Cybersecurity Incident Response Plan Template v.1

Data Privacy Institute

Cybersecurity Incident Response Plan: TEMPLATE v.1

This document should not be considered legal advice and should not be used in the determination of compliance or adherence to CCPA or CPRA, it is information and intended to be an overview and guide for businesses to use in assisting with compliance efforts. For questions please contact Data Privacy Institute and info@dataprivacyinsitute.org.

www.dataprivacyinstitute.org

INCIDENT MANAGEMENT HANDLING AND RESPONSE

Information Security Policy

Purpose and Scope:

To ensure that a consistent, methodical, and timely incident response process is completed by the designated response personnel after a security incident is believed to have taken place involving ________________ information and information systems. This process will help identify if a systems resource has been compromised, limit the exposure of sensitive data, clean the resource(s), and determine if breach notification is required.

This policy applies to all employees, contractors and vendors, or other persons that have, or may require, access to information and information technology resources at ________________.

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

1.0 DEFINITIONS

Incident - An actual or potential event involving loss or compromise of data or the loss of functionality of an information system or network. Examples include unauthorized access to a PC, data theft, unauthorized data modification, a computer virus, unauthorized network probing, denial of service attacks, and violations of information technology policy, lost or stolen computer equipment and /or intelligent devices.

Event of Interest – Any information system, application or other event data that relates to an incident.

Compromise – A confirmed security incident resulting in harm to the businesses reputation, assets, information or ability to operate.

Breach – A security incident that may result in the acquisition or disclosure of private information to unauthorized parties in accordance to major operating state law as defined in section 4.3 of this policy document.

2.0 ROLES AND RESPONSIBILITIES

Incident Reporter – All persons with access to ________________ information resources or sensitive information are responsible for prompt and accurate notification to ________________ of all suspected incidents. The Incident reporter is responsible for providing complete and accurate detail as possible regarding a suspected incident as well as contact information for use by the Incident Handler and Computer Emergency Response Team.

Incident Handler – Members of ________________ Information Technology or Information Security teams, physical security or third-party Incident Handlers as required that are responsible for implementing incident response procedures, recovery, notification and reporting as detailed within this policy. The Incident Handler may operate alone in confirmation of a suspected incident or as a member of the Computer Emergency Response Team as required.

Computer Emergency Response Team (CERT) –Mitigate and recover compromised systems and data in adherence to response procedures and implement any required incident handling tasks appropriate to their operational role within the CERT.

Computer Emergency Response Team Leader – The Director of Information Technology is responsible for formation and coordination of the Computer Emergency Response Team. The incident team leader is responsible for notifying the Breach Communication Team of breaches and coordination of other communications and resources required by the Computer Emergency Response Team.

Breach Communication Team - The breach communication team consists of the DIRECTOR OF INFORMATION TECHNOLOGY, President and Legal Counsel and is responsible for appropriate breach notification as required by state or regulatory laws in response to a confirmed breach

3.0 INCIDENT NOTIFICATION

Reporting an Information Security Incident

All persons accessing and using ________________ Information Technology resources have a responsibility to immediately report any suspected security incidents to the Director of Information Technology, IT Specialist or to the IT department.

Incident reporters are responsible for providing as much detail as possible regarding the suspected incident when reporting or working with the Incident Handler or Computer Emergency Response Team in response to an incident report. Contact details for the individual reporting the incident must be included in the incident report.

Third-Party Incidents

All third-parties, contractors and vendors in possession of or with access to ________________ information or information technology systems must immediately report all security incidents or breaches affecting ________________information or information systems.

Contact of Authorities

911 should be contacted immediately for any incident that appears an immediate threat to the health, safety or life of an individual.

The Computer Emergency Response Team Leader will work with the Computer Emergency Response Team to liaise with external law enforcement when, and where, necessary. The Breach Communication Team will be responsible for notifying the appropriate state agencies including state law enforcement upon determination of confirmed breach.

4.0 INCIDENT LEVEL DEFINITIONS

Incident level Definitions provide a clear standard of definition to assist with communication and reporting of incidents within ________________ as well as supporting the required decision making needed by response actions during incident handling.

An incident level is defined by the confidence in validity of the suspected incident, potential severity of impact and indicators as to a risk of breach.

Incident handling phases, participants and decision-making scopes of authority may be in part dictated by the Incident Level definition.

