

Security Incident Response Policy

| | |
|--------------------|--|
| Effective | September 1, 2008 |
| ✓ Purpose | To set forth departmental policy to ensure uniformity and consistency in how Department employees response to a Security Incident. |
| 📖 Authority | Statewide Information Technology Policy Ohio IT Policy; ITP-B.7; Security Incident Response |
| 📄 Reference | Ohio IT Bulletin; ITB-2007.02; Data Encryption and Securing Sensitive Data Office of Information Technology Enterprise Procedure; OEP SEC.4001; Statewide Incident Response Reporting |
| 📞 Resource | Office of Information Technology |

1.0 Purpose

The purpose of this policy is to ensure that the Ohio Department of Natural Resources (ODNR) implements and maintains an adequate security response capability for reported or identified security events and incidents.

2.0 Scope

This policy defines the requirements necessary to provide a coordinated information security incident response for all of ODNR. The requirements of this policy apply to all ODNR programs and include all ODNR owned or operated computer and telecommunications systems and the ODNR employees, contractors, temporary personnel and other agents of the state who use or administer such systems. This policy does not apply to ODNR customers.

3.0 Background

Information technology (IT) is an integral part of how ODNR conducts business and maintains information in support of its stated mission. As the use of technology increases, the threats associated with IT security incidents continue to grow. As a result, ODNR must be prepared to respond when incidents occur. Lack of preparation can

have significant consequences as organizations attempting to respond to an incident with limited or no advance planning may actually cause more damage. Poorly handled incidents can result in compromised evidence, loss of time, conflicting information, negative publicity, and loss of data confidentiality, integrity and availability. Responses to an IT security incident can range from simply recovering 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 ODNR's ability to adequately detect, respond to and recover from an IT security incident.

4.0 References

- 4.1. **Ohio IT Policy; ITP-B.7; Security Incident Response (June 14, 2006):** This state level directive requires state agencies to develop and maintain an adequate security response capability for reported or identified security events and incidents.
- 4.2. **Ohio IT Bulletin; ITB-2007.02; Data Encryption and Securing Sensitive Data (July 25, 2007):** This IT Bulletin provides guidance to agencies on protecting sensitive data.
- 4.3. **Office of Information Technology Enterprise Procedure; OEP SEC.4001; Statewide Incident Response Reporting (August 10, 2006):** This statewide procedure defines the steps to be followed by State of Ohio agencies reporting information, computer system, or network security incidents.
- 4.4. **ODNR Procedure; Incident Response (April 1, 2008):** This ODNR procedure defines the steps to follow for ODNR's response to any type of critical incident, including security incidents, that affects ODNR's applications, systems, networks, infrastructure or capability to deliver services.
- 4.5. A glossary of terms found in this policy is included in section **8.0 – Definitions**.

5.0 Policy

The cornerstone of ODNR's security incident response capability is the ODNR Incident Response Procedure. All employees shall follow the Incident Response Procedure whenever a security incident or other critical incident is reported or identified.

In accordance with Ohio IT Policy ITP-B.7; Security Incident Response, ODNR shall implement additional incident response capabilities as they become feasible. As a minimum, such capabilities shall include the following provisions.

Should ODNR experience a security event, which is a system anomaly or attempted breach, it shall have a structured means of evaluating that event to determine if it

indeed rises to the level of an actual security incident, which is a verified breach or violation of an IT asset.

5.1 Preparation

ODNR shall define procedures for how it will detect, evaluate and respond to security events, and report, prepare for, manage and recover from IT security incidents. Such procedures shall incorporate an ODNR response plan based on the scope, impact and potential damage of an incident. ODNR preparation procedures shall include:

- 5.1.1 Incident Response Team. ODNR has defined and continues to develop an incident response team (IRT) responsible for responding to, managing, supporting and participating in incident response activities. The IRT acts at the time of an information security incident to minimize and contain damage, gather evidence and resume normal processing. Roles, responsibilities and levels of authority are defined for IRT members in the ODNR Incident Response Procedure and ODNR Incident Response Contact List.
- 5.1.2 IR Documentation. ODNR shall create an incident response (IR) reference guide documenting IRT roles, responsibilities and level of authority for resources and staff participating in ODNR 's incident response plan. The reference guide shall address security event detection, evaluation and response; security incident reporting, communication methods, and escalation procedures; and an IR plan as defined in Section 5.2 – Incident Response Plan.
- 5.1.3 Recovery Preparation. ODNR shall evaluate what risks to ODNR may be associated with a given IT security incident and develop procedures to ensure critical tools, data and equipment are available to facilitate containment and recovery. The procedures shall address:
 - 5.1.3.1 System Back-ups. ODNR Programs shall create and maintain trusted system, data and application back-ups. Back-ups shall be tested on a regular basis to maintain a high confidence of a successful recovery. Back-ups shall be created on a regular basis and securely maintained in accordance with Ohio IT Bulletin; ITB-2007; Data Encryption and Securing Sensitive Data.
 - 5.1.3.2 System and Application Software Versions. ODNR Programs shall maintain verified copies of all critical system and application installation software. The Programs shall ensure 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 IT systems or assets while preserving evidence of a compromised IT asset. All systems deemed mission critical shall have redundant configurations.

