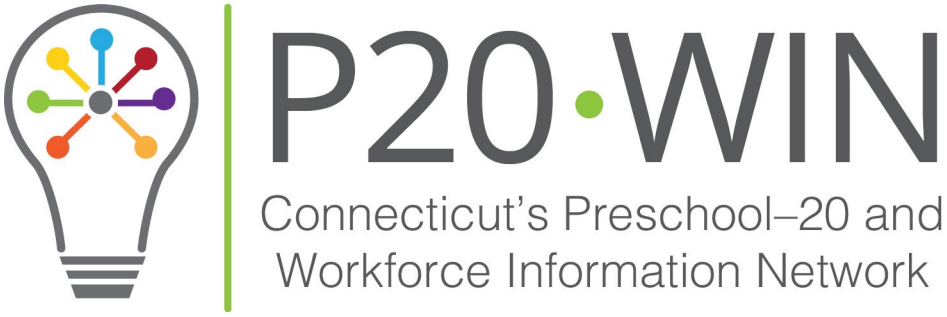
12/1/2022

P20 WIN

Incident Response Plan



State of Connecticut

Release 1.1

Table of Contents

Executive Summary

The P20 WIN Data Governing Board (DGB), as established per C.G.S. 10a-57g, evaluates, approves/rejects, and tracks requests to link data from participating agencies from both internal and external requestors. The DGB does not collect or maintain any data directly but helps facilitate requests to agencies that collect or maintain the data. The DGB has the ability to identify source data stewards and requestors via the P20 WIN request process allowing them to connect interested areas in case of an incident.

This Incident Response Plan covers all information security incidents occurring with P20 WIN data, to include the following:

- Data provided to the Data Integration Hub (the Connecticut Department of Labor (DOL)), as the centralized enterprise Data matching service for P20 WIN with the Participating Agencies,
- Resultant data, the Data provided by the Participating Agencies and the Data Integration Hub to Data Recipients pursuant to a signed Data Sharing Agreement,
- Documents and data related to Data Request Management, the required review and approval process for each Data Sharing request, or otherwise related to the operation of P20 WIN

This plan describes the response for any incident involving P20 WIN data as defined above, otherwise each entity is responsible for their own incident response using their own organizational policies and procedures.

If deemed necessary by the affected agency, the Bureau of Information Technology Solutions (BITS) Information Security team can be engaged via the BITS Help Desk. Other BITS support teams may be engaged by the Security team to assist to identify, recover, and mitigate the incident. This model maximizes the utilization of existing staff in strategic locations through the organizations centrally coordinating the capabilities of the dedicated team to provide a broader understanding of the security threats and activity affecting the constituency. Full management support backs the assigning of needed resources during times of crisis. All requests for BITS support should be made to the BITS Help Desk (860-622-2300).

Definitions

For the purposes of the Incident Response Plan, the following terms have been defined.

1. Access – The ability or the means necessary to read, write, modify delete or communicate data/information or otherwise use any system resource.
2. Agency – any State group identified as an agency or department.
3. Audit – A methodological examination and review of an Agency's implementation of Security Policies and Procedures, including but not limited to FTI, HIPAA, PCI, etc.
4. BITS – Bureau of Information Technology Solutions (central IT agency)
5. Centralized Procedures – Procedures that are developed and administered by the IT Security Unit pertaining to the Federal regulatory compliance and must be implemented by all Agencies.
6. CIO –Chief Information Officer.
7. CISO – Chief Information Security Officer.
8. Data Stewards – Individuals employed by state agencies, who have been given the responsibility for the integrity, accurate reporting, and use of computerized data.
9. Detection and Analysis: First reports of an incident, may come from a customer complaint or report, a monitoring tool such as IDS or log, or other method.
10. DGB – Data Governing Board, as established per C.G.S. 10a-57g ,which establishes data governance policies to enable, improve and sustain the Data Sharing and Data Request processes for P20 WIN
11. Incident Response Manager – The individual who leads the response to the incident, generally from the IT Security Team.
12. Information Security – Administrative, physical and technical controls that seek to maintain confidentiality, integrity and availability of information.
13. Operating Group – Supports the P20 WIN governing bodies for smooth and efficient operation of P20 WIN for the benefit of the participating agencies and the State and residents
14. Risk Analysis – An assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of IT resources.
15. Risk Management – The process of identifying, measuring, controlling and minimizing or eliminating security risks that may negatively affect information systems.
16. Security Incident – The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system.