4.1 INCIDENT CONFIDENCE LEVELS

Incident Confidence Levels provide differentiation between suspected, confirmed and false incidents.

SUSPECTED

Suspected Incidents have not been confirmed to be valid and are comprised of the incident notification reports, events of interest, monitoring alerts, log files and all other investigation artifacts related to the associated incident.

CONFIRMED

Confirmed Incidents are Suspected Incidents which have been confirmed to involve a loss or compromise of data or the loss of functionality of information system(s), application(s) or business operations.

FALSE

False Incidents are Suspected Incidents which do not involve a loss or compromise of data or the loss of functionality of information system(s), application(s) or business operations.

4.0 INCIDENT LEVEL DEFINITIONS (CONT.)

4.2 INCIDENT IMPACT SEVERITY LEVELS

Incident impact severity levels help communicate the amount of potential damage to _________________ financial and/or operational statuses because of the incident.

MINOR

Minor incidents potentially affect a small portion of employees, information systems, access accounts or data within a subset of _________________ business operation processes and does not greatly impact or impede normal operations of any whole _________________ business operation processes. Personal information impacted by the Breach if indicated, must not exceed 500 records.

MAJOR

Major incidents affect employees, information systems, access accounts or data of an entire _________________ business operations process, or subsets of multiple operational processes such that a portion of _________________ business operations processes cannot operate within normal functions. Personal information impacted by the Breach if indicated, must not exceed 2000 records.

SEVERE

Severe incidents affect most employees, information systems, access accounts or data of _________________ business operations processes and impacts normal operation for a majority of business processes. Personal information impacted by the Breach if indicated, exceeds 2000 records.

4.0 INCIDENT LEVEL DEFINITIONS (CONT.)

4.3 BREACH INDICATOR

A breach indicator is added to the incident level if the compromised applications or information systems are suspected to hold private:

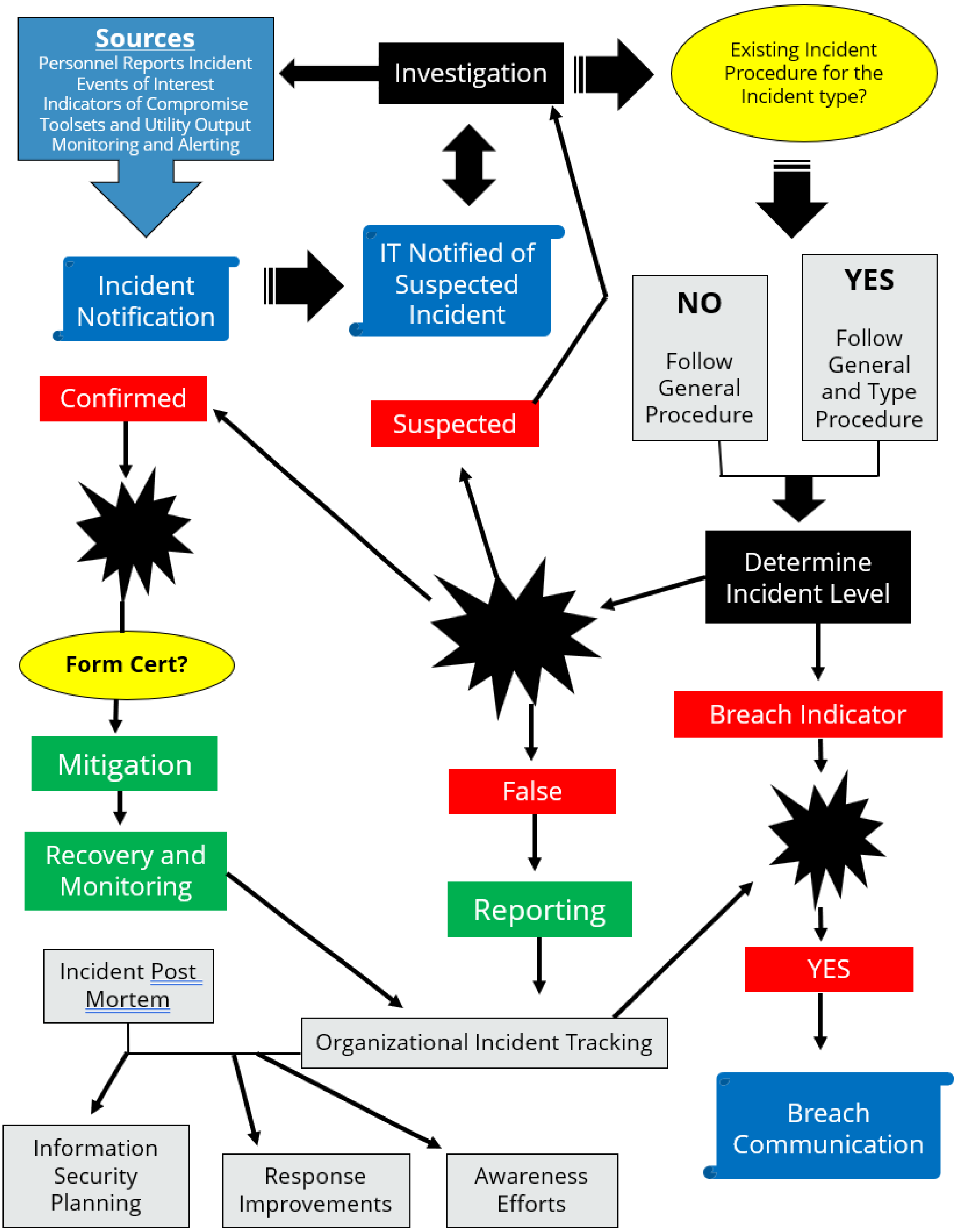
> "Private information" shall mean personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:
>
> - social security number;
> - driver's license number or non-driver identification card number; or
> - account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.
>
> "Private information" does not include publicly available information that is lawfully made available to the public from federal, state, or local government records.

