Ohio Supercomputer Center Policy Name	**No:** **OSC-7**
	Effective: **5/21/09**
	Issued By: Kevin Wohlever Director of Supercomputer Operations **Published By:** Ohio Supercomputer Center **Original Publication Date:** TBD

1.0 Purpose

This policy defines adequate security response for identified security ***incidents***.

2.0 Scope

Pursuant to Ohio IT Policy ITP-A.1, "Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services," this policy applies to all systems under the control of the Ohio Supercomputer Center.

The scope of this information technology policy includes OSC computer and telecommunications systems and the employees, contractors, temporary personnel and other agents of the state who use and administer such systems.

3.0 Background

Information technology continues to be an integral part of how OSC conducts business and maintains information in support of its stated mission. The associated information technology security threats continue to grow. ***Adverse events*** such as unauthorized use of system privileges and system crashes may be the first indicators of a security incident. As a result, OSC is prepared to evaluate adverse events effectively and to respond appropriately when incidents are identified. Poorly handled incidents can result in compromised evidence; loss of time; conflicting information; negative publicity; loss of data ***confidentiality***, ***integrity*** and ***availability***; and increased response costs. Responses to an information technology security incident can range from the recovery of compromised systems to the collection of evidence for the purpose of criminal prosecution. Therefore, preparation and planning for an incident, and ensuring that the right resources are available, are critical to an organization's ability to detect, respond and recover from an information technology security incident.

4.0 References

4.1 Ohio IT Policy ITP-A.1, "Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services," defines the authority of the state chief information officer to establish State of Ohio information technology policies

as they relate to state agencies' acquisition and use of information technology, including, but not limited to, hardware, software, technology services and security.

4.2 Ohio Revised Code section 1347.12 requires that state agencies contact individuals residing in Ohio if unencrypted or unredacted personal information about those individuals that is included in computerized data owned or licensed by the agency is accessed and acquired by unauthorized persons and causes or reasonably is believed will create a material risk of the commission of the offense of identity fraud or other fraud to the individual. Ohio Revised Code section 1347.12 also establishes requirements for proper notification.

4.3 Ohio Revised Code section 149.433, exempts certain types of security and infrastructure records from mandatory release or disclosure under Ohio's public records laws. The exemptions are intended to help protect critical information regarding agency security practices and vulnerabilities.

4.4 Ohio IT Policy ITP-B.1, "Information Security Framework," is the overarching security policy for state information and services. Ohio IT Policy ITP-B.7, "Security Incident Response," is one of several subpolicies. These security policies should be considered collectively rather than as separate or unrelated policies. Attachment 1 illustrates the interrelationship of state technology security policies.

4.5 Ohio IT Guideline, "Information Technology Business Continuity Planning," provides agencies guidance in the development and implementation of a comprehensive information technology business continuity plan.

4.6 Ohio IT Policy ITP-B.8, "Security Education and Awareness," requires state agencies to provide information technology security education and awareness to employees and other agents of the state.

4.7 Ohio IT Policy ITP-B.11, "Data Classification," provides a high-level data classification methodology to state agencies for the purpose of understanding and managing data and information assets with regard to their level of confidentiality and criticality.

4.8 A glossary of terms found in this policy is located in section 9.0 - Definitions. The first occurrence of a defined term is in ***bold italics***.

5.0 Policy

5.1 Adverse Event and Incident Preparation. OSC shall define procedures for how they will detect, evaluate and respond to adverse events, and how they will prepare for, report, manage and recover from information technology security incidents. Such procedures shall incorporate an response plan based on the scope, impact and potential damage of an incident. OSC preparation procedures shall include:

5.1.1 ***Incident Response Team***. The OSC incident response team will include the appropriate system administrators, a representative of the User support group, a member of outreach / user communications team and the director of supercomputing operations. The director of supercomputer operations will lead this team and assign roles as required.

5.1.2 Incident Response Documentation. OSC shall create an incident response reference guide documenting incident response team roles, responsibilities and level of authority for resources and staff participating in the incident response plan. The reference guide shall address adverse event detection, evaluation and response; security incident reporting, communication methods and escalation procedures; and an incident response plan as defined in section 5.3 Incident Response Plan.

