ADMINISTRATIVE POLICY

Incident Reporting and Response

POLICY STATEMENT

Users of technology devices connected to the Nevada State College network must report all information security incidents promptly and to the appropriate party. Information & Technology Services (ITS) has the responsibility to evaluate incidents for potential of a breach of security and, when necessary, initiate a response.

REASON FOR POLICY

This policy defines the requirements for reporting and responding to incidents related to Nevada State College information systems and security.

PROCEDURES

Reporting Information Security Events

Incident Reporting - All suspected information security incidents must be reported as quickly as possible to Information & Technology Services. This includes, but is not limited to, questionable usage of files, databases, or communications networks, unauthorized loss of, or changes to computerized production data, or unusual requests for Nevada State College information coming from an external party.

Violation and Problem Reporting Protection - Nevada State College will protect workers who report in good faith what they believe to be a violation of laws or regulations, or conditions that could jeopardize the health or safety of other workers. This means that such workers will not be terminated, threatened, or discriminated against because they report what they perceive to be a wrongdoing or dangerous situation.

Requests to Cooperate in Investigations - Nevada State College workers must immediately report every request to participate in an information security investigation to the Chief Legal Counsel. Any sort of cooperation with the requesting party is prohibited until such time that the Chief Legal Counsel has determined that the participation is legal, is unlikely to cause problems for Nevada State College, and is requested by an authorized party.

Reporting Sensitive Information Disclosures - Unintended disclosures of sensitive Nevada State College information are serious matters, and they must all be immediately reported to Information & Technology Services. Such reporting must take place whenever such a disclosure is known to have taken place, or whenever there is a reasonable basis to believe that such a disclosure has taken place.

Reporting a Suspected Virus - Computer viruses can spread quickly and need to be eradicated as soon as possible to limit serious damage to computers and data. Accordingly, any suspected virus should be reported immediately to Information & Technology Services.

Reporting Unexpected Requests for Log-In Information - Other than the regular and expected Nevada State College log-in screens, users must be suspicious of all pop-up windows, web sites, instant messages, and other requests for a Nevada State College user ID and password. Users encountering these requests must refrain from providing their Nevada State College user ID and password, as well as promptly report the circumstances to Information & Technology Services.

Reporting Computer or Access Credential Loss - Employees must promptly report to their manager as well as Information & Technology Services any loss or theft of computer hardware, ID cards, or keys that contain or provide access to Nevada State College data, systems, or facilities.

Response to Incidents

Incident Response Availability - The Information Security Officer or their delegate must be available at all times to respond to alerts that include but are not limited to evidence of unauthorized activity, detection of unauthorized access, critical intrusion alerts, virus outbreaks, and reports of unauthorized critical system or content file changes.

Computer Crime Investigation - Whenever evidence clearly shows that Nevada State College has been victimized by a computer or communications crime, a thorough investigation must be performed. This investigation must provide sufficient information so that management can take steps to ensure that (1) such incidents will not be likely to take place again, and (2) effective security measures have been established.

Computer Crime or Abuse Evidence - To provide evidence for investigation, prosecution, and disciplinary actions, certain information must be immediately captured whenever a computer crime or abuse is suspected. The relevant information must then be securely stored off-line until official custody is given to another authorized person or the chief legal counsel determines that Nevada State College will no longer need the information.

Sensitive Information Disclosures - Whenever a disclosure is reported, the party which disclosed the information along with Information & Technology Services will make every effort to ensure that the information is no longer exposed and determine the extent of disclosure. NSC must then notify those impacted and provide a detailed explanation of any breach of private customer data.

Suspected System Intrusions or Virus Infections - Whenever a system is suspected of compromise, the involved computer must be immediately removed from all networks and procedures followed to ensure that the system is free of compromise before reconnecting it to the network.

Disclosures of Log-In Information - If login credentials are accidentally disclosed, users are required to change their passwords immediately. Information & Technology Services will then assist to ensure that disclosed credentials were not used to access systems.

Computer or Access Credential Loss - Whenever the loss of a computer or access control credential is reported, Information & Technology Services and the Office of Facilities Management & Planning will immediately disable the ability for these devices to authenticate or provide access to Nevada State College data, systems, or facilities.

CONTACTS

SUBJECT	CONTACT	PHONE	EMAIL
Primary Contact(s)	Brian Chongtai	702-992-2410	brian.chongtai@nsc.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 3/19/18