardless of classification.

Incident Reports

Each incident with a classification of Major or Critical must be documented in an Incident Report. ISS provides a standard Incident Report template for use by Incident Coordinators and Incident Handlers for documentation purposes. Incident reports are confidential and can only be shared outside the IRT with authorization by the ISO.

The Incident Coordinator is accountable for incident report completion, but may not be the one completing the report. In some circumstances, there may be a need for multiple Incident Handlers to create individual Incident Reports. In these circumstances, the Incident Coordinator is responsible for collecting the various Incident Reports, ensuring they are completed correctly, and creating an overall Incident Report to which the individual Incident Handler reports are attached.

ISS is responsible for ensuring that incidents are appropriately documented, communicated, and archived.

Wherever possible, incident details should be captured and documented in the report as they occur to ensure the highest degree of accuracy. The following standards should be followed when completing an Incident Report:

- Document the date and time of activities as they happen.
- Each Incident Report must minimally contain:
  - A description of the incident
  - Information about the results of the investigation (attacker, cause, etc)
  - Impact on service, financial damage, violation of privacy, etc.
  - Actions taken
  - Notification decisions and completed notifications
  - Remediation plan information (unless the Remediation Plan will be documented separately).
  - The ITSM ticket number
- Incident Report numbering follows the following convention
  - Next sequential number
  - DDMMYYYY of the Incident
  - Report Submitter Initials – suffix
  - For example, the tenth Incident reported in 2017 occurring on June 4, 2017 that was submitted by John M Doe would use the following incident number – 01004062017JMD

Incident Summary

In addition to the Incident Report, an Incident Summary will be produced for each Major or Critical incident. This summary is intended to provide a high-level overview of the incident, investigation, mitigation, and remediation. The Incident Summary will be created by the Incident Coordinator and is a public document that can be shared without restriction. ISS provides a standard Incident Summary template for use by Incident Coordinators for documentation purposes.

When warranted, an Incident Summary may also be created for Minor incidents, need to be determined by ISS.

Incident Remediation Plans

There is no formal standard for documenting the remediation plan for an incident. IRT's should document the remediation plan in a way that facilitates communication and tracking. Remediation plans are required for all Critical incidents but can be included in the overall Incident Report.

Incident Debriefing

For all Critical Incidents, an after-action debriefing involving the IRT, Incident Handlers, Subject Matter Experts, and other relevant stakeholders will be conducted by ISS. The objective of this debrief is discuss and agree to lessons learned while responding to and remediating the incident and to identify opportunities for improving the overall Incident Response and Recovery process. This may include:

- Identification of process improvement opportunities within the Incident Response and Recovery processes
- Identification of process improvement opportunities to other business processes to prevent future incidents
- Identification of the need for policy, standard, or procedure revisions (not limited to policies, standards, and procedures related to Incident Response and Recovery)
- Identification of information security training opportunities (specific to incident response or as a preventative measure)

Incident debriefs should occur as quickly as possible after the incident response and recovery has been completed, especially for critical incidents.

Results of Incident debriefs will be used by ISS to prioritize improvements across the UNH Information Security Program as a whole.

Incident Communication and Notification Processes

The Incident Coordinator is responsible for communicating information about the Incident to appropriate personnel and for maintaining contact with key stakeholders, for the purpose of update and coordination, for the duration of the Incident.

Incidents classified as Major are communicated to the ISO immediately upon IRT confirmation of the Incident's classification. The ISO will determine if communication/notification to the CIO is appropriate.

All Incidents classified as critical are communicated to the ISO and CIO immediately upon IRT confirmation of the Incident's classification. The CIO will determine if communication/notification to UNH executive leadership (which may include the VPFA, Cabinet, University President, USNH) is appropriate.

When required, UNH Communications and Public Affairs (CPA) will be engaged to manage any communications/contact with the public, media, external agencies, etc. CPA will also be consulted in the event there is the need for a University-wide communication.

Mandatory notifications of regulated data (FERPA, HIPAA, CJIS, etc.) will be coordinated through the appropriate UNH subject matter expert (UNH HIPAA Compliance Officer, USNH Legal Counsel, etc.)

7 INCIDENT RESPONSE PLAN MANAGEMENT

Incident Response Plan Testing

ISS shall conduct an annual table-top test of the Information Security Incident Response Plan and is responsible for addressing any deficiencies in processes and procedures identified as a result of this testing. Two incidents, one critical and one major, will be simulated during the annual test. Testing scenarios will be defined and agreed to by the UNH Information Security Committee and should mimic tangible threat/attack vectors.

