

Chapter Name

8.0 Security

Chapter Number Title

8.6 Information Systems Security Incident Response Policy

1.0 Purpose

This policy defines the requirements necessary to ensure security incidents are identified, contained, investigated, and remedied. It also provides a process for documentation, appropriate reporting internally and externally, and communication so that organizational learning occurs. Finally, it establishes responsibility and accountability for all steps in the process of addressing computer security incidents.

2.0 Scope

This policy applies to all Users. It applies to any computing devices owned or leased by Eastern Michigan University that experience a Computer Security Incident. It also applies to any computing device regardless of ownership, which either is used to store Confidential University Data, or which - if lost, stolen, or compromised, and based on its privileged access - could lead to the unauthorized disclosure of Confidential University Data. Examples of systems in scope include but are not limited to a User's personally owned home computer that is used to store Confidential University Data, or that contains credentials that would give access to Confidential University Data.

3.0 Policy

3.1. Overview of EMU's Incident Response Program

3.1.1. All Computer Security Incidents must be reported to Director IT, Security Administrator or the Chair of the Incident Response Team (IRT) promptly. See Section 3.2 below.

3.1.2. All Confidential Data Security Incidents must:

3.1.2.1. Be reviewed by the IRT on a per incident basis. See Section 3.3 below.

3.1.2.2. Follow appropriate incident handling procedures. See Sections 3.4 and 3.5 below.

3.1.3. IRT - under the direction of Security Administrator Director for the Division of Information Technology (DoIT) - is responsible for documenting, investigating, and reporting on security incidents. See Sections 3.6 and 3.7 below.

3.2. Identifying and Reporting Computer Security Incidents

3.2.1. *Users.* In the event that a User detects a suspected or confirmed Computer Security Incident, the User must report for issues including but not limited to viruses, worms, local attacks, denial of service attacks, or possible disclosure of Confidential University Data to it-irt-incident@list2.emich.edu.

3.2.2. *IT Administrators.* IT Administrators must notify the Chair of the IRT of all Computer Security Incidents, except for categories of incidents that DoIT Information Security may designate in an Appendix I (Section 3.8) of this policy.

3.2.3. *DoIT Information Security.* DoIT Information Security and IRT shall notify appropriate systems administrators and other personnel of all emergency and attack incidents, as well as all suspicious activity incidents when it believes that an administrator's system is at risk. The system's administrators will then work with DoIT Information Security or IRT members to properly address the incident and minimize the risk of future occurrences.

3.3. Incident Response Team

3.3.1. *Purpose.* The purpose of the Incident Response Team is to supplement EMU's information security infrastructure and minimize the threat of damage resulting from Computer Security Incidents.

3.3.2. *Per Incident Basis.* The Incident Response Team shall be fully assembled for Confidential Data Security Incidents.

3.3.3. *Membership.* See DoIT Incident Response and Management Team Charter

3.3.4. *Responsibilities.* Responsibilities of the Incident Response Team are to assess the incident and follow incident handling procedures, appropriate to the incident.

3.3.5. *Confidentiality.* During an investigation IRT members will share information about security incidents beyond the IRT, Director IT, Security Administration, CIO, and Senior Response Team only on a need-to-know basis.

3.4. Incident Handling. For incidents requiring the assembly of the Incident Response Team, the following is a list of response priorities that should be reviewed and followed. Law Enforcement shall be immediately notified of any incident in which a criminal act or purpose is suspected. The most important items are listed first:

3.4.1. *Safety and Human Issues.* If an information system involved in an incident affects human life and safety, responding to any incident involving any life-critical or safety-related system is the most important priority. Example includes a physical threat of harm to persons for confidential information. In these situations Law Enforcement should be immediately notified.

3.4.2. *Address Urgent Concerns.* The University may have urgent concerns about the availability or integrity of critical systems or data that must be addressed promptly. DoIT Information Security and IRT shall be available for consultation in such cases.

3.4.3. *Establish Scope of Incident.* The Incident Response Team shall promptly work to establish the scope of the incident and to identify the extent of systems and data affected. If it appears that personally identifiable information or Production Environment may have been compromised, the Incident Response Team shall immediately inform the Director IT, Security Administrator and Chief Information Officer (CIO). See section 3.5.

