FOR OFFICIAL USE ONLY

DPI Data Incident Response Plan

Wisconsin Department of Public Instruction

(July 5, 2013)

FOR OFFICIAL USE ONLY

Document Change History

Version Number	Date	Author	Description
1.1	7/25/2016	Sean Cottrell	Addtl. External Agencies to be notified (FPCO) and (PTAC) [p.9]
1.2	9/1/2016	Sean Cottrell	Add: Legal Contact pg.12; HR Contact pg.13; & Comm. Contact pg.14;

Incident Response Plan

An Incident Response Plan is documented to provide a well-defined, organized approach for handling any potential threat to computers and data, as well as taking appropriate action when the source of the intrusion or incident at a third party is traced back to the organization. The Plan identifies and describes the roles and responsibilities of the Incident Response Team. The Incident Response Team is responsible for putting the plan into action.

Incident Response Team

An Incident Response Team is established to provide a quick, effective and orderly response to computer related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications. The Incident Response Team's mission is to prevent a serious loss of profits, public confidence or information assets by providing an immediate, effective and skillful response to any unexpected event involving computer information systems, networks or databases.

The Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident. The Team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to management and the appropriate authorities as necessary. The Information Technology Management team will coordinate these investigations.

The Incident Response Team will subscribe to various security industry alert services to keep abreast of relevant threats, vulnerabilities or alerts from actual incidents.

Incident Response Team Members

Each of the following areas will have a primary and alternate point of contact:

- Information Technology Management
- DPI Helpdesk
- Information Systems, Security and Infrastructure (ISSI)
- DPI Applications Team
- Internal Auditing

Incident Response Team Roles and Responsibilities

Information Technology Management

- Documents the types of personal information that may have been breached
- Provides guidance throughout the investigation on issues relating to privacy of customer and employee personal information
- Assists in developing appropriate communication to impacted parties

- Assesses the need to change privacy policies, procedures, and/or practices as a result of the breach
- Determines the nature and scope of the incident
- Contacts qualified information security specialists for advice as needed
- Contacts members of the Incident Response Team
- Determines which Incident Response Team members play an active role in the investigation
- Provides proper training on incident handling
- Escalates to executive management as appropriate
- Contacts auxiliary departments as appropriate
- Monitors progress of the investigation
- Ensures evidence gathering, chain of custody, and preservation is appropriate
- Prepares a written summary of the incident and corrective action taken

DPI Helpdesk

- Central point of contact for all computer incidents
- Notifies Information Technology Management to activate computer incident response team

Information Systems, Security and Infrastructure (ISSI)

- Analyzes network traffic for signs of denial of service, distributed denial of service, or other external attacks
- Runs tracing tools such as sniffers, Transmission Control Protocol (TCP) port monitors, and event loggers
- Looks for signs of a firewall breach
- Contacts external Internet service provider for assistance in handling the incident
- Takes action necessary to block traffic from suspected intruder
- Ensures all service packs and patches are current on mission-critical computers
- Ensures backups are in place for all critical systems
- Examines system logs of critical systems for unusual activity

DPI Applications Team

- Monitors DPI applications and services for signs of attack
- Reviews audit logs of mission-critical servers for signs of suspicious activity
- Contacts the Information DPI Helpdesk with any information relating to a suspected breach
- Collects pertinent information regarding the incident at the request of the Information Technology Management Team.

Internal Auditing

- Reviews systems to ensure compliance with information security policy and controls
- Performs appropriate audit test work to ensure mission-critical systems are current with service packs and patches
- Reports any system control gaps to management for corrective action

Incident Response Team Notification

The DPI Helpdesk will be the central point of contact for reporting computer incidents or intrusions. The DPI Helpdesk will notify the Information Technology Management Team of any reported incidents.

All computer security incidents must be reported to the Information Technology Management Team. The Information Technology Management Team will triage the incident and will determine whether Incident Response Team activation is appropriate.

Types of Incidents

There are many types of computer incidents that may require Incident Response Team activation. 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
- Excessive Port Scans
- Firewall Breach
- Virus Outbreak
- Denial of Service / Distributed 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
- Potential violations of Federal, Statewide or DPI's Policies
- Natural disasters and power failures
- Acts related to violence, warfare or terrorism
- Serious wrongdoing
- Other

Breach of Personal Information - Overview

This Incident Response Plan outlines steps our organization will take upon discovery of unauthorized access to sensitive personal information on an individual that could result in harm or inconvenience to the individual such as fraud or identity theft. The affected individual(s) could either be internal or external of DPI.