The annual test process will involve all participants necessary to respond to and recover from the specific scenario being tested. All required documentation will be produced during the test and a debriefing will be held once the exercise is complete.

The goal of the annual test is two-fold. First, to ensure the processes and procedures are adequate to guide a quick, thorough response to a real incident. Second, to provide training for incident coordinators, incident handlers, subject matter experts, and IT management on the Incident Response and Recovery processes.

With the written approval of the UNH CIO, this annual test requirement can be waived if warranted based on Incident Response activity during the previous year.

Incident Response Plan Review

As part of the annual Incident Response Plan test process, ISS will conduct a review of the Information Security Incident Response Plan and all related documentation to ensure the plan is up to date. Revisions will also be made between formal reviews when necessary changes are identified as a result of incident debrief sessions.

ISS is responsible for addressing any deficiencies in the plan and its related processes and procedures identified as a result of this testing and review process.

Incident Response Plan Approval

Annually, as part of the Incident Response Plan test and review process, the UNH CIO will review and approve any revisions made to the Incident Response Plan. Additionally, if major modifications are made to this plan outside the annual testing and review process (ex. as the result of an incident debrief finding) the revised plan will be submitted to the UNH CIO for review and approval prior to publication.

Incident Response Plan Training

Information Security Services (ISS) provides training on the Incident Response Plan process and any related, role-specific procedure and guideline documentation to aid University constituents in following the approved processes and procedures. Contact ISS for more information.

8 ROLES & RESPONSIBILITIES

Incident Responders	
Incident Response Coordinator	• Ensure that the university's response to the incident is handled according to this plan • Coordinate all Incident Response activities, chair Incident Response Team • Inform the UNH CIO and UNH ISO when an incident classified as Critical according to the Incident Classification Matrix is reported • Inform the UNH ISO when an incident classified as Major according to the Incident Classification Matrix is reported • Determine initial Incident Classification • Assemble Incident Response Team and ensure agreement on roles and responsibilities within the team • Involve subject matter experts from across UNH and USNH as needed • Monitor and coordinate Incident Handler activity • Ensure all required documentation is created and completed for each Major and Critical Incident according to this plan • Act as primary point of contact for UNH Administration, UNH IT Leadership, Incident reporter, and other stakeholders • Work with incident communications officer (ex. University Media Relations personnel) as requested. • Create Incident Summary
Incident Response Team (IRT)	• Participate in Incident Response and Recovery activities as required • Assess incident details and confirm classification per the Incident Classification Matrix • Determine on-going risks related to active incidents, recommend appropriate mitigation strategies to prevent further loss/damage • Investigate information security incidents • Identify the need for subject matter expertise • Assist in Incident Report creation as requested by Incident Coordinator • Maintain confidentiality of incident response activities

	• Participate in incident recovery activities as needed • Participate in incident debriefing •
Incident Handlers (Sys/DB/APP Admins, other resources)	• Participate in incident response and recovery activities as needed • Create incident reports when requested by Incident Coordinator • Maintain appropriate confidentiality when working on incident response and remediation activities
UNH Police Department and/or external Law Enforcement	• Escalate information security incident reports to UNH ISO • Investigate and assume responsibility for incidents that involve violation of law
UNH IT Service Desk/ATSC	• Intake of information security incidents per the procedures outlined in the *Operational Procedures for First Level Support Teams Handling Information Security Incident Reports*
Information Security Leadership	
UNH Information Security Officer (ISO)	• Ensure development and enforcement of Incident Response Plan and related process and procedure documentation • Provide overall Incident response oversight • Determination of communication/notification to CIO for incidents classified as major
UNH CIO	• Provide overall guidance as necessary for incidents classified as Critical and Major involving UNH resources and/or services provided by UNH • Serve as contact to senior University administration • Approval of the Information Security Incident Response Plan • Determination of and guidance on communication/notification to UNH executive leadership
UNH Information Security Compliance Program Manager (ISCPM)	• Act as primary Incident Coordinator for Critical and Major incidents • Provide training on Incident Response Plan and related processes and procedures • Development and maintenance of the Information Security Incident Response Plan and related process and procedure documentation
UNH Information Security Committee (UNH-ISC)	• Oversight, review, and initial approval of the Information Security Incident Response Plan • Serve on the incident response team as necessary • Review actual incident documentation to:

	○ identify corrective actions to be taken to avoid similar breaches in the future ○ identify improvements to the incident response process as may be desirable • Review and initial approval of all modifications to the Incident Response Plan • Define and approve scenarios for annual Incident Response Plan testing
UNH Administration	• Provide general oversight to incident response as needed • Set response priorities to conform to University goals and standards • Ensure appropriate resources are provided to respond to incidents as may be required
Subject Matter Experts	
USNH Legal Counsel	• Provide general legal guidance • Provide specific guidance to a specific incident (ex. reporting requirements) •
UNH Communications and Public Affairs (CPA)	• Communication with involved individuals, the public and the news media • Communication with the UNH community as may be required
UNH HIPAA Compliance Officer	• Provide guidance on any information security incident involving protected health information
UNH Procurement	• Provide guidance on information security incidents involved contracted vendors
Data Stewards	• Provide relevant information on incident handing requirements and responsibilities for incidents involving regulated data within their subject matter area
Human Resources	• Handle or assist in handling personnel issues related to information security incidents
Technology Resources	
Academic Technology Liaisons and Information Technology Contacts	• Serve as an informed first responder in cases that involve technology and/or clients for which the Liaison or Contact is responsible

	• Inform the client about appropriate reporting procedures and post-incident report activities • Work with ISS to execute the UNH Information Security Response Plan as appropriate
Service Owners (ex. Banner, email, etc.)	• Provide the personnel resources necessary to conduct timely incident response and recovery activities • Understand contractual responsibilities for any vendor-hosted systems in relation to Incident reporting, response, and recovery • Act as vendor liaison for incidents involving vendor-hosted systems within their control
Other USNH Institutions	• Collaborate with investigations and protecting information in shared systems as necessary • When possible, assist as partners and colleagues in investigations and protecting information in local/institutional systems as requested • Notify other institutions of incidents of all classifications that may have implications across institutions (ex. Compromised credentials) •
Third-party Service Providers	• Provide services in a manner that is consistent with university policies • Immediately reporting of information security incidents including potential security breaches involving UNH data
UNH Community Members	
Managers and Supervisors	• Make available appropriate staff and resources to enable an effective incident response • Maintain sufficient awareness and train employees to ensure prompt reporting of incidents • Report incidents immediately per the process outlined in this plan
Information System Users	• Be aware of information security policies and procedures • Report incidents immediately per the process outlined in this plan

9 DEFINITIONS

Availability: Protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Incident: Unauthorized access to University information systems or information which can include a breach, data theft, injection of malicious code, accidental or malicious disclosure or display of protected information. Includes violation or lack of compliance with the policies, procedures or principles in this document.

Integrity: Protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).

Unauthorized Access: Access or attempted access by known or unknown persons, and/or automated processes in order to view, modify, or copy University information systems or information.

Protected Information: Also see USNH Data Classification Policy. Information that requires protection from unauthorized access, viewing, and/or modification, including but not limited to Social Security Numbers, Credit Card Numbers, Health Care Data, Passwords, Financial information, Account information that would enable access, and other information that is considered confidential by the University or must be protected according to policy or legal mandate. May include information that is visible to the public, but is protected from unauthorized changes. Includes Restricted, Sensitive and Public information as defined by the USNH Data Classification Policy.

10 RELATED POLICIES, STANDARDS, PROCEDURES, AND GUIDELINES

- UNH Information Security Policy (in development)
- UNH Information Security Incident Response Standard (In Development)
- Guidelines for Incident Reporters (In development)
- Operational Procedures for First Level Support Teams Handling Information Security Incident Reports (In development)
- Operational Procedures for Incident Handlers (In development)
- Operational Procedures for Incident Response Team Participants (In development)

CONTACT INFORMATION

SUBJECT	CONTACT	EMAIL/URL
Policy Questions Report a Violation Request for Information	UNH Information Security Services (ISS)	It.security@unh.edu https://itsupport.unh.edu/itsec/

DOCUMENT HISTORY

Effective Date:	30 AUG 2017
Approved by:	5th Revision, • S. WADDELL, CIO, 30 AUG 2017 • B. GAON, ISO, 22 August 2017 • UNH-ISC, 17 August 2017
Reviewed by:	5th Revision • S. WADDELL, CIO, August 2017 • B. GAON, ISO, August 2017 • UNH-ISC, August 2017
Revision History:	5th Revision, audit response, R. BOYCE, UNH IT Security Committee May - August 2017
	4th Revision, complete update, Nino Coletti, UNH ISCO and UNH IT Security Committee, 2015
	3rd Revision, Cybertrust Training, Petr Brym, Training Attendees, 21 JUN 2011
	2nd Revision of Original Draft, Petr Brym, IT Security Committee, 07 JUN 2011
	ESI Incident Clarifications, Petr Brym, USNH Legal Counsel, 22 FEB 2010
	Original Draft, Petr Brym, 12 MAY 2008