

# Security Incident Response Procedure

<b>Effective</b>	Draft
 <b>Purpose</b>	To set forth the procedures for the Ohio Department of Natural Resources employees to follow in response to a potential security incident
 <b>Authority</b>	State Wide IT Policy Ohio IT Policy; ITP-B.7; Security Incident Response (June 14, 2006)
 <b>Reference</b>	Ohio IT Bulletin; ITB-2007.02; Data Encryption and Securing Sensitive Data (July 25, 2007) Office of Information Technology Enterprise Procedure; OEP SEC.4001; Statewide Incident Response Reporting (August 10, 2006)
 <b>Resource</b>	ODNR - Office of Information Technology

## Purpose

This procedure defines the steps to follow for ODNR's response to any type of critical incident that affects ODNR's applications, systems, networks, infrastructure, or capability to deliver services.

## Scope

The scope of this procedure includes all incidents determined to be critical that affect the ODNR infrastructure, services, or related technology.

The term "incident" refers to an adverse event impacting one or more computer systems, networks, or other components of ODNR's technology infrastructure or to the threat of such an event. An "incident" can also be defined as a situation in which an entity's information or technical infrastructure is at risk, whether the situation is real or simply perceived. Examples of incidents would be:

- Viruses
- E-mail viruses
- E-mail harassment

- Worms
- Other malicious code
- Denial of service attacks
- Intrusions
- Lost or Stolen data (Example: lost or stolen laptop, pc, external hard drive)
- Network or system sabotage
- Website defacements
- Unauthorized access to files or systems
- Physical damage to computer systems, networks, or storage media

An incident is defined as “critical” if its potential impact on ODNR’s technology infrastructure, services, or customers is so severe, sensitive, or widespread that it requires escalation and/ or mitigation efforts well above the norm.

## **Procedure**

### ***3.1 Responsibilities***

ODNR employees are responsible for informing their supervisors about suspicious activities or unusual events that might indicate an incident has occurred or are in progress.

The manager of the ODNR service or program involved or the originally notified supervisor is responsible for determining if an incident is in progress.

When an employee or supervisor believes an incident may be in progress or may have occurred, they are responsible for notifying the ODNR IT support desk (614 265-7082) immediately to begin the security logging and investigation process. If the incident happens after ODNR IT support desk hours 7:30AM – 5:00PM (Monday through Friday) then contact the Emergency Operation Center EOC at (614 799-9572). In addition, a ticket must be logged through the Ohio Customer Service and Security Center by ODNR’s designated primary or alternate security contacts.

The ODNR Incident Coordinator (ODNR IC) is notified by the ODNR- Office of Information Technology Support Desk when a security ticket is logged. The ODNR IC then contacts the ODNR Director, Ohio Chief Privacy Officer, and the ODNR Security/Risk Management Services Administrator.

If the incident involves alleged illegal activity or missing data, the ODNR IC contacts the ODNR Chief Legal Counsel. The ODNR Chief Legal Counsel will then contact the Ohio State Highway Patrol and the Governor’s Office. In emergency situations, the ODNR IC may contact the Ohio State Highway Patrol and then the ODNR Chief Legal Counsel.

The manager of the ODNR service or program involved, or the originally notified supervisor, is responsible for incident containment and damage control procedures specific to their service area.

The manager of the ODNR service or program involved, or the originally notified supervisor is responsible for determining what technical information about the incident will be documented and what files will be preserved for future reference or used as evidence.

### ***3. 2 Logging of Incident***

When a Supervisor, Service Manager, or Program Manager determines that a critical incident has occurred or is in progress and have contacted the ODNR IT help desk or the EOC, the Incident Response Primary or Alternate Contact shall log a security incident ticket by calling the Ohio Customer Service and Security Center at 614-644-0701 or 800-644-0701 or sending an email to OCSSC@ohio.gov. The logging of the ticket will trigger notification to the OIT Incident Coordinator.

If an incident, per **Ohio IT Policy ITP-B.7, Security Incident Response**, is logged with the OCSSC that requires State OIT to respond to a request for emergency technical assistance from an agency, the State OIT Incident Coordinator (State OIT IC) will also be notified by the OCSSC. The State OIT IC will notify the appropriate service manager if an State OIT service is involved.

If the logged incident could potentially involve multiple agencies, the State OIT IC will send an e-mail to the Agency Incident Response Contacts to notify them of the situation. No agency names will be mentioned when describing the incident.

### ***3. 3 Critical Incident Response***

ODNR will respond to a critical incident using the process diagramed in the attached flow chart and instructions contained in the contact list document. (The contact list is maintained separately from this procedure document.)

## **Incident Response Roles**

### ***1.1 ODNR Incident Coordinators***

The ODNR Incident Coordinator is the single point of contact for overall coordination of a critical incident that has been logged with the (Office of Information Technology Support Desk). The incident could involve another agency or be internal to ODNR.