Breach status indication may only be removed if it can be adequately determined and proven that no “Private Information” was acquired by or disclosed to unauthorized parties because of the incident.

5.0 INCIDENT HANDLING PHASES

The following design (5.0a) provides a basic flowchart of incident response actions and phases of handling. This chart is intended as a general overview for reference and may vary given requirements of a specific response scenario. For example, some mitigation steps may be required for specific incident types when the incident level is still defined as “Suspected” and not “Confirmed”. Notification is demonstrated for simplicity as initial incident reporting but extends to incident communication and may be required at additional phases of incident handling between the CERT and ________________ or inter ________________ as appropriate to the incident type and level definition.

5.0a INCIDENT HANDLING PHASES



Sources
Personnel Reports Incident
Events of Interest
Indicators of Compromise
Toolsets and Utility Output
Monitoring and Alerting

Investigation

Existing Incident Procedure for the Incident type?

Incident Notification

IT Notified of Suspected Incident

NO

Follow General Procedure

YES

Follow General and Type Procedure

Confirmed

Suspected

Determine Incident Level

Form Cert?

Mitigation

Recovery and Monitoring

False

Reporting

Breach Indicator

YES

Breach Communication

Incident Post Mortem

Organizational Incident Tracking

Information Security Planning

Response Improvements

Awareness Efforts

5.0 INCIDENT HANDLING PHASES (CONT.)

5.1 DETECTION AND NOTIFICATION

Detection details technologies and methodologies for the collection, review, normalization and alerting required for the effective monitoring of event and system data for indicators of compromise which are indicative of suspected incidents.

Notification of a suspected incident can come from any persons, software monitoring and alerts, anomalous activity or other technical indicators of compromise. Upon notification of a suspected incident an Incident Handler must be assigned to begin investigation into the incident. Notification steps also apply to communication between Incident Handlers, the CERT, and within the _________________. Notification messages during incident handling should maintain a current and accurate incident definition.

5.0 INCIDENT HANDLING PHASES (CONT.)

5.2 INVESTIGATION

Incident investigation is the responsibility of the Incident Handlers operating alone or in conjunction with the CERT. Investigation uses correlation between incident reports, events of interest from log sources or other indicators of compromise along with other available tools to determine an accurate incident definition and aide in determining appropriate actions for mitigation, recovery and reporting.

INCIDENT DEFINITION

The incident definition is comprised of the incident level as defined in section 4 of this policy, the scope of the incident and type. Incident definition may be subject to change during the course of incident handling as investigation may uncover more components of the incident which extends or reduces the scope, level or involved incident types, and it is the job of the Incident Handlers to maintain and communicate appropriate incident definition within all incident handling communication including notifications and reports.

SCOPE

The scope of the incident must be determined by the Incident Handlers and is an inventory of the affected accounts, applications, and information systems, operational processes along with potentially affected data definitions.

TYPE

Incident types are defined by ________________ and specific handling procedures related to the defined incident types developed. The general incident handling procedure provides general guidance for all incidents including matched and unmatched incident types. A specific incident type handling procedure takes precedence when it conflicts with requirements of the general incident handling procedure. Conflicts and deviations are to be clearly noted in type procedures. Some actions may only apply to a specific incident definition such as “Confirmed” or “Severe”, actions within the procedure will be noted to be applicable only within those definitions where required.

5.0 INCIDENT HANDLING PHASES (CONT.)

5.3 MITIGATION

Mitigation actions are the responsibility of the Incident Handlers and CERT and are actions taken to:

- Contain the definition of the incident while investigating incident details
- Remove active threats from the environment as it pertains to the incident following adequate investigation
- Prevent future recurrence of the incident by controlling, removing or remediating used attack vectors

5.4 RECOVERY AND MONITORING

Some incident types may leave information systems or data in non-operable or untrusted states. Recovery tasks are the responsibility of the Incident Handlers and CERT to:

- Restore normal business operations from a failed state
- Restore business data or information systems from an untrusted to trusted state

Additional monitoring actions may be required to be put temporarily into place following an incident to continue monitoring the environment for ongoing indicators of compromise or to confirm and incident has been successfully contained and mitigated.

5.0 INCIDENT HANDLING PHASES (CONT.)

5.5 REPORTING

Incidents and handling actions must be internally tracked and reported to assist in improving incident handling procedures and information security controls. See Appendix A for a sample Cyber Incident Report form. Additionally, there are situations requiring *external* reporting to entities such as Law Enforcement, in cases where criminal activity is suspected or determined. Reporting also pertains to reports required by state authorities and persons whose information has been breached in accordance to relevant state laws.

BREACH COMMUNICATION LAWS

Breach communications will be handled in accordance with State Law for the state of residency of breach victims. Appropriate notification and breach communication actions to required state agencies must be handled at that time in accordance with those laws. Breach communication and handling may vary between states or may be amended by future acts. All relevant laws should be checked at the time of breach to ensure proper breach handling steps are followed.

INCIDENT TRACKING

All incidents along with their definition, investigation actions, mitigation actions and recovery actions should be tracked and reported to ________________ for use in Risk Assessment and Information Security Planning.

INCIDENT POST-MORTEM

All incidents along with their definition, investigation actions, mitigation actions and recovery actions should be reviewed at the end of the incident with the intent to create and improve documented incident response procedures. Output from the post-mortem should also consider required improvements to policy, training, implemented controls or other relevant security planning.

5.0 INCIDENT HANDLING PHASES (CONT.)

5.6 COMPUTER EMERGENCY RESPONSE TEAM (CERT)

At any time, an Incident Handler may determine the incident definition requires additional response resources to effectively mitigate and recover from the incident and must escalate the request to the Computer Emergency Response Team Leader to form a Computer Emergency Response Team (CERT) to assist in incident handling. The CERT will be comprised of all appropriate personnel required to effectively respond to and handle the defined incident. Personnel may be added or removed from the CERT as required during the course of incident handling by the CERT Leader. CERT members may also include third parties aiding in response activities. A CERT must be established along with formation of a Breach Notification Team when the incident definition indicates a breach.

6.0 INCIDENT TYPE HANDLING PROCEDURES

6.1 GENERAL

DETECTION AND NOTIFICATION

The Director of Information Technology must be notified as the CERT Leader of any incident definition when it reaches a breach indicator.

The CERT Leader must notify appropriate personnel on the Breach Communication Team of incident definitions with a breach indicator.

Notification of any mitigation actions that could impact the service availability of information systems which would have an impact to business operation processes must be made to the owner of the business operation and information.

INVESTIGATION

Alerts from all sources will be investigated and coordinated to determine:

- Incident Confidence Levels: Suspected, Confirmed or False
- Incident Impact Severity Levels: Minor, Major or Severe.
- Whether a Breach of Private Information has occurred.
- The scope of the incident – to determine specific targets for detailed further investigation, such as forensic examination or personnel interviews.
- The possible sources of the incident – to help determine the direction of Mitigation

6.0 INCIDENT TYPE HANDLING PROCEDURES (CONT.)

6.1 GENERAL (CONT.)

MITIGATION

Based on the findings of the investigation, mitigations will require the following:

The specific targets that require remediation, for example:

- Physical controls around sensitive areas housing personnel, computing devices, physical or electronic data, or other valuable company assets. These may involve security systems, environmental controls, or the business procedures relating to them.
- Logical controls around Operating Systems, software platforms or applications that may require updates, repairs or replacement.
- Procedural controls related to all the above such as building access, application access, software change management, security awareness training, etc.

The sources of the incident. These may include:

- Burglars or other types of thieves.
- Known malicious websites or attack vectors such as vulnerable system ports, Spam, or other methods of malware infection
- Malicious or Accidental actions by personnel.

In all cases immediate action must be taken to eliminate identified active threats to business operations. These actions may include suspension of processing, physical or logical access, evacuation of staff, confiscation of computer equipment, disconnection of computer equipment from company networks, or other actions necessary to ensure the safety of company personnel, assets and business processes. All activities in Mitigation must be communicated to the CERT Team Leader and documented in the Incident Report.

6.0 INCIDENT TYPE HANDLING PROCEDURES (CONT.)

6.1 GENERAL (CONT.)

RECOVERY AND MONITORING

The Incident Handler, in coordination with the CERT team where necessary, will work to restore normal business operations from a failed state, and to restore business data or information systems from an untrusted to a trusted state. This may involve actions such as the following:

- Recovering data from local or offsite backups
- Restoring or rebuilding workstations or servers from saved images
- Installing Security updates or patches.
- Re-installing application platforms or other types of software
- Run anti-malware software on system to ensure they clean and can be reconnected to the company network.

In addition, any affected systems (or personnel) may require heightened monitoring to ensure the completion of recovery efforts.

REPORTING

Post mortem review of confirmed incidents will include review of incident details with the Information Security Management Committee and Physical security committee as required Improvement to handling procedures will be enacted by the Information Security Committee, Incident Handlers and Computer Emergency Response Team that were involved in the incident. All incident details will be reviewed annually during ________________ at risk assessment to identify improvements to handling procedures or control requirements. Response handling procedures will be updated within this document following each review process that results in requirements to update and improve content of this document.

6.0 INCIDENT TYPE HANDLING PROCEDURES (CONT.)

6.2 MALWARE

Managed anti-virus infection reports and alerts will be reviewed daily by incident handlers for indicators of persistent compromise such as large infection thresholds, recurring infections on the same machines and recurring infections on multiple machines. Out of date definitions will be reviewed daily by incident handlers to ensure anti-virus software is working as effectively as possible. Where possible additional alerting mechanisms for malware activity will be established for the following events and thresholds:

- System Infected
- Greater than 1% of systems experiencing infection within a 24-hour period.
- Greater than 1% of systems experiencing infection within a 72-hour period.
- Greater than 3% of managed systems experiencing infection within a 30-day period.
- Same infection on Same Machine within a 24-hour period
- Same infection on Same Machine within a 7-day period
- Same infection on Same Machine within a 30-day period.
- Same infection on Multiple machines within a 72-hour period.
- Same infection on Multiple machines within a 30-day period
- Virus Definitions Out of Date
- Outbound Connections to Known Command and Control sites.
- Inbound Connections from Known Command and Control sites.
- Web Access filters Malicious Executable Content or Malware Sites
- DNS queries to known malware domains and botnets
- Malformed/Non-DNS Traffic Over DNS

6.0 INCIDENT TYPE HANDLING PROCEDURES (CONT.)

6.2 MALWARE (CONT.)

INVESTIGATION

Execute full anti-virus scans against information systems.

Execute a Malware policy scan against all information systems. Create and include a custom md5 hash of discovered malware files if available. Review output for untrusted and never before seen processes to determine a trust level for processes executing on information systems.

Scan suspected malware executable and files with multi-vendor signature checker.

Check outbound connections for the system and investigate IP address communications and DNS queries for any unknown host communication. Check IP's being communicated with against known command and control and malware sites

Infected files on file shares or shared storage locations should be reviewed for user owner and access properties to determine a source of infection.

Inspect file share connections and turn on access auditing for file shares as required to determine source and scope of potential infection.

Confirmed major malware incident on the file server or other shared storage locations will result in the storage location being taken offline to prevent further spread or infection of crypto virus or other virus types until the infection has been resolved.

6.0 INCIDENT TYPE HANDLING PROCEDURES (CONT.)

6.2 MALWARE (CONT.)

MITIGATION

All accounts logged into the suspected system and owner of the system should assume a potential account compromise event and have the appropriate actions taken as per Access Account Compromise response plan.

Confirmed or suspected major malware incidents on ________________ workstations and laptops will result in the reinstallation and imaging of ________________ workstations and laptops.

RECOVERY AND MONITORING

Malware events will be actively monitored for previously confirmed or suspected infected systems for a period of:

Minor Incident: **7 days**
Major Incident: **30 days**
Severe Incident: **90 days**

REPORTING

Minor malware incidents not involving the compromise of private information will be documented in the ________________ CYBER SECURITY INCIDENT REPORT (Appendix A.) Major and Severe malware events, or those involving the breach of private information, must also be reported to the Director of Information Technology. As CERT Team leader, the Director of IT may convene the CERT team for more comprehensive Incident Response, as well as initiate Breach Handling procedures where necessary.

6.0 INCIDENT TYPE HANDLING PROCEDURES (CONT.)

6.3 SOCIAL ENGINEERING

DETECTION AND NOTIFICATION

The Director of Information Technology must be notified of social engineering attacks and is responsible for delegation of company-wide notification regarding social engineering attack details.

Suspected malicious email is to be forwarded by the incident reporter.

INVESTIGATION

Review email headers and email content in attached email.
Review destinations of links and content present within the email.
Scan suspected malicious attachments through VirusTotal.com

If interaction with infected content is suspected, review workstation for any unknown active processes and connections to external IP addresses, and treat as potential malware type response.

MITIGATION

Company-wide notification will be made to all employees regarding details of the attempted social engineering attack.

Suspected or confirmed account or malware compromises should be treated by the appropriate incident type.

Awareness training and social engineering exercises to maintain awareness will be performed periodically against internal personnel.

6.0 INCIDENT TYPE HANDLING PROCEDURES (CONT.)

6.3 SOCIAL ENGINEERING (CONT.)

RECOVERY AND MONITORING

This should follow requirements of the appropriate incident type(s).

REPORTING

In addition to the company-wide notification cited above, the incident will be documented in the _________________ CYBER SECURITY INCIDENT REPORT (Appendix A.) Other reporting requirements should follow the requirements of the appropriate incident type(s).

6.0 INCIDENT TYPE HANDLING PROCEDURES (CONT.)

6.4 ACCESS ACCOUNT COMPROMISE

DETECTION AND NOTIFICATION

Notification by the Incident Handler must be made to employees whose accounts have been reset while mitigating an incident. Notification should first be attempted but may be made after the account has been reset, such that notification does not impede the need to contain the incident definition.

Event Alerts will be created for the following events and indicated thresholds and sent to the incident reporter where they will be investigated as appropriate to the level of indicator of compromise.

- Threshold for failed login attempts within a set time period.
- Login attempts to remotely accessible services from known malicious IP
- Login attempts to remotely accessible services from foreign Countries
- Login attempts to remotely accessible services outside of normal business hours
- Failed login attempts to internal information systems by invalid accounts
- Failed login attempts to internal information systems by valid accounts
- Successful and Failed logins for administrative and privileged users.
- Successful and Failed logins for all third-party service provider access accounts.

6.0 INCIDENT TYPE HANDLING PROCEDURES (CONT.)

6.4 ACCESS ACCOUNT COMPROMISE (CONT.)

INVESTIGATION

Determine if any active source of compromised connections made by suspected compromised accounts by reviewing access to public facing and internal information systems.

MITIGATION

An Incident Handler may revoke access to the network for suspected accounts. Any accounts affected by the incident must have their passwords changed immediately by the Incident Handler.

RECOVERY AND MONITORING

Access to VPN and other available access logs will monitor and alert on failed or successful thresholds or suspicious access attempts made by suspected and confirmed compromised accounts for a period of 30 days post incident mitigation

REPORTING

In addition to the notification to individuals cited above, the incident will be documented in the ________________ CYBER SECURITY INCIDENT REPORT (Appendix A.) Other reporting requirements should follow the requirements of the appropriate incident type(s).

6.0 INCIDENT TYPE HANDLING PROCEDURES (CONT.)

6.5 LOST OR STOLEN DEVICE

DETECTION AND NOTIFICATION

The IT department must be notified of any planned device upgrade or change.