0. Plan Summary

Incident response occurs in four phases.

1. Preparation: Preparation must be completed before effective response to an incident can occur. Different incident types require different preparation. The Operating Group acts as a communicator and provider of information to participating agencies, through their DGB representatives and to the data recipients using P20 WIN data.

2. Detection and Analysis: First reports of an incident may come from several different sources (i.e., data requestor, agency report, monitoring tools or other methods). During this step the incident is vetted for validity and categorized for type and severity by the DGB members. Preliminary notifications and communications are established. Appropriate response procedures, personnel, and tools are assembled.

3. Containment, Eradication, and Recovery: Based on the results of detection and analysis, the proper response procedure is implemented by the participating agenc(ies). Immediate steps are taken as appropriate to limit loss from the incident and the DGB notifies impacted P20 WIN users. Evidence is preserved. Impact of this containment to customers and the enterprise is communicated to those affected. A long-term resolution of the incident is developed and implemented by the affected participating agenc(ies), with potential assistance from DGB members. This step may include policy alteration or development, system redesign, introduction of new systems or technologies, training, or other actions deemed necessary to permanently resolve an incident. As necessary, systems are restored and brought back online, data is restored, and appropriate parties are notified.

4. Post-Incident Activity: Report of the incident from start to conclusion is finalized. Updated incident response procedures, lessons learned, and documentation of any permanent changes to systems because of the incident, are generated. Incident data collected is analyzed to determine such things as the cost of the incident in money, time, etc. Evidence retention policies and procedures are implemented.

General points about implementing the framework:

1. Communication to appropriate parties will be maintained throughout the incident. Critical communication paths are between response team members, between the response team, whose members will be determined by the DGB representatives for the affected agencies, and P20 WIN Operating Group, between the P20 WIN Operating Group and data recipients, and with the Data Governing Board and Executive Board members. Some of these communication paths may need to be secure. Communication procedures should be developed to be consistent across incident response procedures.

2. All procedures should be available and accessible. This means that all procedures should be maintained through several different methods in case an incident renders one or more methods unavailable. All updates must be communicated to all those who may be involved in a response.

3. The plan will be reviewed annually for updates, and incorporated into documentation and onboarding processes for new agencies and staff.

Preparation Phase

PREPARATION PLANNING

The agencies are responsible for all preparation planning. DGB responsibility in this phase is consulting.

STAFF SUPPORT

Roles:
The DGB, if requested, provides information on agency preparation, prevention, and response to the Data Governing Board representative from BITS as well as notifies interested parties.

INCIDENT PREVENTION

Agencies carry out incident prevention activities, including patch management, training, etc. as part of their ongoing risk assessment and risk management activities. Periodic review of potential risks through a risk assessment and audit process will occur. As a result of this risk assessment and audit process, additional procedures and roles will be identified in the incident management plan.

1. Detection and Analysis

INCIDENT DETECTION

Incidents may be detected by any P20 WIN participating agency, the Operating Group, the BITS IT Security Division or by internal or external data requestors. Once a security incident is identified, it is reported to the Operating Group by email. When possible, email should be sent with 'high priority' status. The Operating Group will then notify the relevant members of the Data Governing Board immediately, and always within 24 hours. The Operating Group will notify and consult with the BITS IT Security Division if BITS-supported agencies are involved in the incident. The affected agencies then identify members to serve on an Incident Response Team. The Incident Response Team should seek to meet within 24 hours of receiving a report of an incident, unless the members determine otherwise. All P20 WIN incidents will be entered into the incident log maintained by the Operating Group at the time they are reported. When known, initial notification should include description of the files and metadata / column headers. Otherwise, OPM will provide any documentation associated with the data request from DOL or participating agencies. Agencies may maintain their own incident logs in addition.