3.4.4. *Containment.* Once life-critical and safety issues have been resolved, the Incident Response Team shall identify and implement actions to be taken to reduce the potential for the spread of an incident or its consequences across additional systems and networks. Such steps may include requiring that the system be disconnected from the network.

3.4.5. *Develop Plan for Preservation of Evidence.* The Incident Response Team shall develop a plan promptly upon learning about an incident for identifying and implementing appropriate steps to preserve evidence, consistent with needs to restore availability. Preservation plans may include preserving relevant logs and screen captures. The affected system may not be rebuilt until the Incident Response Team determines that appropriate evidence has been preserved. Preservation will be addressed as quickly as possible to restore availability that is critical to maintain business operations.

3.4.6. *Investigate the Incident.* The Incident Response Team shall investigate the causes of the incident and future preventative actions. During the investigation phase, members of the incident response team will attempt to determine exactly what happened during the incident, especially the vulnerability that made the incident possible. In short, investigators will attempt to answer the following questions: Who? What? Where? When? How? Incident Response Team members will be informed of status of ongoing investigation.

3.4.7. *Incident-Specific Risk Mitigation.* The Incident Response Team shall identify and recommend strategies to mitigate risk of harm arising from the incident, including but not limited to reducing, segregating, or better protecting personal, proprietary, or mission critical data.

3.4.8. *Restore Availability.* Once the above steps have been taken, and upon authorization by the Incident Response Team, the availability of affected devices or networks may be restored.

3.4.9. *EMU-Wide Learning.* DoIT Information Security shall develop and arrange for implementation of a communications plan to spread learning from the security incident throughout EMU to individuals best able to reduce risk of recurrence of such incident.

3.5. Senior Response Team (SRT). If the CIO and Director IT, Security Administrator in their judgment believe that the incident reasonably may cause significant harm to the subjects of the data or to EMU, they may recommend to the Executive Vice President that a Senior Response Team be established. The Senior Response Team shall be comprised of senior-level officials as designated by the CIO and Executive Vice President. The Senior Response Team shall:

3.5.1. Establish whether additional executive management should be briefed and the plan for such briefing.

3.5.2. Determine - with final approval by the General Counsel - whether EMU shall make best efforts to notify individuals whose personal identifiable information may have been at risk. In making this determination, the following factors shall be considered:

- a. legal duty to notify
- b. length of compromise
- c. human involvement
- d. sensitivity of data
- e. existence of evidence that data was accessed and acquired
- f. concerns about personnel with access to the data
- g. existence of evidence that machine was compromised for reasons other than accessing and acquiring data
- h. additional factors recommended for consideration by members of the Incident Response Team or the Senior Response Team.

3.5.3. Review and approve any external communication regarding the incident.

3.6. Documentation

3.6.1. *Log of security incidents.* IRT shall maintain a log of all reportable security incidents recording the date, Colleges, Institutes, Centers affected, whether or not the affected machine was determined as Production Environment, the type of Confidential University Data affected (if any), number of

subjects (if applicable), and a summary of the reason for the intrusion, and the corrective measure taken.

3.6.2. *Critical Incident Report.* IRT shall issue a Critical Incident Report for every reportable security incident affecting machines qualifying as Production Environment, or other priority incidents in the judgment of IRT describing in detail the circumstances that led to the incident, and a plan to eliminate the risk.

3.7 IRT member and IT Administrator Best Practices

3.7.1. It is essential to consult IRT when handling Computer Security Incidents.

- a. Assigning members of the IRT: In cases where an incident involves an investigation into misconduct, the IRT Chair should consider carefully whom to assign. For example, one may not wish to assign an IT professional who works closely with the individual(s) being investigated.
- b. IRT focus should be on incident command and containment. Unless authorized by the Chair of IRT, Director, Information Security, or CIO IRT members or IT Administrators should make as few changes to a system as possible and only if changes are needed to prevent further harm. All containment actions must be documented in detail.

3.8 Appendix

Violations of the acceptable use policy or other dangers to network performance or security which meet both of the following conditions need not be reported to IRT.

- a.) contained by network engineering and/or automated systems AND,
- b.) do not result in device compromise,

Examples (within the above constraints) include:

- network scanning
- denial-of-service attempts,
- brute-force login attempts,
- quarantined/deleted malicious software,
- traffic blocked by the intrusion detection system or firewalls,
- compromised non-privileged accounts,
- unauthorized network connections,
- server or peer-to-peer software,
- violation of network configuration, flow or admission control policies, and
- network/topology maintenance.

3.9 References

PennNet *Information Systems Security Incident Response Policy* at <http://www.upenn.edu/almanac/volumes/v53/n18/or.html>

4.0 Responsibility for Implementation

The Division of Information Technology is responsible for the operation of Eastern Michigan University data networks as well as the establishment of information security policies, guidelines, and standards. DoIT has authority to develop and oversee policies and procedures regarding the privacy of personal information. DoIT

therefore has the authority and responsibility to specify security incident response requirements to protect those networks as well as University data contained on those networks.

5.0 Enforcement

5.1. Verification: The Director IT, Security Administrator or Chair of the IRT will verify any known computing security incidents as having been reported and documented as defined by this policy.

5.2. Notification: Violations of this policy will be reported by Chair of the IRT or Director IT, Security Administrator to the Senior Management of the Department affected.

5.3. Remedy: The incident will be recorded by IRT and any required action to mitigate the harmful affects of the attack will be initiated in cooperation with the Department, School, IT Administrator, or User.

5.4. Financial Implications: The owner of the system shall bear the costs associated with ensuring compliance with this policy.

5.5. Responsibility: Responsibility for compliance with this policy lies with all users.

5.6. Time Frame: All incidents involving Production Environment systems and networks must be reported immediately. All other incidents should be reported within one business day of determining something has occurred.

5.7. Enforcement: Users not adhering to the policy may be subject to sanctions as defined by University policies.

Any employee found to violate federal or state of Michigan laws, EMU policies, procedures or standards of conduct, will be subject to disciplinary action under University policy. Any suspected violation of State or Federal laws will be reported to the appropriate legal authority for investigation.

Consequences for violations (in no particular order) include, but are not limited to:

- Verbal warnings.
- Revocation of access privileges.
- Disciplinary actions up to and including discharge.
- Criminal prosecution.

Any student found to violate federal or state of Michigan laws, EMU policies, procedures or standards of conduct, will be subject to disciplinary action under EMU's Student Code of Conduct. Any suspected violation of State or Federal laws will be reported to the appropriate legal authority for investigation.

Consequences for violations (in no particular order) include, but are not limited to:

- Verbal warnings.
- Revocation of access privileges.
- Disciplinary actions up to and including permanent dismissal.
- Criminal prosecution.

If you break the law, you can be prosecuted. Even if you are not charged criminally, you can be held personally liable, and you can be suspended or dismissed from the University, or fired if you are an employee.

The University reserves the right to protect its electronic resources from threats of immediate harm. This may include activities such as disconnecting an offending computer system from the campus network, terminating a running job on a computer system, or taking other action.

6.0 Definitions	
<u>Term</u>	<u>Definition</u>
Confidential University Data	<p>Sensitive Data - institutional data for which users must be granted specific authorization to access, because the data's unauthorized disclosure, alteration, or destruction will cause perceivable damage to the institution. Non-public or Internal data is moderately sensitive in nature. Often, this data is used for making decisions and therefore it is important this information remain timely and accurate.</p> <p>Confidential Data - institutional data for which the highest levels of restriction should apply due to the risk of harm that may result from disclosure or inappropriate use (data protected by state and federal regulations such as FERPA, HIPAA & GLBA). Confidential data may have personal privacy considerations, Only those individuals designated with approved access and signed non-disclosure agreements may be granted access to this data.</p> <p>Any other data the disclosure of which could cause significant harm to EMU or its constituents.</p>
Computer Security Incident	Any event that threatens the confidentiality, integrity, or availability of University systems, applications, data, or networks. University systems include, but are not limited to: servers, desktops, laptops, workstations, PDAs, network servers/processors, or any other electronic data storage or transmission device.
Confidential Data Security Incident	A subset of Computer Security Incidents that specifically threatens the security or privacy of Confidential University Data.
FERPA	Family Educational Rights and Privacy Act, as amended.
HIPAA	Health Insurance Portability and Accountability Act, as amended.
GLBA	Gramm-Leach-Bliley Act, as amended.
User	An EMU user is any faculty, staff, consultant, contractor, student, or agent of any of the above.
IT Administrator	Any faculty, staff, consultant, contractor, student, or agent of any of the listed who manages or administers an information technology system, device, or application.

