COLUMBUS STATE UNIVERSITY
Information Security
Incident Management Response Plan
(3/7/2016)

Authority This information security incident response plan was approved by the Chief Information Officer (CIO).

Summary This Memo describes the procedures to be followed when a computer system, network or breach of security involving personally identifiable information (PII), regardless of its medium (e.g., paper, electronic, verbal) incident is discovered to have occurred involving an Academic or Administrative Department and\or Computing System operated by Columbus State University (CSU) involving students, faculty, and staff. This policy outlines the procedures for decision-making regarding emergency actions taken for the protection of CSU's information resources from accidental or intentional unauthorized access, disclosure or damage.

Applicability This policy is applicable to all CSU students, faculty, staff, partners and guests granted use of CSU resources ("CSU community") who become aware of an information security incident concerning an Academic or Administrative Department and\or Computing System. Every user of any of CSU's information resources has responsibility toward the protection of CSU's information assets.

Those reporting or responding to an incident will follow the Information Security Incident Response Procedures and relevant sections of the Columbus State University Emergency Management Plan. All individuals involved in reporting or investigating an information security event are obliged to maintain confidentiality, unless the Chief Information Security Officer (CISO), Chief Information Officer (CIO) or cognizant University Officer authorizes information disclosure in advance.

The Chief Information Security Officer (CISO) or designee will direct any action deemed necessary to facilitate incident response. CSU reserves the right to take any action necessary to protect CSU resources or preserve evidence.

Section headings are:

COLUMBUS STATE UNIVERSITY
Information Security
Incident Management Response Plan
(3/7/2016)

1. PURPOSE

The purpose of the information security incident response plan is to mitigate the effects caused by such an incident and to protect the information resources of CSU from future unauthorized access, use or damage. CSU recognizes the need to follow established procedures to address situations that may indicate that the security of CSU's information assets may have been compromised. Such procedures include ensuring that the appropriate level of CSU management becomes involved in the determination of actions implemented in response to an information security incident. A standard, university-wide approach to information security events is important because of the following factors:

- The need to promptly and effectively address any improper access of CSU information systems or the data contained therein
- Legal and regulatory requirements regarding the safeguarding of CSU information assets
- CSU's implementation and reliance on university-wide systems and applications which impact the entire campus
- Intellectual capital that CSU both produces and owns needs to be protected against premature disclosure or unauthorized tampering
- Damage to CSU's reputation as a world-class institution can have both direct and indirect negative effects
- A general worldwide increase in the number and severity of information security incidents
- The need to protect the privacy of persons whose information is stored on CSU information systems.

2. DEFINITIONS

Information Security Incident — An information security incident is defined as any real or suspected adverse event in relation to the security of computer systems, computer networks and breaches of security involving personally identifiable information (PII), regardless of its medium (e.g., paper, electronic, verbal). Examples of incidents include activities such as:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- The unauthorized use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
- Events that extend beyond the borders of the local hardware or software system, and pose a threat of an adverse impact on CSU's reputation, financial position, information systems security posture, or health and safety of faculty, staff and students.

A breach of personally identifiable information (PII) would expose individuals to possible financial/identity theft, risks, and concerns.

Administrative and/or Academic Computing System — Any application, or information system, that directly or indirectly deals with or supports CSU's primary mission of teaching, learning and research.

3. NOTIFICATION (Incident Discovery)

A member of the university community who becomes aware of an information security incident involving an Academic or Administrative Computing System should immediately:
• Contact the UITS Help Desk 706-507-8199 or (helpdesk@columbusstate.edu) and/or
• Contact CSU's Chief Information Security Officer (CISO) at 706-507-8137 or (spivey_dee@columbusstate.edu)
The university's Chief Information Security Officer may convene a preliminary fact-finding working group comprised of cognizant business and technical personnel and, where appropriate (such as instances where legal requirements are implicated, e.g., where private data of individuals is compromised), will communicate the incident to the Chief Information Officer, Emergency Management Team's (EMT) University Incident Commander (or designatee(s)).

4. INFORMATION SECURITY INCIDENT RESPONSE TEAM (ISIRT)

When warranted by information obtained during preliminary fact-finding of an incident, the Chief Information Security Officer (CISO) will promptly appoint and convene a meeting of an ad hoc Information Security Incident Response Team (ISIRT). Depending on the circumstances of each situation, the Chief Information Security Officer shall also include the Emergency Management Team

The ad hoc ISIRT Team consists of:
• Chief Information Officer
• Executive Director IT Services and/or IT Services Staff
• Executive Director Operations and Infrastructure Services and/or Operations and Infrastructure Staff

The Emergency Management Team may consist of:
• University Incident Commander
• Assistant Incident Commander
• Plant Operations Representative
• Human Resources Representative
• Student Affairs Representative
• Public Information Representative
• Environmental Health and Safety Representative
• Homeland Security Representative
• Academic Affairs Representative
• Information Technology Representative