Personal information is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Most information the organization collects about an individual is likely to be considered personal information if it can be attributed to an individual.

Personally Identifiable Information that can cause harm to an individual or organization is sensitive personally identifiable information and cannot be shared or viewed with anyone unless the person receiving the information has a legitimate purpose to know.

For our purposes, sensitive personally identifiable information is defined as an individual's first name or first initial and last name, in combination with any of the following data:

General Data

- Social Security Number
- Driver's License or State ID Card
- Passport Number
- DNA Profile
- Biometric Identifiers (x-ray, retinal scan fingerprints, etc.)
- Medical Information
- Authentication Information (passwords and information to re-enable passwords)
- Financial Information (bank account, credit / debit card, etc.)
- Sensitive context where personally identifiable information is viewed (queried or reported)

Student Data

- Wisconsin Student Number (WSN)
- Attendance
- Habitual Truancy
- Suspension
- Expulsion
- Dropout
- Course-Taking
- Retention
- Test Results (WKCE, AP, ACT, AA-SwD, ACCESS, etc.)
- Primary Disability Category
- Migrant Status
- Homeless Status
- English Language Proficiency Level
- Educational Environment
- Free and Reduced Lunch Eligibility Status

Definitions of a Security Breach

A security breach is defined as unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by DPI. Good faith acquisition of personal information by DPI personnel for organization purposes is not a breach, provided that the personal information is not used or subject to further unauthorized disclosure.

Requirements

Data owners must identify and document all systems and processes that store or utilize personal information on individuals. Documentation must contain system name, device name, file name, location, database administrator and system administrator (primary and secondary contacts for each). The business area and the IT development group must maintain the contact list of database and system administrators.

Likewise, all authorized users who access or utilize personal information on individuals should be identified and documented. Documentation must contain user name, department, device name (i.e., workstation or server), file name, location, and system administrator (primary and secondary contacts).

Data Owner Responsibilities

Data owners responsible for personal information play an active role in the discovery and reporting of any breach or suspected breach of information on an individual. In addition, they will serve as a liaison between the company and any third party involved with a privacy breach affecting the organization's data.

All data owners must report any suspected or confirmed breach of personal information on individuals to the DPI Helpdesk immediately upon discovery. This includes notification received from any third party service providers or other business partners with whom the organization shares personal information on individuals. The DPI Helpdesk will notify Information Technology Management Team and data owners whenever a breach or suspected breach of personal information on individuals affects their Program Area.

The Information Technology Management Team will determine whether the breach or suspected breach is serious enough to warrant full incident response plan activation (See "Incident Response" section.) The data owner will assist in acquiring information, preserving evidence, and providing additional resources as deemed necessary by Information Technology Management Team, Legal or other Incident Response Team members throughout the investigation.

Program Area Director Responsibilities

Program Area Directors are responsible for ensuring all employees in their unit are aware of policies and procedures for protecting personal information.

If a breach or suspected breach of personal information occurs in their Program Area, the Program Area Director must notify the DPI Helpdesk immediately and open an incident report. (See "Incident Response" Section, DPI Helpdesk).

Note: Education and awareness communication will be directed to all employees informing them of the proper procedures for reporting a suspected breach of personal information on an individual.

When Notification Is Required

The following incidents may require notification to individuals under contractual commitments or applicable laws and regulations:

- A user (employee, contractor, or third-party provider) has obtained unauthorized access to personal information maintained in either paper or electronic form.
- An intruder has broken into database(s) that contain personal information on an individual.
- Computer equipment such as a workstation, laptop, CD-ROM, or other electronic media containing personal information on an individual has been lost or stolen.
- A department or unit has not properly disposed of records containing personal information on an individual.
- A third party service provider has experienced any of the incidents above, affecting the organization's data containing personal information.

Education and Awareness

DPI shall ensure that incident response is addressed in education and awareness programs. The programs shall address proper data privacy, confidentiality, handling, using and security.

Incident Response – Breach of Personal Information

Incident Response Team members must keep accurate notes of all actions taken, by whom, and the exact time and date. Each person involved in the investigation must record his or her own actions.

DPI Helpdesk

Contacts	Office Phone	E-Mail
Primary: DPI Helpdesk **Alternate:**	**608/266-3700**	**helpdesk@dpi.wi.gov**

1. The DPI Helpdesk will serve as a central point of contact for reporting any suspected or confirmed breach of personal information on an individual.

   DPI Helpdesk contact information: 608/266-3700

2. After documenting the facts presented by the caller and verifying that a privacy breach or suspected privacy breach occurred, the DPI Helpdesk will open a Priority Incident Request. This will start the notification process by documenting the incident and notifying the Information Technology Management team.

Information Technology Management Team

Contacts	Office Phone	E-Mail
Primary: Kurt Kiefer	**608-266-2205**	**Kurt.Kiefer@dpi.wi.gov**
Jeff Knutsen	**608-266-3856**	**Jeffrey.Knutsen@dpi.wi.gov**

Dan Retzlaff	**608-267-2285**	**Daniel.Retzlaff@dpi.wi.gov**
Melissa Straw	**608-266-1089**	**Melissa.Straw@dpi.wi.gov**

1. When notified by the DPI Helpdesk, the Information Technology Management team creates the DPI Data Analysis document to record findings, performs a preliminary analysis of the facts and assesses the situation to determine the nature and scope of the incident.

2. Informs the Legal Department that a possible privacy breach has been reported and provides them an overview of the situation.

3. Contacts the individual who reported the problem.

4. Identifies the systems and type(s) of information affected and determines whether the incident could be a breach, or suspected breach of personal information about an individual. Every breach may not require participation of all Incident Response Team members (e.g., if the breach was a result of hard copy disposal or theft, the investigation may not require the involvement of system administrators, the firewall administrator, and other technical support staff).

5. Reviews the preliminary details with the Legal Department.

6. If a privacy breach affecting personal information is confirmed, Incident Response Team activation is warranted. Contact the DPI Helpdesk and advise them to update the Incident Request with “Incident Response Team Activation – Critical Security Problem”.

7. If external communication deems necessary, notify the DPI Communications Department of the details of the investigation and breach. Keep them updated on key findings as the investigation proceeds.

8. The Information Technology Management team is responsible to assign an Incident Response Point of Contact for documenting all details of an incident and facilitating communication to executive management and other auxiliary members as needed.

9. Contact all appropriate database and system administrators to assist in the investigation effort. Direct and coordinate all activities involved with Incident Response Team members in determining the details of the breach.

10. Contact appropriate Incident Response Team members and First-Level Escalation members.

11. Identify and contact the appropriate Data Owner affected by the breach. In coordination with the Legal Department and Data Owner, determine additional notification requirements {e.g., Human Resources, external parties [i.e. Family Policy Compliance Office (FPCO), Privacy Technical Assistance Center (PTAC)]}.

12. If the breach occurred at a third party location, determine if a legal contract exists. Work with the Legal Department and Data Owner to review contract terms and determine next course of action.

13. Work with the appropriate parties to determine the extent of the potential breach. Identify data stored and compromised on all test, development and production systems and the number of individuals at risk.

14. Determine the type of personal information that is at risk.

15. If personal information is involved, have the Data Owner determine who might be affected. Coordinate next steps with the Legal Department and Communications (e.g., individual notification procedures).

16. Determine if an intruder has exported, or deleted any personal information data.

17. Determine where and how the breach occurred.

    - Identify the source of compromise, and the timeframe involved.
    - Review the network to identify all compromised or affected systems. Consider e-commerce third party connections, the internal corporate network, test and production environments, virtual private networks, and modem connections. Look at appropriate system and audit logs for each type of system affected.
    - Document all internet protocol (IP) addresses, operating systems, domain name system names and other pertinent system information.

18. Take measures to contain and control the incident to prevent further unauthorized access to or use of personal information on individuals, including shutting down particular applications or third party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls.

    - Change all applicable passwords for IDs that have access to personal information, including system processes and authorized users. If it is determined that an authorized user's account was compromised and used by the intruder, disable the account.
    - Do not access or alter the compromised system.
    - Do not turn off the compromised machine. Isolate the system from the network (i.e., unplug cable).
    - Change the wireless network Service Set Identifier (SSID) on the access point (AP) and other authorized devices that may be using the corporate wireless network.

19. Monitor systems and the network for signs of continued intruder access.

20. Preserve all system and audit logs and evidence for law enforcement and potential criminal investigations. Ensure that the format and platform used is suitable for review and analysis by a court of law if needed. Document all actions taken, by whom, and the exact time and date. Each employee involved in the investigation must record his or her own actions. Record all forensic tools used in the investigation.

21. If an internal user (authorized or unauthorized employee, contractor, consultant, etc.) was responsible for the breach, contact the appropriate Human Resource Manager for disciplinary

action and possible termination. In the case of contractors, temporaries, or other third-party personnel, ensure discontinuance of the user's service agreement with the company.

DPI Applications Team

Contacts	Office Phone	E-Mail
Primary: Dan Retzlaff (Applications)	**608-267-2285**	**Daniel.Retzlaff@dpi.wi.gov**
Melissa Straw (Warehouse)	**608-266-1089**	**Melissa.Straw@dpi.wi.gov**
Information Systems Security and Infrastructure (ISSI)	**608/266-3700**	**dpidlitissi@dpi.wi.gov**

Notification Steps

1. If the DPI Application Team member hears of or identify a privacy breach, immediately contact the DPI Helpdesk to ensure that the Information Technology Management Team and other primary contacts are notified.

2. The DPI Application Team will assist the Information Technology Management Team as needed in the investigation.

Process Steps

1. When notified by Information Technology Management Team that the privacy breach Incident Response Plan has been activated, perform a preliminary analysis of the facts and assess the situation to determine the nature of incident.

    a. Determine the type of personal information breached.
    b. Determine data sources and method of breach (hardcopy, electronic)
    c. Determine method of breach if possible.
    d. Identify additional resources needed to complete investigation

2. Determine the scope of the breach.
    a. Time Frame
    b. Specific Data Elements
    c. Specific Individuals

3. Take necessary steps to prevent additional compromise of personal information about individuals.

4. Monitor access to application database files to identify and alert any attempts to gain unauthorized access. Review appropriate system and audit logs to see if there were access failures prior to or just following the suspected breach. Other log data should provide information on who touched what file and when. If applicable, review security logs on any non-host device involved (e.g., user workstation).

5. Identify individuals whose information may have been compromised. An assumption could be "all" if an entire table or file was compromised.

6. Secure all files and/or tables that have been the subject of unauthorized access or use to prevent further access.

7. Upon request from the Information Technology Management Team, provide a list of affected individuals, including all available contact information (i.e., address, telephone number, email address, etc.).

8. Report all findings to the Incident Response Plan Team.

Networking

Contacts	Office Phone	E-Mail
Primary: Information Systems Security and Infrastructure (ISSI) **Alternate:**	**608/266-3700**	**dpidlitissi@dpi.wi.gov**

1. When notified by the DPI Helpdesk that the privacy breach Incident Response Plan is activated, provide assistance as determined by the details of the potential breach.

2. Review firewall logs for correlating evidence of unauthorized access.

3. Implement firewall rules as needed to close any exposures identified during the investigation.

Legal

Contacts	Office Phone	E-Mail
Primary: Ryan Nilsestuen **Alternate:**	**608/266-8762**	**Ryan.Nilsestuen@dpi.wi.gov**

Ongoing:

1. Monitor relevant privacy-related legislation, provide input as appropriate, and communicate to our clients the effect that any enacted legislation may have on them.

2. Be cognizant of major contracts which the organization enters that may have an impact or effect on our constituents, districts, employees, and other data.

3. Be aware of other agencies' privacy policies that may affect our organization and affiliates.

When a Privacy Breach Occurs:

1. Coordinate activities between DPI Program Area and other departments (e.g., Human Resources, if necessary).

2. If necessary, notify the appropriate authorities

3. Coordinate with DPI Communications on the timing and content of notification to individuals.

4. If Information Technology Management team determines that the breach warrants law enforcement involvement, any notification to individuals may be delayed if law enforcement determines the notification will impede a criminal investigation. Notification will take place after law enforcement determines that it will not compromise the investigation.

5. Notification to individuals may be delayed until the Information Technology Management team is assured that necessary measures have been taken to determine the scope of the breach and properly investigated.

6. Follow approved procedures for any notice of unauthorized access to personal information about individuals.

7. Notification to individuals should be timely, conspicuous, and delivered in any manner that will ensure the individual receives it. Notice should be consistent with laws and regulations the organization is subject to.

Appropriate delivery methods include:

- Written notice
- Email notice
- Substitute notice
  - Conspicuous posting of the notice on the DPI website.
  - Notification to major media

Items to consider including in notification to individuals:

- A general description of the incident and information to assist individuals in mitigating potential harm, steps individuals can take to obtain and review their credit reports and to file fraud alerts with nationwide credit reporting agencies, and sources of information designed to assist individuals in protecting against identity theft.