5.1.3.4 System and Application Test Results. ODNR shall 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.

These procedures may be the same or be complementary to the procedures developed to address business continuity issues.

5.1.4 IR Contact List. ODNR has developed and continues to refine and maintain an incident response contact list. The contact list shall include the names, telephone numbers, pager numbers, mobile telephone numbers, email addresses, organization names, titles, and incident response roles and responsibilities for all key incident response resources, including but not limited to IRT members, key ODNR management personnel, public information officers, legal counsel, law enforcement officials and those from other key state agencies and organizations.

5.1.5 Readiness Testing. ODNR shall establish procedures for testing and evaluating incident response capabilities on a periodic basis. As a minimum, ODNR shall conduct an incident response evaluation and readiness test on an annual basis.

5.2 Incident Response Plan

ODNR has defined and continues to develop and maintain an IR plan to evaluate IT security events to determine if an event has become an incident and to detail ODNR's IRT actions in response to an identified security incident. The plan is documented in ODNR's Incident Response Procedure and ODNR's Incident Response Contact List. In accordance with Ohio IT Policy; ITP-B.7; Security Incident Response, the ODNR IR plan shall include the following elements:

5.2.1 Event Evaluation. ODNR shall determine how to evaluate IT security events. The evaluation process shall assess if an IT security incident has occurred and to what extent data or other state assets have been compromised. Events shall be investigated with the assumption that the event will be found to be an IT-specific security incident until proven otherwise. Security events such as fire, flood, civil disorder, natural disaster, bomb threat or other such environmental anomalies that are determined not to have risen to the level of a security

incident shall nevertheless be handled in accordance with ODNR 's business continuity process as appropriate. ODNR IT security event evaluation procedures shall include at a minimum:

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

5.2.1.2 Event Data Collection and Analysis. As part of event evaluation, ODNR shall collect and securely maintain information concerning reported events to assess whether a security event is a general system anomaly or potential security incident. Data collection and analysis shall focus on identifying who, what, when, where and how of a reported security 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 (IDS) 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 Event Classification. ODNR IR resources shall review the results of an event evaluation and determine if there is sufficient evidence to determine if an actual IT security incident has occurred. ODNR IR plans shall be executed for security events that are determined to be security incidents. ODNR shall determine an appropriate level of response regarding the impact, scope and potential damage of any incident. Such ODNR procedures shall include at a minimum:

5.2.1.3.1 Security Incident Evidence File. 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 files shall

be securely maintained and safeguarded throughout the incident response actions. Incident evidence shall be maintained and safeguarded to preserve the evidence chain of custody.

5.2.1.3.2 IR Communication. Individuals, agencies and organizations identified in ODNR's IRT Contact List shall be notified in accordance with ODNR's Incident Response Procedure. 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. ODNR shall develop criteria that will determine whether IRT 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 5.2.1.2.

5.2.2 Incident Containment. ODNR shall deploy containment strategies to identify and eliminate an incident's impact to compromised systems, limit the extent of the incident, prevent further damage and regain normal operations of affected systems. ODNR containment measures should take into consideration the assessment of an incident including its scope, impact, and damage, results of the incident evaluation, ODNR business continuity plans and ODNR procedures regarding response methods. Containment measures shall also be evaluated against the potential loss or corruption of security incident evidence in the event the ODNR elects to pursue the intruder for possible legal actions or remedy. Containment methods may include, but are not limited to:

- Ensuring 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. ODNR shall develop and employ procedures to eliminate unauthorized access and remove unauthorized modifications prior to returning compromised systems to service. ODNR shall ensure systems are protected against like or similar types of incidents in the future. Elimination methods may include, but are not limited to:

- Changing passwords on compromised systems. Highly recommended if evidence indicates the system password files were compromised.
- Disabling compromised accounts;
- Reinstalling compromised systems from trusted back-ups;
- Identifying and removing an intruder's access methods such as backdoors;
- 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 IDS technologies to detect access and intrusion methods.

5.2.4 Notification of a Personal Information Security Breach. ODNR shall determine if the incident resulted in a breach 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. ODNR shall evaluate and determine when to return compromised systems back to normal operations. Access to compromised system assets shall be limited to authorized personnel until the security incident has been contained and root cause of the incident eliminated. If ODNR returns the system to operations before full analysis and elimination procedures are completed, ODNR shall assess the risk to ongoing operations while increasing system monitoring and heightening security awareness. Analysis and elimination procedures shall be completed as soon as possible, recognizing ODNR systems are vulnerable to another occurrence of the same type of intrusion. Recovery procedures shall address:

5.2.5.1 Recovery Requirements. ODNR shall define the requirements to be met and their priority before returning an affected or compromised system to normal operations.

5.2.5.2 Validate Restored Systems. ODNR 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. ODNR shall heighten awareness and monitor for a recurrence of the IT security incident.

5.2.6 Lessons Learned. ODNR shall capture and disseminate incident lessons learned to reduce the possibility for similar incidents and thereby enhance the overall IT security posture. ODNR shall establish a lessons learned capability by:

5.2.6.1 Post Mortem Analysis. In accordance with ODNR's Incident Response Procedure, ODNR shall perform a post mortem analysis and review meeting within five 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 ODNR 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 during the ODNR's risk assessment process as a potential threat?
- 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 points shall be documented and incorporated into a report for senior ODNR management.

5.2.6.2 Lessons Learned Implementation. ODNR shall apply as applicable new and improved methods from lessons learned in their post mortem analysis process.

5.2.6.3 Risk Assessment. ODNR shall perform a new risk assessment if the impact of a security incident was significant.

5.2.6.4 Incident Reporting. Pursuant to Ohio IT Policy ITP-B.7, Security Incident Response, and Office of Information Technology Enterprise Procedure OEP SEC.4001, Statewide Incident Response Reporting, OIT serves as Ohio's centralized reporting authority for IT security incidents and shall implement internal procedures to fulfill that role.

5.3 Legal Review

ODNR shall conduct a legal review of incident response procedures. The review shall determine if IR procedures:

- Protect evidence chain of custody;
- Are legally defensible and enforceable;
- Comply with overall ODNR and state policies;
- Demonstrate due diligence;
- Conform to national, state or local laws or regulations;
- Maintain the confidentiality for all investigative data and evidence;
- Protect ODNR staff or other agents of the state from legal liability; and
- Safeguard ODNR from legal liability during a system compromise if an intruder was allowed access while evidence was gathered or ODNR assets were used to launch an attack on another organization.

5.4 Education & Awareness

ODNR shall ensure that incident response concepts are addressed in education and awareness programs. The programs 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 Related Procedures

Procedures must be developed in order to effectively and efficiently implement this policy. The ODNR Programs, with support from the ONDR- Office of Information Technology, are responsible for the establishment and implementation of procedures that comply with the requirements of this policy. The primary procedure governing ODNR's security incident response is the ODNR Incident Response Procedure.

7.0 Compliance

It is the responsibility of management to implement and ensure compliance with the laws, rules, policies, procedures, standards, and license agreements applicable to the use of IT resources within their functional areas.

It is the responsibility of the user of IT resources to ascertain, understand, and comply with the laws, rules, policies, procedures, standards, and license agreements applicable to their use of those resources.

Violation of this policy by the user of IT resources may result in loss of access to those resources. Any ODNR employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Any contractor, vendor, or other agent of the state performing work for or on behalf of ODNR found to have violated this policy may be subject to consequences specified in the contract or other agreement governing their engagement by ODNR , up to and including termination of the contract.

8.0 Definitions

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

Cryptographic Checksums. A secret or coded value used to ensure 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 with the 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.

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

Event. Any observable occurrence in a system or network. Examples of events include the system boot sequence, a system crash and packet flooding within a network. Events sometimes provide an indication that an incident is occurring.

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

Incident. A reported security event or group of events that has proven to be a verified IT security breach, or a violation of IT security policies, or a threat to the security of system assets that results in at least one of the following categories:

- Loss of confidentiality of information
- **Compromise of integrity of information**
- **Loss of system availability**
- Lost or Stolen Data (Example: Lost or stolen laptop, desktop, external storage device)
- Denial of service
- Misuse of service, systems or information
- Damage to systems from malicious code attacks such as viruses, trojan horses or logic bombs

Incident Response. A structured and organized response to any IT security event or incident that threatens an agency's system assets including systems, networks and telecommunication systems.

Incident Response Contact List. A list of resources identified as part of an agency's incident response team. The contact list includes the names, contact numbers, organization, roles and responsibilities of all team members.

Incident Response Team. A group of professionals within an organization trained and chartered to respond to identified IT 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.

ODNR Contractors. For the purposes of this policy, ODNR contractors are defined as contracted staff and vendor technicians.

ODNR Employees. For the purposes of this policy, ODNR employees are defined as all employees and representatives of ODNR, whether they are permanent staff or temporary staff.

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

Risk Assessment. A process concerned with identifying, analyzing and responding to IT security risks. Risk assessment attempts to maximize the results of positive events and minimize the results of negative events. See Ohio ITP B.1, "Information Security Framework," for assessment guidelines.

System Assets. System assets include 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."

9.0 Related Resources

ODNR Incident Response Contact List

10.0 Inquiries

Direct inquiries about this policy to:

Security Privacy Officer – Ken Fritz
Ohio Department of Natural Resources
Office of Information Technology
2045 Morse Road Building I-2
Columbus, Ohio 43229

Telephone: 614 265-6853

E-mail: Ken Fritz