Emergency Management Plan url:
https://police.columbusstate.edu/docs/emp.pdf

5. ESCALATION OF DECISION-MAKING

The ISIRT will plan and coordinate the activities performed during the incident, keeping other concerned offices including the University Systems of Georgia Board of Regents (USG/BOR) advised as necessary.
http://www.usg.edu/infosec/incident_management/incident_report_faq/
In carrying out this responsibility, the ISIRT will ensure that important operational decisions are elevated to the appropriate levels to protect the fundamental interests of CSU and others impacted by the incident. Such decisions include, but are not limited to:
• Restricting information system access or operations to protect against unauthorized information disclosures
• Reporting and/or publicizing unauthorized information disclosures, as required by law
• Involving law enforcement agencies in cases where applicable statutes appear to have been violated
The Chief Information Security Officer will also be responsible for documenting the deliberations and decisions of the ISIRT as well as all actions taken pursuant to ISIRT deliberations.

6. PROCEDURES & FLOWCHART

All information security incidents occurring at CSU are classified into one of the following categories:

Impact Classification	Impact Rank	Impact Description
Functional Impact	**4**	**HIGH** – UITS has lost the ability to provide all critical services to all system users.
	3	**MEDIUM** – UITS has lost the ability to provide a critical service to a subset of system users.
	2	**LOW** – UITS has experienced a loss of efficiency, but can still provide all critical services to all users with minimal effect on performance.
	1	**NONE** – UITS has experienced no loss in ability to provide all services to all users.

Impact Classification	Impact Rank	Impact Description
Information Impact	**3**	**PRIVACY** - The confidentiality of CSU students/faculty/staff personally identifiable information (PII), health information, financial information, intellectual property and/or any CSU protected critical infrastructure information was compromised and exposed.
	2	**INTEGRITY** - The necessary integrity of CSU students/faculty/staff personally identifiable information (PII), health information, financial information, intellectual property and/or any CSU protected critical infrastructure information was modified or system/application access obtained without authorization.
	1	**NONE** - No CSU students/faculty/staff personally identifiable information (PII), health information, financial information, intellectual property and/or any CSU protected critical infrastructure information was modified, deleted, or otherwise compromised and exposed

Impact Classification	Impact Rank	Impact Description
Recoverability	**4**	**NOT RECOVERABLE** – Recovery from the incident is not possible (e.g., CSU (PII) information compromised and exposed).
	3	**EXTENDED** – Time to recovery is unpredictable and outside resources are needed.
	2	**REGULAR** – Time to recovery is predictable with existing resources.
	1	**NOT APPLICABLE –** Incident does not require recovery.

Impact Risk Classification	Impact Risk Rank (From total by adding Impact ranks above)	Impact Risk Notification Result
HIGH LEVEL (Tier 3)	**9 - 11**	External & Internal UITS Communication
MEDIUM LEVEL (Tier 2)	**6 - 8**	External & Internal UITS Communications
LOW LEVEL (Tier 1)	**3 - 5**	Internal UITS Only Communication

High severity incidents include any incident that is known or suspected to meet one or more of the following criteria:

• Involves unauthorized access to, loss or theft of a device known to store, process or transmit highly sensitive and\or confidential university information and/or personally identifiable information (PII).
• Involves an enterprise security device, such as a data center firewall or authentication service etc.
• Involves compromise of a networking device, such as a router or switch.
• Security monitoring devices report an unauthorized change in the configuration of any device described in the first 3 bullet points.
• Causes the unavailability of a mission-critical service.
• Involves a significant number of university systems, indicating a widespread attack.
• In the judgment of CISO, poses a high severity risk to CSU systems or information.

If an event meets the criteria for a high severity incident any ISIRT member may take and/or direct immediate action to protect CSU systems and/or data. This includes, but is not limited to, the immediate and complete disconnection of a suspected compromised computer from university networks. If this action is necessary, the ISIRT member will notify the CISO and\or the CIO as soon as practical. In cases when necessary to support an active investigation, or to preserve evidence, the ISIRT member, CISO or CIO may also take physical possession of any computer believed to be involved in the incident.

Low severity incidents include any information security incident that does not meet the foregoing high severity criteria, but may have a negative impact on the conduct of university business.
The CISO will determine the initial incident classification when declaring the incident, subject to later reclassification.

The highest priority is to protect the campus community and any sensitive information. For all incidents, the priority of response will be:

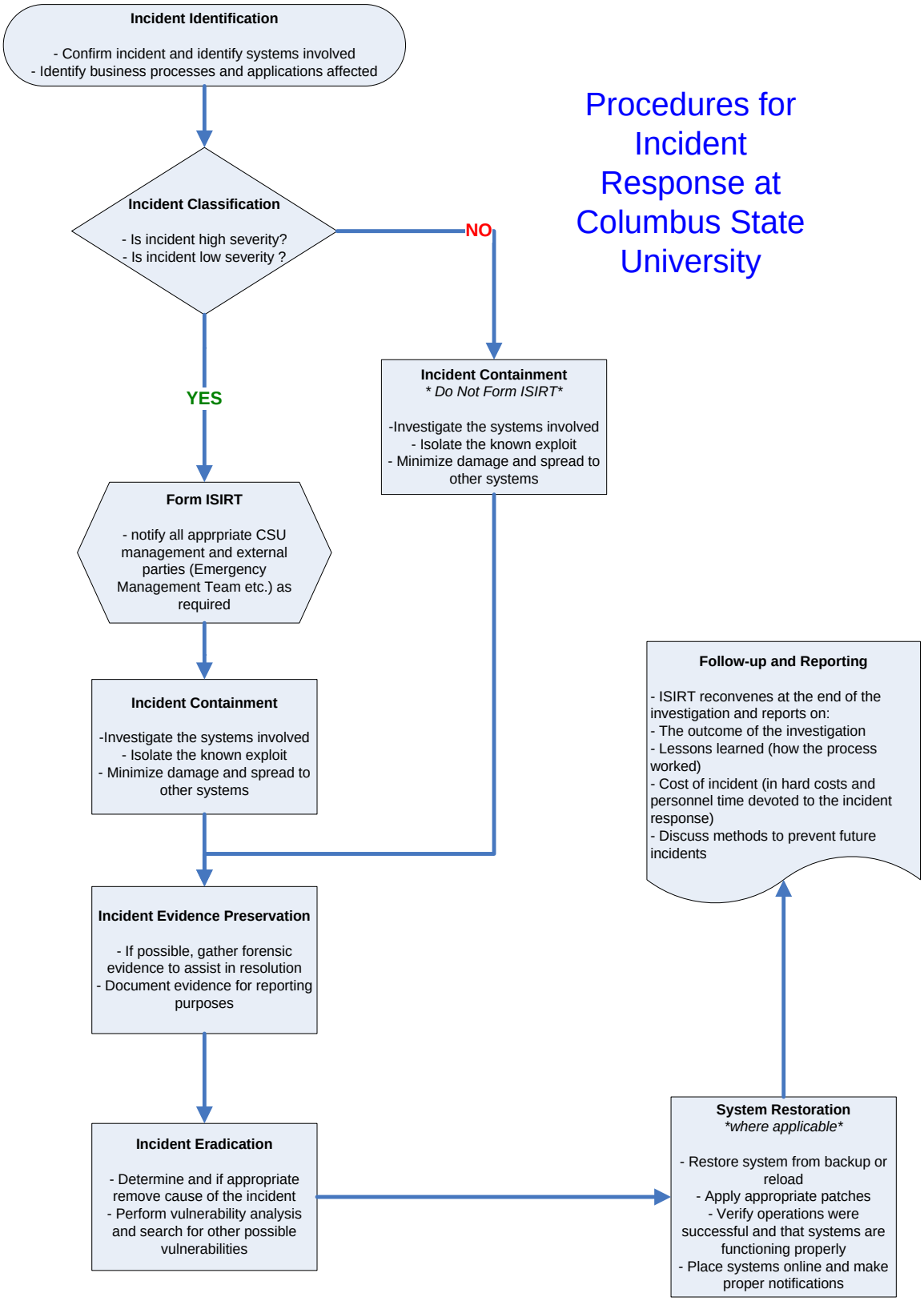
- Identify incident
- Classify incident
- Form ISIRT and notify
- Contain incident damage or spread
- Preserve incident evidence if possible
- Eradicate any damages
- Restore systems and services
- Follow-up and reporting

7. INCIDENT REPORT NOTIFICATION

Follow the steps below to send an incident report notification to CIO and/or CIO designates: (*** note: CIO designates may be UITS or external business executives***)

1. Identify functional impact (see Impact Classification table) ***required**
2. Identify information impact (see Impact Classification table) ***required**
3. Identify impact to recoverability (see Impact Classification table) ***required**
4. Identify threat vector (see Cause Analysis flowchart), if possible
5. Provide any mitigation details, if possible
6. Provide contact information and any available incident details ***required**

COLUMBUS STATE UNIVERSITY
Information Security
Incident Management Response Plan
(3/7/2016)



Procedures for Incident Response at Columbus State University

8. DOCUMENTATION

On a periodic basis, the CISO and\or designated ISIRT member will prepare a summary report of all information security incidents, and provide it to the CIO.

Upon declaration of an information security incident, the CISO and\or designated ISIRT member will prepare a summary of the relevant technical and operational details and provide it to the CIO.

If a high severity incident extends beyond 24 hours, the CISO and\or designated ISIRT member will send the CIO daily updates on the status of the incident and remediation efforts.

Within four business days of the conclusion of an incident, the CISO and\or ISIRT member will prepare an incident report and provide it to the CIO.

The University will comply with all reporting requirements imposed upon it by law or contractual obligation. The Emergency Management Team with the assistance of the ISIRT will coordinate any such action.