INCIDENT CLASSIFICATIONS

The incident is then classified and prioritized by the incident response team, with representatives from the agencies whose data are involved in the incident.

All incidents for BITS-supported agencies are classified according to the following criteria. An incident may fit into more than one defined type. A 'security incident' can be defined as any security related event that has an actual or potential adverse effect on any computing resource or the data contained therein; or the violation of an explicit or implied security policy.

Incident Types:

Denial of Service: An incident by which authorized access to systems or data is prevented or impaired. Usually a denial of service (DoS) incident is a security event if the DoS is due to malicious intent. Not all events that prevent or hinder authorized access to systems or data are security incidents. The mechanical, electrical, or administrative failure of a system or access mechanism may not be a security incident.

Unauthorized Access: An incident where unauthorized access is attempted or gained to systems or data. This access can be logical or physical in nature. Unauthorized access is any access for which permission has not been granted. Such permissions would include connect, authenticate, read, write, create, delete, modify, etc. This unauthorized access can be by an individual or another system.

Inappropriate Usage: An incident by which acceptable use policies are violated. Acceptable use policies may include what types of data may be accessed or transmitted, how information may be accessed or transmitted, and where information may be received from or transmitted to.

Although references to many other incident types can be found in documentation, they seem to all fall in one of the three categories noted above. For example, malicious code such as a virus or trojan will be first recognized as a denial of service, unauthorized access, or inappropriate usage, depending on the payload of the malicious code. Using these three incident types, responses can be developed to cover any incident that might affect the enterprise.

References:

1. RFC 2350 “Expectations for Security Incident Response” http://www.ietf.org/rfc/rfc2350.txt
2. CERT incident Reporting Guidelines http://www.cert.org/tech_tips/incident_reporting.html#I.A
3. RFC 2196 “Site Security Handbook” http://www.ietf.org/rfc/rfc2196.txt?Number=2196
4. NIST Special Publication 800-61 “Computer Security Incident Handling Guide” http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

INCIDENT SEVERITY

Once the incident is categorized by the incident response team it is prioritized according to its severity level. The appropriate response to an incident is dependent on the severity rating of the incident. It is recommended that business impact for data sources and their elements be flagged in the data dictionary to assist in addressing the incidents.

Method for Determining Severity:

By adding the scores from the following evaluation criteria, a severity rating is established:

1. Potential number of affected parties:
   How much productivity is impacted by this incident?
   1.1. Two or fewer agencies = 1
   1.2. More than 2 but less than half of agencies = 2
   1.3. More than 50% of agencies = 3
2. Probability of widespread escalation:
   Does this incident have the potential to spread to as yet unaffected systems?
   2.1. Minimal = 1
   2.2. Moderate = 2
   2.3. High = 3
3. Commonality:
   Has this occurred in the past; is there experience in mitigating this particular incident?
   3.1. Commonly Seen = 1
   3.2. Occasionally happens = 2
   3.3. Rare = 3
4. Potential for damage or loss[1]
   How expensive is the incident expected to be, both in lost production and in mitigation costs?
   4.1. Minimal = 1
   4.2. Moderate = 2
   4.3. High = 3
5. Business impact[1]
   What is the expected negative impact on the overall health and sustainability of P20 WIN both in short and long-term contexts?
   5.1. Minimal = 1
   5.2. Moderate = 2
   5.3. High = 3, incidents involving certain types of data, due to regulatory and/or legal definitions are always classified as ‘High’. One example would be HIPAA covered Electronic Protected Health Information

This score can be used to determine the severity as follows:

Priority Guideline	Score	Initial Action	Containment Goal
Severity Severe:	13-15	Immediately	ASAP

Severe impact on enterprise			
Severity High: Loss of a major service	11-12	Immediately	<24 Hours
Severity Medium: Some impact some portion of enterprise	8-10	Within 4 hours	<72 Hours
Severity Low: Minor impact on a small portion of enterprise	5-7	Within 24 hours	<7 Days

(1. Reference: SANS Incident Handling and Intrusion detection)

INCIDENT ANALYSIS

All incidents of Medium-level or higher should automatically involve the BITS IT Security Division. Low-level incidents may be addressed by the agencies without direct involvement of the BITS IT Security Division. The BITS IT Security Division coordinates incident analysis at a high level to understand what is occurring across the state and the work with the agency security officers to implement incident response actions required.