In the event that the scope of the incident is too large for one ODNR IC to facilitate, a second ODNR IC will be called to assist. The ODNR IC will gather and communicate information about the incident and contact Program Incident Coordinators to obtain resources and notify them of the incident. The ODNR IC will also assist with customer communications, assist in archiving incident related documentation, assess situations, and communicate with the Executive Team should they need to be contacted. The ODNR IC will chair the post mortem meeting for closed critical incidents and be responsible for updating the incident ticket and ensuring that the incident is documented and the ticket is closed.

The ODNR Incident Coordinator has the authority to request and receive non-technical and technical support and assistance from other ODNR staff as needed.

The ODNR IC will also be able to use appropriate e-mail distribution lists, or phone tree lists, and other contact lists, or have access to people who can.

The ODNR IC is responsible for assuring that the logged ticket is closed, or in the case of an incident logged by another agency, the ODNR IC works with the Agency Incident Response Contact to confirm that they have closed the ticket for their agency.

### ***1.2 Program Incident Coordinators***

The role of Program Incident Coordinator (PIC) includes being the primary or alternate coordinator for an ODNR Program Area and also filling the role of an ODNR IC when one is not available. The PIC works directly with the ODNR IC to coordinate resources. The PIC is responsible for managing and coordinating communications and resources within their program area and between their area and other areas. The PIC may be asked to provide resources from their area to other areas in order to assist in mitigation of an incident. The PIC will assess situations and respond as needed, archive incident related documentation, and participate in post mortem meetings.

The PIC will contact the appropriate Technical Team members for assistance in mitigating an incident.

### ***1.3 Technical Incident Contacts***

The role of Technical Incident Contact (TIC) is to provide technical assistance in mitigating the incident. The TIC may provide this assistance in their program area as well as be deployed to assist in other program areas.

When the ODNR Call Center or the OCSSC is notified and a critical incident ticket is created, the ODNR Incident Coordinator or a Program Incident Coordinator will call and/or page individuals on the Technical Incident Contacts

Call List in order to request technical expertise assistance to mitigate the incident.

Technical Incident Contacts will include management and staff from the ODNR service areas impacted by the incident, but they may also include people from other areas and technical disciplines.

The ODNR areas providing Technical Incident Contacts must have Technical Team contacts available at all times. If a primary contact is not available, an alternate should be substituted. The alternate will be responsible for responding to attempts made to reach the primary contact.

#### ***1.4 Executive Team Contacts***

Executive Team contacts are individuals who will be contacted depending upon the scope and severity of the incident. An Executive Team contact may be asked by the ODNR IC to contact Director level staff.

#### ***1.5 Agency Incident Response Contacts***

Each cabinet level agency has an identified Primary and Alternate Contact for Incident Response communications. The names and contact information for the Primary and Alternate Contacts are maintained in the OIT Incident Response Call list which is maintained separately from this procedure document.

### **Requests for Information**

The ODNR Incident Coordinator (ODNR IC) will be the focal point for communications with the ODNR Executive Team, Program Incident Coordinators and if needed with the ODNR Customers. Keeping ODNR management, staff, and customers updated on the status of the incident as it progresses will be a high priority. The ODNR Executive Team Contacts will be notified by the ODNR Incident Coordinator on an as needed basis depending upon the severity and scope of the critical incident.

If an ODNR staff member receives a request for incident information directly from the news media, general public, or from any individual whose organizational affiliation is unknown, no information will be given out, and the request will be directed to the ODNR Communications Office.

All requests for information from the news media should go through the ODNR Communications Office before any public statements are made.

## Post Mortem

No more than five business days after the incident is resolved, the ODNR IC will facilitate an incident post mortem with the appropriate PIC, TIC and Executive Team individuals. During the post mortem, information collected about the incident will be verified and lessons learned will be documented. Use of the Production Incident Explanation (PIE) report is assigned by the ODNR IC.

### *1.6 Documentation*

The ODNR IC and PIC will assist the service managers and Technical Teams in archiving incident related documentation for future reference. Potential legal evidence collected during incident resolution must be preserved.

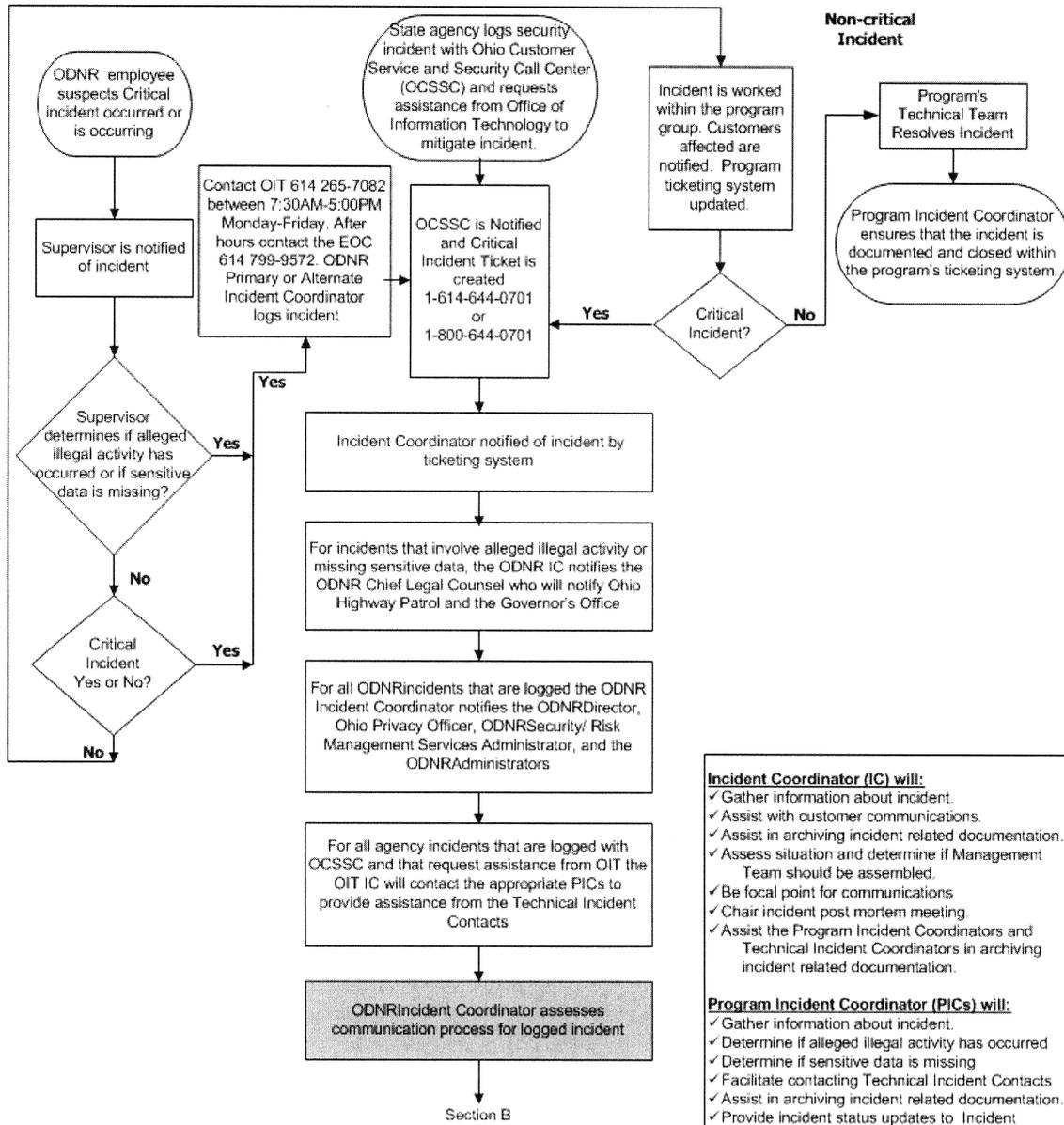
## Inquiries

Direct inquiries about this procedure to:

Chief 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@dnr.state.oh.us](mailto:ken.fritz@dnr.state.oh.us)

**Critical Incident Response Flow Chart**  
ODNR's Procedure for Logging Incidents  
Section A - Incident Assessment Process



- Incident Coordinator (IC) will:**
- ✓ Gather information about incident.
  - ✓ Assist with customer communications.
  - ✓ Assist in archiving incident related documentation.
  - ✓ Assess situation and determine if Management Team should be assembled.
  - ✓ Be focal point for communications
  - ✓ Chair incident post mortem meeting.
  - ✓ Assist the Program Incident Coordinators and Technical Incident Coordinators in archiving incident related documentation.
- Program Incident Coordinator (PICs) will:**
- ✓ Gather information about incident.
  - ✓ Determine if alleged illegal activity has occurred
  - ✓ Determine if sensitive data is missing
  - ✓ Facilitate contacting Technical Incident Contacts
  - ✓ Assist in archiving incident related documentation.
  - ✓ Provide incident status updates to Incident Coordinator
  - ✓ Assist with customer communications.
  - ✓ Participate in incident post mortem meeting
- Technical Incident Contacts (TICs) will:**
- ✓ Continue incident containment and damage control efforts.
  - ✓ Keep Program Incident Coordinator apprised of the status of the incident.

## Critical Incident Response Flow Chart

### Section B - Communication Process