Production Environment	<p>Any machine used to store or transfer data between two machines where both machines meet the requirements below:</p> <p>1) are part of the Eastern Michigan University (EMU) Enterprise Resource and Planning System (ERP), or</p> <p>2) system(s) approved for purchase by the Enterprise Resource and Planning System Tactical Committee (ERP-TAC), or</p> <p>3) system(s) whose contract is signed by the CIO, or</p> <p>4) any hardware/software where memorandum of understanding (MOU) agreements are present between DoIT and a department/division, making a machine part of the EMU production environment.</p> <p>Exceptions to the above definition are: applications used for academic classroom projects; systems purchased for DoIT internal use; and duplicate production environments used for testing and training</p>
-------------------------------	---

7.0 Revision History			
<u>Creator</u>	<u>Description</u>	<u>Submission Date</u>	<u>Approval Date</u>
Justin Sherenco		11/29/2007	
Justin Sherenco	Reformat layout	12/17/2007	
Justin Sherenco	Changed number, grammar,	12/18/2008	
Justin Sherenco	Wording.	1/4/2007	
J. French	Several revisions	04-07-2008	
A. Barr	New IT Logo; Replace ICT with DoIT	04-21-2008	
A. Barr	Sent revisions to Policy Committee for review	04-21-2008	
A. Barr	Policy on agenda for 04-22-2008	04-21-2008	
A. Barr	Section 8 Document Progress Added	06-19-2008	
J. Sherenco	Removed critical host and replaced with "Production Environment. Added incident response e-mail. Modified 3.4 for law enforcement notification. Modified 3.4.3 for CIO notification. Changed "IT Management" to IT Administrator and added definition	6-24-08	
	3.2.1 added e-mail address. 3.4 Added law enforcement notification	7/07/2008	
A. Barr	5.3 changed IT Manager to IT Administrator	07-25-2008	
A. Barr	Definition of Confidential University Data - deleted asterisk in front of "Any other data . . ." sentence.	07-25-2008	
A. Barr	Corrected name of Division in Section 4.0; added definitions for FERPA, HIPAA, and GLBA.		
A. Barr	5.7 Enforcement – substantial additions.		
A. Barr	Spell check done	07-25-2008	
A. Barr	Revisions made as discussed in Policy Committee	07-29-2008	
J. French	Substantial re-write of Section 3.8 Appendix	07-29-2008	
J. French and J. Sherenco, with A. Barr	Modification to language in 3.8 Appendix	07-30-2008	
A. Barr	Sent to Policy Committee	07-30-2008	

8.0 Document Progress (List steps taken to secure approval and next steps needed with appropriate dates.)

<u>Person Responsible</u>	<u>Description</u>	<u>Begin Date</u>	<u>Finish Date</u>
	Begin in Technical Security Committee on:		
	Referred to DoIT Policy Committee on:		
AD Barr	Confirm this policy on agenda for July 1, 2008 Send reminder copy to Policy Committee to review and prepare for committee action on July 1, 2008.	June 19, 2008	
A. Barr	Re-submit to Policy Committee with changes suggested by LD.	July 25, 2008	
A. Barr	Placed on Agenda for final approval at July 29, 2008 meeting	July 25, 2008	
A. Barr	Discussed at Policy Meeting – approved subject to making minor changes.	July 29, 2008	
Dorendorf	Discussed at Policy Meeting	November 18, 2008	
Policy Committee	Set for Town Hall March 24, 2009. Approved extended period for public comments by email before Town Hall meeting. Minor formatting changes.	February 24, 2009	
Policy Committee	Town Hall March 24 changed to Town Hall June 2, 2009. Modified document dates and republished to Web.	May 20, 2009	
Policy Committee – A. Barr	Town Hall held June 2, 2009. Policy approved for submission to CIO. Policy prepared and submitted to CIO.	June 2, 2009	