- Remind individuals of the need to remain vigilant over the next 12 to 24 months and to promptly report incidents of suspected identity theft.

- Inform each individual about the federal law and state statutes regarding privacy and confidentiality.

Human Resources

Contacts	**Office Phone**	**E-Mail**
Primary: Denise Kohout **Alternate:**	**608/266-0282**	**Denise.Kohout@dpi.wi.gov**

1. If notified of a privacy breach affecting employee personal information, open an incident request with the DPI Helpdesk to document and activate the Incident Response Plan for suspected privacy breach.

2. When notified by the Information Technology Management team that the privacy breach incident response plan has been activated for a breach of information on an individual perform a preliminary analysis of the facts and assess the situation to determine the nature of the incident.

3. Work with the Information Technology Management team and DPI Program Area to identify the extent of the breach.

4. If appropriate, notify the DPI Program Area that a breach has been reported and is under investigation.

5. Work with the DPI Program Area to ensure there is no further exposure to privacy breaches.

6. Work with the Information Technology Management team and Legal Department to determine if the incident warrants further action.

DPI Communications

Contacts	Office Phone	E-Mail
Primary: Thomas McCarthy **Alternate:**	**608/266-3559**	**Thomas.McCarthy@dpi.wi.gov**

Ongoing:

1. Monitor consumer privacy issues and practices of other companies.

2. Monitor consumer privacy breaches of other companies and how they respond.

3. Keep generic/situational talking points current.

When Privacy Breach Occurs:

1. Coordinate with the Information Technology Management team and Legal on the timing, content and method of notification. Prepare and issue press release or statement, if needed.

   Vehicles for communicating include:

   a. News wire services
   b. DPI web site – Post statement on home page or conspicuous location of web site.
   c. DPI Intranet web site – If appropriate for breach of employee information
   d. E-mail
   e. News conference – If privacy breach should reach a national and/or crisis level, coordinate brief news conference at headquarters or appropriate location.
      i. Appoint appropriate spokesperson
      ii. Prepare statement and, if necessary, potential Q & A.
      iii. Coach spokesperson on statement and potential Q & A.
      iv. Invite select media to attend and cover organization’s proactive message.

v. Use conference as a platform for communicating who the breach involves, what the organization is doing to correct breach, how it happened and the organization’s apology but reassurance of its privacy policies

2. Prepare appropriate response to media, individual, and/or employee; and have the Information Technology Management team and Legal Department approve prior to distribution.

3. Proactively respond to media inquiries, if necessary.

4. Monitor media coverage and circulate accordingly.

DPI Program Area

Contacts	**Office Phone**	**E-Mail**
Primary:		

Notification Steps

1. If the DPI Program Area hears of or identify a privacy breach, contact the DPI Helpdesk to ensure that the Information Technology Management Team and other primary contacts are notified.

2. The DPI Program Area will assist the Information Technology Management Team as needed in the investigation.

Terms and Definitions

Asset: Anything that has value to the agency
Control: Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature
Incident: A single or a series of unwanted or unexpected information security events (see definition of "information security event") that result in harm, or pose a significant threat of harm to information assets and require non-routine preventative or corrective action.
Incident Response Plan: Written document that states the approach to addressing and managing incidents, defines organizational structure for incident response, defines roles and responsibilities, and lists the requirements for responding to and reporting incidents.
Incident Response Procedures: Written document(s) of the series of steps taken when responding to incidents.
Incident Response Program: Combination of incident response plan and procedures.
Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, including electronic, paper and verbal communication.
Information Security: Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
Information Security Event: An observable, measurable occurrence in respect to an information asset that is a deviation from normal operations.
Threat: A potential cause of an unwanted incident, which may result in harm to a system or the agency
Program Area Director - Responsible for information security procedure for their respective Program Area, for reducing risk exposure, and for ensuring the Program Area's activities do not introduce undue risk to the enterprise. The director also is responsible for ensuring compliance with DPI enterprise security policies, standards, and security initiatives, and with state and federal regulations.
Incident Response Point of Contact - Responsible for communicating with DPI management and coordinating agency actions in response to an information security incident.
Data Owner - Responsible for creating initial information classification, approving decisions regarding controls and access privileges, performing periodic reclassification, and ensuring regular reviews for value and updates to manage changes to risk.
User - Responsible for complying with the provisions of policies, procedures and practices.

Approval

By: ____
Kurt Kiefer Date
Assistant State Superintendent – Division of Libraries and Technology

By: ____
Name, title Date