The Incident Response Team uses resources through the State to conduct analysis. Tasks such as reviewing logs or monitoring intrusion detection systems can be assigned to distributed team members or handled by the central team. If handled at the local level, the results of these reviews are then shared with the centralized team members in the BITS IT Security Division, who consolidate the data to determine patterns and trends across the organization and identify any additional work or follow-up actions to be passed back to the distributed team members for implementation.

Results of analysis should be archived in an incident folder for daily operations and for future reference by all team members.

2. Containment, Eradication and Recovery

Incident Response support and coordination will primarily be the responsibility of the participating agency or agencies whose data are involved in the incident, through the incident response team. BITS is available to provide support to BITS-supported agencies and for coordination with external agency partners.

3. Post Incident Review

The IT Security Division focuses on analyzing patterns of activity across the enterprise. They support comprehensive tracking, recording, and dissemination of information to the enterprise. By consolidating the information collected, the team is better able to identify similar attacks, artifacts, exploits, trends and patterns. Potential new threats to the enterprise can also be identified. For P20 WIN, incident response will focus on patterns of activity within the LAN and agency applications used for the data sharing process at the Data Integration Hub, the transmittal of data using state-supported tools and incidents involving data released through the data request process. In this model, it is important that the team have expertise or familiarity with the data transmittal and data integration platforms and tools used by P20 WIN participating agencies and data requestors. If this does not exist within the centralized team component, then there must be mechanisms in place to collaborate with the distributed team members or other organizational experts who can provide the required knowledge.

Based on the results of the analysis of any vulnerability or artifact information, the BITS IT Security Division coordinates the release of remediation, detection, and recovery steps throughout the enterprise as required.

Post Incident Activity – The Incident Response Team(s) from the impacted agencies will attend a debriefing meeting and an After-Action Report (AAR) of the incident from start to conclusion is developed which will include an improvement plan. Documentation of any permanent changes to systems as a result of the incident are generated. Incident data collected is analyzed to determine such things as the cost of the incident in money, time, etc. Evidence retention policies and procedures are implemented.

DGB representatives will review the incident data and AAR to determine if other steps or changes are needed to be taken in the data request process, including further review or policy changes by the DGB. Notification of the incident and meeting to review, including recommended steps or changes, will occur within two weeks of the initial report, sooner if warranted by the severity of the incident.

General contacts:

Contacts	Email	Phone
OPM (Operating Group), general email	dapa@ct.gov	860-418-6236
BITS Help Desk	best.helpdesk@ct.gov	860-622-2300
BITS DGB representative	Robert.Barry@ct.gov	860-622-2016

Data Governing Board representatives:

Agency	Email	Phone
BITS	Robert.Barry@ct.gov	860-622-2016
CCEH	pschmitz@cceh.org	630-890-6184
CCIC	widnessj@theccic.org	860-331-3948
CSDE	ajit.gopalakrishnan@ct.gov	860-713-6888
CSCU	Kiehnej@ct.edu	860-723-0236
CSCU	Security@ct.edu	
DCF	fred.north@ct.gov	860-770-8746
DMHAS	michael.girlamo@ct.gov	
DOL	patrick.flaherty@ct.gov	860-263-6281
DSS	susan.smith@ct.gov	860-550-6436
OEC	julie.bisi@ct.gov	
OHE	ram.aberasturia@ct.gov	860-947-1819
OPM	scott.gaul@ct.gov	860-371-5058
UCONN	lauren.jorgensen@uconn.edu	860-486-1904

Flow chart for incident response: