Title: **Cyber Incident Response Policy**	**Policy Category:** **Risk Management & Security**
Issuing Authority: **Enterprise Risk Management**	**Responsibility:** **Information Security Program Council**
Publication Date: **11/18/2022**	**Next Review Date:** **11/18/2025**

Policy Statement/Background:

This policy governs Stony Brook University (SBU) detection, response, documentation, and reporting of incidents affecting information resources. It also establishes an Incident Response Team and the requirements for identifying, reporting, investigating, classifying, documenting and communicating incident details and responder procedures.

Scope

This policy applies to all individuals who manage, are responsible for or have access to SBU information resources.

Policy:

In order to achieve this policy's objectives, the University's Information Security Program Council (ISPC) shall ensure:

- Procedures and processes are in place to identify and respond to suspected or known incidents. Such procedures and processes should: mitigate incidents to the extent practicable, measure harmful effects of known incidents, document incidents and their outcomes, include the collection of evidence, and provide appropriate reporting about incidents management.
- Incident response plans are in place. Such plans will include examples of security incidents and the appropriate responses.

- An Incident Response Team is assembled to receive notice of events of interest (EOI) and incidents and to manage the process of investigating, responding to, and reporting of an incident.
- Incident Response Team members understand their roles and responsibilities.

Establishment of an Incident Response Team

The ISPC, sensitive system workers and sensitive information workers are responsible for incident detection and remediation of information resources. The CISO or designee and other ISPC members will consult key representatives of Stony Brook University (SBU) IT, Human Resources, Office of General Counsel, Enterprise Risk Management, or other departments as warranted to establish an Incident Response Team appropriate to respond to a specific incident.

As necessary, staff shall be assigned to manage specific security incidents:

- **Initial Investigations.** An Incident Response Plan (Plan) shall provide a quick and orderly response to incidents. The Plan will identify steps to be followed for the initial reporting of EOI and subsequent investigations. Where appropriate, staff should be available to handle incidents reported outside of standard business hours.
- **High Impact Decisions**. An Incident Management Advisory Board (Advisory Board) comprised of senior leaders will make select decisions throughout an incident.
- **Pursue or Protect.** The Advisory Board will decide if an incident response calls for pursuit (watch and learn) instead of protect (containment). Until the Advisory Board makes a clear decision, the default response will always be to protect and steps to contain any potential damage will be taken as soon as possible.
- **Documentation and Communications.** The initial investigations staff will inform the CISO or designee of the incident and the preliminary risk classification. The CISO shall follow the guidelines identified in the Documentation and Communication of Incidents section of this policy.
- **Responder Procedures.** Appropriate procedures and staff shall be identified to address the specific incident. Responders will attempt to identify as much information about the event to limit additional adverse effects. Responders and appropriate staff will follow procedures where appropriate or recommend to the CISO or designee appropriate actions to be taken.

- **Incident Reporting.** Management will be informed on the status of ongoing incidents. A post incident report shall be created.

Identifying and Reporting Incidents

The Incident Response Team shall work with SBU departments to establish proactive monitoring systems that can identify potential incidents. In addition, any SBU community member may refer an EOI or concern to the Incident Response Team or designee. A triage team comprised of a subset of Incident Response Team members will determine if the reported event should be classified as an incident as outlined in a Plan.

Once an EOI has been classified as a high severity incident, the Incident Response Team will log and track incidents and take steps to investigate, escalate, remediate, refer to others, or otherwise address as outlined in this policy and the Plan.

In addition to reporting incidents, community members should report to the appropriate management any suspected weaknesses or deficiencies in information resources.

Incident Classification

Confirmed incidents are assigned to one or more of the classifications as defined by the vocabulary for event recording and incident sharing (VERIS), such as Malware, Hacking, Social, Misuse, Physical, Error or Environmental.

Documentation and Communication of Incidents

The ISPC will ensure that incidents are appropriately logged and archived. Incident reporting will be provided by the CISO or designee to senior leadership and the ISPC.

The CISO or designee and Incident Response Team representatives are responsible for communicating incident details to appropriate personnel and maintaining contact, for the purpose of update and instruction, for the duration of the incident.

Responder Procedures

The CISO or designee shall maintain standard responder procedures throughout the response and investigation of each incident, as well as securing the custody of any evidence obtained during the investigation. The classification described above as well as an Incident Response Plan shall set forth the procedures that should be followed. Staff shall refer to the Incident Response Plan for specific information on how to manage and respond to incidents.

Special Situations and Exceptions

By using mobile devices within the SBU network for business purposes, staff are subject to SBU policies restricting their use. Any mobile devices, including those that are personally owned, such as phones, wireless devices or other electronic transmitters, may be subject to examination by SBU staff in the event of an incident.

In the event a follow-up action concerning a person or organization after an information security incident requires legal action, proper forensic procedures including chain of custody shall be required for collection, retention, and presentation of evidence to support potential legal action subject to the relevant jurisdiction.

Cloud computing agreements shall be put in place to ensure privacy and tenant breach formal notification upon the compromise of SBU system(s) or data.

Over time, the CISO and ISPC shall identify and document how to address special situations and exceptions as needed.

Breach of Sensitive Information

Where sensitive data is involved, the breach will be reported according to all mandates applicable to the category of sensitive data involved.

Incident Reporting

The CISO shall provide appropriate reporting to senior leadership and identified management. Such reporting may include, but is not limited to; updates to inform management of relevant details, risks, current status and progress, tasks to be completed, and expected outcomes and dates.

Post incident reporting shall include appropriate details, mitigation actions and timeframes, and lessons learned.

In addition to reporting of specific incidents, the ISPC shall provide annual reporting to University Senior Leadership summarizing incidents reported and actions taken. The annual report may identify numbers and types of incidents, impact, costs incurred, lessons learned, and other relevant factors.

Incident reports and supporting documents shall be retained in accordance with New York State (NYS) and SUNY data retention policies.

Criminal Prosecution

SBU retains the right to prosecute for any and all cybercrime. In the event that an individual complainant is needed for prosecution, the highest ranking official responsible in the affected area or the VP of IT shall act as such. The Advisory Board will be consulted throughout an incident and assist in the investigation as needed for criminal prosecutions or University administrative proceedings.

Enforcement

Any substantiated act(s) by an employee that violates this policy may result in sanctions or other disciplinary action as covered by labor management processes, collective bargaining agreements, and/or applicable University policies.

Definitions:[1]

Event of Interest (EOI): potential incident that warrants further investigation.

Incident: adverse event or significant threat of such in an information system, network or resource.

Management: individuals within the organization that have supervisory responsibilities.

[1] Additional definitions are listed in the Information Security Program Administration Policy.

Contact:

Additional information about this policy is available here:

Enterprise Risk Management
180 Administration Building
Stony Brook, NY 11794
(631) 632-9500

Information Security Program Council (ISPC)
ISPC@stonybrook.edu

Relevant Standards, Codes, Rules, Regulations, Statutes and Policies:

- New York State Breach Notification Law
- Information Security Program Administration Policy
- Records Retention and Disposition Policy
- SUNY Policy 6900: Information Security
- VERIS Incident Vocabulary
- Stony Brook Cybersecurity Incident Reporting and Planning