FOR OFFICIAL USE ONLY

DPI Data Incident Response Procedure

Wisconsin Department of Public Instruction

(July 7, 2013)

FOR OFFICIAL USE ONLY

Document Change History

Version Number	Date	Author	Description

Department of Public Instruction Data Incident Response Procedure

Background

In support of the DPI Incident Response Plan, the following procedures are identified as the process DPI will engage for a reported potential data incident to ensure the potential reported incident is reviewed, documented and communicated appropriately.

Incident Response Procedure

1) Reported Potential Incident

A potential incident is reported to the DPI Helpdesk, a ticket is created to track the issue and communications to the Information Technology Management team to initiate the incident response.

2) Incident Analysis Document created

The Information Technology Management team will create a DPI Incident Response Analysis document to centrally manage the incident information to validate the incident facts and guide decisions regarding the incident.

3) Identification

Identification of an incident is the process of analyzing an event and determining if that event is normal or if it is an incident. An incident is an adverse event and it usually implies either harm, or the attempt to harm DPI. Events occur routinely and will be examined for impact. Those showing either harm or intent to harm may be escalated to an incident.

The term "incident" refers to an adverse event impacting one or more DPI's information assets or to the threat of such an event. Examples include, but are not limited to, the following:

- Unauthorized use
- Denial of Service
- Malicious code
- Network system failures (widespread)
- Application system failures (widespread)
- Unauthorized disclosure or loss of information
- Information Security Breach
- Other

Incidents can result from any of the following:

- Intentional and unintentional acts
- Actions of state employees
- Actions of vendors or constituents
- Actions of third parties
- External or internal acts
- Credit card fraud

- Potential violations of Federal, Statewide or DPI's Policies
- Natural disasters and power failures
- Acts related to violence, warfare or terrorism
- Serious wrongdoing
- Other

4) Incident Classification

Once an event is determined to be an incident by the Information Technology Management Team, the Incident Response team will be selected and the incident will be classified. There are several methods exist for classifying incidents.

The following factors are considered when evaluating incidents:

- Criticality of systems that are (or could be) made unavailable
- Value of the information compromised (if any)
- Number of people or functions impacted
- Agency considerations
- Public relations
- Enterprise impact
- Multi-agency scope

5) Triage

The Incident Response Team will review the DPI Incident Response Analysis document and triage the information provided. The objective of the triage process is to gather information, assess the nature of an incident and begin making decisions about how to respond to it. It is critical to ensure when an incident is discovered and assessed the situation does not become more severe.

- What type of incident has occurred
- Who is involved
- What is the scope
- What is the urgency
- What is the impact thus far
- What is the projected impact
- What can be done to contain the incident
- Are there other vulnerable or affected systems
- What are the effects of the incident
- What actions have been taken
- Recommendations for proceeding
- May perform analysis to identify the root cause of the incident

6) Evidence Preservation

Carefully balancing the need to restore operations against the need to preserve evidence is a critical part of incident response. Gathering evidence and preserving it are essential for proper identification of an incident, and for business recovery. Follow-up activities, such as personnel actions or criminal prosecution, also rely on gathering and preserving evidence.

7) Computer Forensics

In information security incidents involving computers, when necessary DPI will technically analyze computing devices to identify the cause of an incident or to analyze and preserve evidence.

8) Threat/Vulnerability Eradication

After an incident, efforts will focus on identifying, removing and repairing the vulnerability that led to the incident and thoroughly clean the system. To do this, the vulnerability(s) needs to be clearly identified so the incident isn't repeated. The goal is to prepare for the resumption of normal operations with confidence that the initial problem has been fixed.

9) Confirm that Threat/Vulnerability has been Eliminated

After the cause of an incident has been removed or eradicated and data or related information is restored, it is critical to confirm all threats and vulnerabilities have been successfully mitigated and that new threats or vulnerabilities have not been introduced.

10) Resumption of Operations

Resuming operations is a business decision, but it is important to conduct the preceding steps to ensure it is safe to do so.

11) Post-incident Activities

An after-action analysis will be performed for all incidents. The analysis may consist of one or more meetings and/or reports. The purpose of the analysis is to give participants an opportunity to share and document details about the incident and to facilitate lessons learned. The meetings should be held within one week of closing the incident.