INVESTIGATION

Incident handlers will assist personnel in attempting to locate the device through the appropriate mobile device utilities.

Physical surveillance cameras will be reviewed where possible for identification of perpetrators of physical theft from ________________ office locations.

If the device is believed to contain personal information, the Director of Information Technology must be notified and, if necessary, Breach Handling procedures must be initiated.

MITIGATION

If a device is suspected or confirmed to be lost or stolen and reasonable measure has been taken to locate the device, Incident Handlers will remote wipe the device and remove the device association from ActiveSync.

Phones with company data must be factory defaulted before trade in.

Suspected and confirmed stolen devices are to have an appropriate police report filed with authorities.

Accounts associated to the device are to be treated as suspected account compromise incident type and response plans for the account(s) followed accordingly.

6.0 INCIDENT TYPE HANDLING PROCEDURES (CONT.)

6.5 LOST OR STOLEN DEVICE (CONT.)

RECOVERY AND MONITORING

A list of ActiveSync connected devices will be generated and reviewed by incident handlers periodically and inactive or multiple mobile devices beyond three devices will be disassociated from ________________ActiveSync and other resources.

REPORTING

The incident will be documented in the ________________ CYBER SECURITY INCIDENT REPORT (Appendix A.) If the device appears to have contained customer private information, the Director of Information Technology must initiate Breach Handling procedures, which have additional reporting requirements.

6.0 INCIDENT TYPE HANDLING PROCEDURES (CONT.)

6.6 POLICY VIOLATION

Policy violations must also be regarded as Security Incidents, although the methods of Detection, Investigation, Mitigation, Recovery and Reporting will be different. Although policy violations *may* lead to more IT-related incidents, they are primarily a Human Resources (HR) concern, which explains the difference in Response methodology.

DETECTION AND NOTIFICATION

As with all incidents, any user of _______________ systems should report suspicion or discovery of a policy violation to their company manager, the IT department, or HR. Ultimately, policy violations, if confirmed, are disciplinary issues that should involve HR.

INVESTIGATION

The investigation will still involve the assignment of an IT incident handler. If the matter involves HR, then the incident handler will work with the department to perform a *forensic* investigation to help gather evidence to confirm the incident, and aid in the determination of appropriate disciplinary action. It is likely creation of a forensic image of the suspected violators hard drive will need to be created to ensure no actual files on the hard drive are modified during the investigation. Each step of the forensic investigation must be carefully documented to properly support any disciplinary proceeding that may arise from the investigation results.

6.0 INCIDENT TYPE HANDLING PROCEDURES (CONT.)

6.6 POLICY VIOLATION (CONT.)

MITIGATION

If there is suspicion or confirmation of a malware infection on the device or devices involved (e.g. due to an acceptable use violation,) then the related devices must be removed from the network until the investigation is concluded. At that time, the normal mitigation steps for a malware infection incident type should be followed before the device(s) returns to use.

Accounts associated to the device are to be treated as suspected account compromise incident type and response plans for the account(s) followed accordingly.

RECOVERY AND MONITORING

Depending on the outcome of the investigation, HR may require close monitoring of the computer activity of the individual(s) involved.

REPORTING

The incident report for this type of investigation must very thoroughly document all the steps taken. This report must be delivered to HR, and their procedures will govern the confidentiality of the information, and any further distribution of the report.

7.0 VIOLATIONS AND SANCTIONS

The Director of Information Technology will administer this policy, including the review of reported violations and the recommendation of appropriate actions.

Violation of the policies detailed within this document could result in disciplinary actions up to and including termination with legal prosecution.

8.0 DOCUMENT CONTROL

Version	*Date*	*Comments*
v.1	12/15/22	Initial Publication
v.2	TBD	N/A

Data Privacy Institute

CYBERSecurity Incident Report

Date: ____________________

Time: ____________________

Reported by: ____________________

Description:

____

____

____

____

____

____

____

____

____

____

Suspected □ Confirmed □ False □

Minor □ Major □ Severe □

Breach Indicator □

Incident Handler(s): ____

____

____

CERT Convened? ______

CERT Members: ____

____

____

____

CYBERSecurity Incident Report

INCIDENT RESPONSE

Investigation:

____

____

____

____

____

Mitigation:

____

____

____

____

____

Recovery and Monitoring:

____

____

____

____

____

Reporting:

____

____

____

____

____