5.1.2.1 Incident Response Contact List. OSC shall develop and maintain an incident response contact list. The contact list shall include the names, telephone numbers, pager numbers, mobile telephone numbers, e-mail addresses, organization names, titles, and incident response roles and responsibilities for all key incident response resources, including, but not limited to, incident response team members, key management personnel, public information officers, legal counsel, law enforcement officials and those from other key state agencies and organizations.

5.1.3 ***Recovery*** Preparation. OSC shall regularly evaluate the risks that may be associated with a given information technology security incident and develop procedures to ensure that critical tools, data and equipment are available to facilitate containment and recovery. The procedures shall address the following:

5.1.3.1 System Back-ups. OSC shall create and maintain trusted system, data and application back-ups. Back-ups shall be tested frequently to maintain a high confidence of a successful recovery. Back-ups shall be created on a regular basis and securely maintained.

5.1.3.2 System and Application Software Versions. OSC shall maintain verified copies of all critical system and application installation software. OSC shall ensure that the system and application software versions and security-related patches are current and securely maintained.

5.1.3.3 Configuration Redundancy. Redundant configurations can facilitate the recovery of information technology systems or assets while preserving evidence of a compromised information technology asset. Mission critical systems shall have redundant configurations.

5.1.3.4 System and Application Test Results. OSC will maintain a file or log of trusted system or application test results such as

cryptographic checksums or authoritative lists of services to increase the level of confidence of a restored ***system asset***.

5.2 Adverse Event Evaluation. OSC shall assess if an information technology security incident has occurred and to what extent data or other OSC assets have been compromised. Adverse events shall be investigated with the assumption that the adverse event will be found to be an information technology-specific security incident until proven otherwise. Adverse events such as fire, flood, civil disorder, natural disaster, bomb threat or other such environmental anomalies that are determined to not have risen to the level of a security incident shall nevertheless be handled in accordance with Ohio IT Guideline, "Information Technology Business Continuity Planning," as appropriate. Agency adverse event evaluation procedures shall include the following, at a minimum:

5.2.1.1 Security Adverse Events Log. An information technology security adverse event log shall be securely maintained. At a minimum, the log shall include who reported the adverse event, when the adverse event was reported, a description of the adverse event, how the adverse event was identified, what actions were taken, and who performed each action.

5.2.1.2 Adverse Event Data Collection and Analysis. OSC will determine on a per incident basis, if an incident shall securely maintain any information collected, generated or assessed in the course of determining whether an adverse event is a potential security incident. Data collection and analysis shall focus on identifying the who, what, when, where and how of a reported adverse event. Collected information shall be properly documented and safeguarded. Evidence such as system and network log files, user files, system administrator logs and notes, back-up tapes and intrusion detection system logs, alarms or alerts shall be securely maintained and the ***chain of custody*** preserved by:

- Ensuring the evidence has not been altered;
- Ensuring the evidence is accounted for at all times;
- Verifying the passage of evidence from one party to another is fully documented; and
- Verifying the passage of evidence from one location to another is fully documented.

5.2.1.3 Adverse Event Classification. OSC incident response resources shall review the results of an adverse event evaluation and determine if there is sufficient evidence that an actual information technology security incident has occurred. If ***sensitive data*** is compromised by accident or without an identified, specific attacker or vulnerability, the adverse event may still require treatment as a security incident to ensure proper handling, investigation and

notification. OSC incident response plans shall be executed for adverse events that are determined to be security incidents. OSC shall prioritize security incidents, considering the impact, scope and potential damage to determine the appropriate order and level of response. Such procedures shall include the following, at a minimum:

5.2.1.3.1 Security Incident Evidence File. Incident evidence shall be maintained and safeguarded to preserve the evidence chain of custody. An evidence file shall be created to log and maintain an inventory of all actions taken, action timestamps, and correspondence associated with a security incident. The security incident evidence file shall be securely maintained and safeguarded throughout incident response actions.

5.2.1.3.2 Incident Response Communication. Individuals, OSC and organizations identified in the Incident Response Team Contact List and any other person, company or organization that may be involved in the incident shall be notified in accordance with the agency's notification and escalation procedures. Communication shall be on a need-to-know basis and shall be considered confidential information during a security incident investigation.

5.2.1.3.3 ***Forensic Back-ups***. OSC shall develop criteria that will determine whether incident response team resources shall create forensic back-ups of compromised systems. Any such back-ups shall be obtained using techniques consistent with retaining forensic evidence, such as sector or binary techniques. Any such back-ups shall be maintained in a secure location and preserved following chain of custody requirements identified in section 5.3.1.2.

5.2.2 Incident Containment. OSC shall deploy containment strategies to identify and eliminate an incident's impact on compromised systems, limit the extent of the incident, prevent further damage, and regain normal operation of affected systems. OSC containment measures should take into consideration the priority of an incident, results of the adverse event evaluation, OSC business continuity plans, and OSC procedures regarding response methods. Containment measures shall also be evaluated against the potential loss or corruption of security incident evidence in the event the agency elects to pursue the intruder for possible legal actions or remedy. At a minimum, containment methods shall include the following:

- Ensuring that redundant systems and data have not been compromised;
- Monitoring system and network activity;

- Disabling access to compromised shared file systems;
- Disabling specific system services;
- Changing passwords or disabling accounts;
- Temporarily shutting down the compromised or at risk systems; and
- Disconnecting compromised or at risk systems from the network.

5.2.3 ***Elimination***. OSC will employ procedures to eliminate unauthorized access and remove unauthorized modifications prior to returning compromised systems to service. Agencies shall ensure that systems are protected against like or similar types of incidents in the future. Elimination methods may include, but are not limited to, the following:

- Changing passwords on compromised systems;
- Disabling compromised accounts;
- Reinstalling compromised systems from trusted back-ups;
- Identifying and removing an intruder's access methods, such as back doors;
- Installing system patches for known weaknesses or vulnerabilities;
- Reinstalling system user files from trusted versions;
- Reinstalling system settings from trusted sources;
- Reinstalling system start-up routines from trusted versions; and
- Adjusting or deploying firewall or intrusion detection system technologies to detect access and intrusion methods.

5.2.4 Notification. Agencies shall determine if the incident resulted in a breach of security of a system containing personal information as defined by Ohio Revised Code 1347.12 and then notify affected individuals as required by Ohio Revised Code 1347.12.

5.2.5 Recovery. OSC shall evaluate security incidents and determine when to return compromised systems to normal operation. Access to compromised ***system assets*** shall be limited to authorized personnel until the security incident has been contained and the root cause of the incident eliminated. If OSC returns the system to operation before full analysis and elimination procedures are completed, OSC shall assess the risk to ongoing operations while increasing system monitoring and heightening security awareness. Recognizing that OSC systems are vulnerable to another occurrence of the same type of intrusion, analysis and elimination procedures shall be completed as soon as possible. Recovery procedures shall address the following:

5.2.5.1 Recovery Requirements. OSC shall define and prioritize the requirements to be met before returning an affected or compromised system to normal operation.

5.2.5.2 Validate Restored Systems. OSC shall validate the restored systems through system or application regression tests, user verification, penetration tests, vulnerability testing and test result comparisons.

5.2.5.3 Increased Security Awareness. OSC shall heighten awareness and monitor for a recurrence of the information technology security incident.

5.3 Lessons Learned Procedure. OSC shall capture and disseminate lessons learned from security incidents to reduce the possibility for similar incidents and thereby enhance the overall information technology security posture.

5.3.1 Post-Incident Analysis. OSC shall convene a post-incident analysis and review meeting within three to five business days of completing the incident investigation. Extended delays may reduce the effectiveness of relating critical information. Questions to be addressed may include, but are not limited to:

- Did detection and response systems work as intended? If not, what methods would have prevented the incident?
- Are there additional procedures that would have improved the ability to detect the incident?
- What improvements to existing procedures and tools would have aided in the response process?
- What improvements would have enhanced the ability to contain the incident?
- What correction procedures would have improved the effectiveness of the recovery process?
- What updates to agency policies and procedures would have allowed the response and recovery processes to operate more smoothly?
- How could user and system administrator preparedness be improved?
- How could communication throughout the detection and response processes be improved?
- Was the incident identified as a potential threat during the agency's risk assessment process?
- What was the impact in terms of financial loss, loss of public trust, legal liability, or harm to public health and welfare?

Results of these questions shall be documented and incorporated into a report for senior OSC management, with further distribution as outlined in section 5.4 of this policy.

5.3.2 Lessons Learned Implementation. OSC shall apply, where appropriate, new and improved methods gained from lessons learned during their post-incident analysis process.

5.4 Incident Reporting. OSC shall report all security incidents as they are identified and their subsequent containment to the director of the Ohio Supercomputer Center who shall forward the results of their post-incident analysis to the Office of Information Technology Security Response Team.

5.5 Revised Risk Assessment. OSC shall perform a new risk assessment if the impact of a security incident was significant.

5.6 Compliance Review. OSC shall conduct a compliance review of their incident response policy with relevant staff (ie. IT, policy, communications, and legal personnel). The review shall determine if an agency's policies and procedures:

- Protect evidence chain of custody;
- Comply with overall agency and state policies;
- Conform to federal, state or local laws; and
- Maintain the confidentiality of all investigative data and evidence;

5.7 Education & Awareness. OSC will use appropriate resources for an education and awareness program. At a minimum, the program shall address:

- How to identify and report suspected intrusion;
- Use of response tools and environments in accordance with defined incident response roles and responsibilities;
- Communication methods;
- Existing and new intrusion threats; and
- Preserving the chain of custody for incident evidence.

6.0 Procedures

6.1 OSC shall provide the following information:

6.1.1 OSC shall, at a minimum, establish a primary and secondary incident response point of contact and register this contact information with the Office of Information Technology Risk Management Services.

6.1.1.1 With regard to this policy, the incident response point of contact is responsible for reporting all security incidents as soon as they are identified.

6.1.2 At a minimum, the incident response point of contact shall provide the following information relating to an identified security incident:

6.1.2.1 Contact Information:

- Name
- Title
- Primary or secondary status
- Organization
- Telephone number
- Cell phone number
- Pager number
- Facsimile

- E-mail
- Mailing address

6.1.2.2 Incident Summary:

- Time elements, to include the date and time reported, date and time detected, date and time occurred, and the duration of adverse event
- Current status of the incident
- Brief description of the incident
- Source or cause of the incident, if known
- Whether or not the incident has occurred before and if so, when, providing previous reports if possible
- Specifics about the affected systems, if known, such as software, Internet protocol address or network, and service
- Any additional information as requested by the Office of Information Technology Risk Management Services that is specific to containing or mitigating the current incident

6.2 Incident reports shall be communicated through one of the following channels to the OSU Buckeye Secure group:

Telephone: (614) 247-2020

E-mail: security@osu.edu

7.0 Implementation

The policy goes into affect immediately up acceptance.

8.0 Revision History

Date	Description of Change
6/1/2009	Original policy.
03/19/2012	Scheduled policy review.

9.0 Definitions

9.1 Adverse Event. Any observable occurrence with a negative consequence in a system or network.[1] Examples of adverse events include system crashes, network packet floods, unauthorized use of system privileges, defacement of a Web page, execution of malicious code that destroys data, physical security,

[1] Grance, Tim, Karen Kent, and Brian Kim. Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology. January 2004. < http://www.csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

data or access compromised by accident, and lost or stolen laptops. Adverse events sometimes provide an indication that an incident is occurring. However, not all adverse events are security incidents.

9.2 Availability. The assurance that information and services are delivered when needed. Certain data must be available on demand or on a timely basis. Information systems that must ensure availability will likely deploy techniques such as uninterrupted power supplies or system redundancy.

