ADMINISTRATIVE PROCEDURE

Incident Response Plan

PURPOSE

This document establishes the procedures for identifying, reporting, and responding to an information security incident. 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.

DEFINITION AND SCOPE

Information security incidents are events that have the potential to compromise the confidentiality, integrity, or availability of Nevada State University (NS) information and/or information technology resources.

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

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

Examples of information security incidents:

- Computer account(s) accessed by an unauthorized person
- Compromise of credentials from a malware infection, phishing attack, or improper disclosure of password(s) to an unauthorized person
- Device(s) infected with ransomware
- Disclosure of protected institutional data to unauthorized individuals
- Unauthorized access to, alteration of, or activity within institutional information systems (unauthorized code changes, compromised/defaced website, etc.)
- Physical breach (ex. unauthorized access to secure IT facilities)
- Theft or loss of a device (ex. computer, laptop, tablet, or smartphone)
- Denial of service attack
- Notification of publicly posted NS credentials
- Notification from a cloud-computing vendor of a breach involving institutional data

If it is not clear whether a specific situation constitutes an information security incident, report it per the “Reporting an Incident” section and Information & Technology Services (ITS) will make the determination.

PROCEDURES

Reporting an Incident

It is the responsibility of all NS users to report any incident that might compromise information security to Information & Technology Services. This includes incidents taking place on or off campus as well as on personal devices used to access NS systems. Incidents reported to NS personnel by vendors must also be reported using this process.

1.) Contact the NS Support Center (help desk) at (702) 992-2400 (option 3) or by e-mailing support@nevadastate.edu

2.) Inform the help desk that you are reporting an information security incident and provide the following information:
   a. What the incident pertains to
   b. Where the incident occurred
   c. When the incident occurred
   d. Who might be involved
   e. Contact information

3.) A member of Information & Technology Services may contact you to request additional details about the incident

Incident Response

Step 1: Assign Incident Response Coordinator
The Chief Information Officer (CIO) assigns an Incident Response Coordinator (IRC) who will be the primary point of contact for the duration of the response and recovery effort. The IRC's name and contact information will be provided to all relevant parties.

With incidents involving NS data stored, accessed, managed, or otherwise used by a 3rd party vendor, the Incident Response Coordinator shall notify contracts and/or 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, NS 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 2: Assess Incident Risk and Assign Classification
The Incident Response Coordinator, in conjunction with any other appropriate personnel, reviews the known details of the incident and determines the incident's initial risk classification according to the Incident Response Classification Matrix.

Step 3: Assemble the Incident Response Team
The Incident Response 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 Incident Response Coordinator will consult with legal counsel, cyber insurance provider, campus police, leadership/administration, individual university administrators, public relations, and other departments or groups to establish an Incident Response Team appropriate to respond to the specific incident.

Step 4: Mitigate the Potential for Additional Loss/Damage
The Incident Response Team 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 the following:

- 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;
- 24×7 guard may need to be provided for physical access control; and/or
- Network access may need to be blocked or restricted to prevent additional intrusion or the spread of malware.

With approval by the CIO, 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.

Step 5: Investigate the Incident
If the Incident Response Team determines the incident is not an active incident or, once steps have been taken to prevent further loss/damage or to mitigate the impact of the incident, the IRT will perform a thorough investigation of 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; and
- 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, that it is necessary to involve other 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:
    - IT Resources – to assist in investigation activities related to specific systems, databases, devices, and/or networks
    - Non-IT Resources – to assist in investigation activities related to systems, infrastructure, and devices managed and administered outside of IT

- Subject Matter Experts:
    - Public Relations – to provide guidance on and assistance with notifications to the community and other entities, to handle any contact with the press
    - Legal Counsel – to provide legal guidance and support
    - Procurement – to advise on and assist with incidents involving contracted vendors
    - Data Stewards – to advise on and assist with incidents involving restricted or sensitive data loss/exposure

In the event the IRT's investigation uncovers criminal activity, the Incident Response Coordinator or the CIO will notify law enforcement 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. These activities will vary depending on the type and scale of the incident and may include:

- Patching vulnerabilities in the impacted infrastructure and identifying similar components that might share the same vulnerability;
- Securing the accounts of compromised users;
- Rolling back to pre-compromised 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; and/or
- 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 these resources is required for remediation, the Incident Response Coordinator will monitor and coordinate these resources and the activities they need to perform.

Incident Documentation

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

- Incidents classified as Critical or Major require a completed Incident Report and a tracking ticket
- Incidents classified as Minor are documented in a tracking ticket
- 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. The Incident Response Coordinator is accountable for incident report completion and the CIO 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. Each Incident Report shall contain the following:

- A description of the incident;
- Date and time of activities as they happen;
- 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; and
- Remediation plan information

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 the Office of Information & Technology Services. 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; and/or
- Identification of information security training opportunities

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

Incident Communication and Notification Processes

The Incident Response 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 critical and major are communicated to the CIO immediately upon IRT confirmation of the Incident's classification. The CIO will determine if communication/notification to NS Executive Leadership is appropriate.

When required, Public Relations will be engaged to manage any communications/contact with the public, media, external agencies, etc. Public Relations will also be consulted in the event there is the need for an institution-wide communication.

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

CONTACTS

SUBJECT	CONTACT	PHONE	EMAIL
Primary Contact(s)	Brian Chongtai	702-992-2410	brian.chongtai@nevadastate.edu

DEFINITIONS

Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

RELATED INFORMATION

HISTORY

Revised 9/8/23