Procedure Title: Information Technology Security Incident Response

Impact: Employees, Students, Affiliates

Responsibility: Chief Information Officer

Effective Date: 3/28/2018

Revised Date:

Reviewed Date:

Relates to Policy(s): 3.08.04

Legal Citation(s):

This procedure outlines the workflow, roles, responsibilities, and escalation process for identifying and handling Information Technology (IT) security incidents at North Idaho College (NIC). Timely communication and an accurate, complete and consistent response are essential to ensure the protection of NIC IT resources and compliance with applicable policies and laws.

I. Roles and Responsibilities

A. Users

All users are responsible for immediately reporting a suspected theft, unauthorized access or any other event that may adversely affect the security of NIC data or systems to the NIC Helpdesk, Chief Information Officer (CIO), or an IT director. All users are responsible for cooperating with NIC officials or Incident Response Teams during an investigation. Incident Response Operational Team.

The Incident Response Operational Team is responsible for initially investigating security incidents at NIC. If restricted information is involved, the investigation must include examining, classifying, documenting, and escalating the event to the Incident Response Management Team. Membership will vary depending on the nature of the incident, but at a minimum will include a member of the affected department, a data custodian for the data involved, and a senior IT staff member.

B. Incident Response Management Team

The Incident Response Management Team is responsible for management decisions related to security incidents classified as critical or high, or involve restricted data or systems. Membership will vary depending on the nature of the incident but at a minimum will include members of the affected department, the data steward for the data involved, the CIO, an appropriate member of the president's cabinet, and the president. Legal counsel will be included at the discretion of the president and the CIO.

C. IT technical staff

The IT technical staff is responsible for the day-to-day monitoring of systems, vulnerability assessment, software patching, and documentation of systems. IT staff will be assigned to participate in or support either the Incident Response Operational Team or the Incident Response Management Team, as appropriate.

II. IT Security Incident Classification

When a potential IT security incident is reported to the NIC Helpdesk or IT department, the Incident Response Operational Team will analyze the situation and confirm whether it qualifies as an IT security incident. If it is determined that an incident occurred, the team will classify the severity of the incident as Critical, High, Medium, or Low.

Any incident classified as Critical or High will be referred to the Incident Response Management Team.

Classification Levels:

A. Critical: Any IT security event that causes a loss of IT services to all users or involves restricted data.

B. High: Any IT security event that causes a loss of IT services to a subset of users or involves sensitive data.

C. Medium: Any IT security event that has a minimal effect on IT services and involves sensitive data.

D. Low: Any IT security event that only affects a single user and involves public data.

III. Investigation and Remediation

Once an incident has been identified and classified, the Incident Response Operational Team will work with appropriate personnel to isolate the affected equipment to prevent secondary threats, attacks on other internal systems, and potential legal liability.

Depending on the nature of the incident, the Incident Response Management Team may be required to work with law enforcement. If served with a warrant or subpoena for information related to security incidents, the Incident Response Management Team will consult with NIC legal counsel to ensure compliance with federal and state regulations and applicable policies and practices.

NIC IT and the Information Technology Policy and Planning Council (ITPPC) will maintain guidelines and standards based on industry best practices for handling IT security incident responses.

IV. Notification

Some incidents require notification to affected parties or individuals to comply with contractual commitments or applicable laws and regulations. Notification may not be required for incidents in which NIC Incident Response Management Team can reasonably conclude that disclosure or misuse of the compromised information is unlikely.

The NIC IT Department will comply with federal and state requirements to notify any individual whose unencrypted personal information has been or reasonably believed to have been accessed by an unauthorized person. Communication with the media or the public regarding a security incident must be coordinated through NIC's Communications and Governmental Relations Department.

V. Documentation

The Incident Response Operational Team will create and maintain a record of each incident until the incident is resolved.

Individuals involved in any investigation or corrective measures are responsible for documenting their actions, communications, and findings related to the incident. This information must be submitted to the NIC Helpdesk so it can be incorporated into the record.

VI. Lost or Stolen Computing Device

If a computing device, including departmental computers, personal computers, USB drives, cell phones, or any device that may contain restricted or sensitive NIC data, is lost or stolen:

A. Contact the NIC Security Office,

B. Contact the NIC Helpdesk,

C. Change your NIC passwords, and

D. Notify the appropriate manager or director of your department.

VII. Enforcement

Regarding employees and other affiliates, the consequences of policy violation will be commensurate with the severity and frequency of the offense and may include termination of employment or contract.
Regarding students, the consequences of policy violations will be commensurate with the severity and frequency of the offense and may include suspension or expulsion.

Violations of this policy will be addressed in accordance with appropriate NIC policies and procedures, as issued and enforced by the appropriate authorities.
Violations of any local, state, or federal law will be reported to law enforcement.
Consequences of policy violation may include, but are not necessarily limited to, the following:

A. Notification: alerting a user to what appears to be an inadvertent violation of this policy in order to educate the user to avoid subsequent violations.
B. Warning: alerting a user to the violation, with the understanding that any additional violation

will result in a greater penalty.

C. Loss of computer and/or network privileges: limitation or removal of computer and/or network privileges, either permanently or for a specified period of time.
D. Penalties: if applicable, the violator may be subject to criminal or civil penalties.

VIII. Appeal

For employees, appeal of actions taken which result in an unresolved dispute will be handled via the Grievance Policy and Procedure. For students, all provisions of the Student Code of Conduct shall apply.

IX. Maintenance

This procedure will be reviewed by NIC's Chief Information Officer (CIO), IT Department, and the ITPPC every three years or as deemed appropriate based on changes in technology or regulatory requirements.

X. Exceptions

Exceptions to this procedure must be approved by the NIC IT Department and formally documented under the guidance of the CIO, and President's Cabinet.