9.3 Chain of Custody. Defined actions taken to ensure that collected evidence has not been compromised, can be accounted for at all times, and documents the secure passage of evidence from one party or location to another. Chain of custody procedures are essential to preserve evidence for legal proceedings.

9.4 Confidentiality. The assurance that information is disclosed only to those systems or persons who are intended to receive the information. Areas in which confidentiality may be important include nonpublic customer information, patient records, information about a pending criminal case, or infrastructure specifications. Information systems that must ensure confidentiality will likely deploy techniques such as passwords, and could possibly include encryption.

9.5 Cryptographic Checksums. A secret or coded value used to ensure that data blocks are stored or transmitted without error. The value is created by calculating the binary values in a block of data using an algorithm, which is encoded and stored with the results and data. Transmitted or retrieved data will be confirmed by recalculating the checksum and comparing the original with the recomputed results. A non-match indicates an error.

9.6 Elimination. Defined step or process within an incident response plan with the goal of eradicating the root cause of a security incident.

9.7 Forensic Back-ups. Back-ups using techniques to generate an identical sector-by-sector back-up of a storage medium.

9.8 Incident. A reported adverse event or group of adverse events that has proven to be a verified information technology security breach. An incident may also be an identified violation or imminent threat of violation of information technology security policies[2], or a threat to the security of system assets. Some examples of possible information technology security incidents are:

- Loss of confidentiality of information
- Compromise of integrity of information
- Loss of system availability
- Denial of service

[2] Grance, Tim, Karen Kent, and Brian Kim. Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology. January 2004. < http://www.csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

- Misuse of service, systems or information
- Damage to systems from malicious code attacks, such as viruses, trojan horses or logic bombs

9.9 Incident Response. A structured and organized response to any information technology security adverse event or incident that threatens an agency's system assets, including systems, networks and telecommunications systems.

9.10 Incident Response Team. A group of professionals within an organization trained and chartered to respond to identified information technology security incidents. The incident response team has both an investigative and problem-solving component and should include management personnel with the authority to act, technical resources with the knowledge and expertise to rapidly diagnose and resolve problems, and communication personnel to keep appropriate individuals and organizations properly informed and develop public image strategies as necessary.

9.11 Integrity. The assurance that information is not changed by accident or through a malicious or otherwise criminal act. Because businesses, citizens and governments depend upon the accuracy of data in state databases, agencies must ensure that data is protected from improper change. Information systems that must ensure integrity will likely deploy techniques such as scheduled comparison programs using cryptographic techniques and audits.

9.12 Recovery. A defined step or process in an incident response plan with the goal of returning the affected or compromised systems to normal operations.

9.13 Risk Assessment. A process for analyzing threats to and the vulnerabilities of information systems as well as determining the potential impact that the loss of information or system capabilities would have on the organization. Risk assessments provide a foundation for risk management planning and the attainment of optimal levels of security. See Ohio IT Policy ITP-B.1, "Information Security Framework," for assessment guidelines.

9.14 Sensitive Data. Any electronic information that a state agency maintains and must not disclose under penalty of law, or "personal information" that consists of any individual's name, including the last name along with the individual's first name or first initial, in combination with and linked to any one or more of the following data elements: social security number; driver's license number or state identification card number; or financial account number or credit or debit card number. Sensitive data also includes any other electronic information that the agency determines to be high-risk should the information be accessed by unauthorized parties.

9.15 System Assets. Information, hardware, software and services required to support the business of the agency, and identified during the risk assessment process as assets that need to be protected in accordance with Ohio IT Policy ITP-B.1, "Information Security Framework."

10.0 Related Resources

Document Name
National Institute of Standards and Technology Special Publication 800-61, "Computer Security Incident Handling Guide."
Ohio IT Bulletin ITB-2007.02, "Data Encryption and Securing Sensitive Data," available at www.ohio.gov/itp.

11.0 Inquiries

Direct inquiries about this policy to:

Director of Supercomputer Operations
1224 Kinnear Rd.
Columbus, OH 43212

Telephone: 614-292-9248

OSC IT Policies can be found on the Internet at: www.osc.edu/policies