Hawaii Office of Homeland Security
Cyber Incident Handling and Response Plan
Information Security Policy

Incident Quick-Links

If you are handling an active incident, use the below links to quickly jump to commonly required guidance contained throughout this document.

Executive Summary

Purpose and Scope

To limit the overall impact of a cyber-security event, appropriate and timely response actions must be taken by Hawaii Office of Homeland Security hereinafter, "OHS." OHS has established this plan to provide consistent, standard guidance, and to ensure a timely process is followed by designated personnel in response to cyber-security attacks.

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

Using this Document

This document is intended to be read and understood by all OHS personnel who are assigned responsibilities within response roles as defined in Section 1: Roles and responsibilities, with exception to "Incident Reporters", which account for all persons accessing information resources. These persons should all receive regular awareness training on the expectations of their role when dealing with a potential incident.

Section 1: Incident Handling Procedures

This section contains full details procedural tables for handling of each incident type. Procedures describe actions to be taken by responsible parties or Entity/Organizational seniors throughout each phase of response, in response to various incident definitions or other triggers.

This section is broken into several parts.

1.1 "Incident Reporting" establishes global policies defining how notification of a suspected or ongoing incident should be made to response personnel with the OHS. All persons with access to the OHS's information resources should be regularly informed and trained on how to appropriately report an incident.

Go to Incident Reporting **(Page: xx)**

1.2 "Contact Directory" provides a contact tree of response personnel, by position and name, along with methods for establishing contact.

Go to Contact Directory **(Page: xx)**

1.3 Response Role Quick Tables provides a quick entry point by response role to examine procedures applicable to your responder role during an incident.

Go to Incident Response Roles Table **(Page: xx)**

1.4 General Response Procedures are applicable globally to all incident types. This includes incidents without a currently defined type. These procedures should be enacted with all incidents meeting the trigger criteria for the procedure except in cases where conflicting guidance is given in a procedure matching the appropriate type.

1.5 and Above outline procedures to be followed with specific incident types. If there is a conflict with guidance in 1.4 General Response Procedures, this guidance takes precedence. Otherwise, guidance in 1.4 General Response

Procedures should be followed in conjunction with the procedures outlined in the specific incident type definition. Procedural tables may provide link and reference to other relevant incident type or general procedures which are intended to be followed.

Procedural sections may include a visual diagram describing the procedure and its participants. In addition to the diagram, a table of procedures contained within the section, along with the response phase and triggers to enact these procedures. The target audience shown in the response procedure overview table is a combination of all responsible parties within the procedure. Links to each specific procedure are provided in this table.

Go to Incident Handling Procedures **(Page: xx)**

Section 2: Roles and Responsibilities
Definitions of roles and their general responsibilities during a cyber incident.

Appendix A: Definitions
Common definition for cyber-security terms. All definitions in this document are based upon NIST and other accepted standards to ensure consistency of the lexicon and response procedures.

Appendix B: Incident Definitions
Establishes common language by which incidents will be defined and communicated. Understanding incident definitions is important as different definitions may be used to trigger different response actions. Details related to communication of the incident are relevant to all possible incident responders, persons in response leadership roles, and participants on post-mortem teams.

Appendix C: Incident Handling Phases
Defines the overall phases of response, establishing expectations of activity for each phase. This allows for categorical understanding of what activity is required at various times during response and to ensure all phases of activity are considered and accounted for during planning and handling execution. All incident handlers should have a general understanding of response phase definitions.

Appendix D: Breach Handling
Global summary and policy definitions for considerations related to handling of cyber-security breaches in accordance with relevant breach laws. This content should be understood by legal, leadership and incident response teams.

Go to Breach Handling **(Page: xx)**

Appendix F: Cyber Incident Report
A cyber incident report must be filed in accordance with general procedures following any incident of major severity or above. Reports should be filed on all incidents, regardless of definition, when the incident handling team determines a post-mortem review of the event be materially beneficial to cyber-security risk management and decision making.

Go to Cyber Incident Report **(Page: xx)**

Appendix G: Incident After-Action Report
This template is designed for post-mortem review of an incident as well as tracking progress towards post-incident actions and security evolution/lessons learned. This form provides a process focused on identification and resolution of root cause problems leading to the incident.

Go to Post-Mortem After-Action Report **(Page: xx)**

Appendix H: Communications Template
Templates for written communications and notices required during incident management.

Go to Communication Templates **(Page: xx)**

Document Governance

The OHS IT Security Manager, along with the IT Director/CISO, will administer this document, including the review of reported violations of policy contained within. This document will serve as the primary tool for conducting incident post-mortem and annual incident response tabletop exercises. The IT Security Manager, with support from the IT Director, will be responsible for reviewing the content of this document and conducting regular exercises to identify improvements to response activities. The IT Security Manager will be responsible for regularly updating response procedures to reflect changes to response activity and ensuring all persons holding response roles are regularly and adequately trained in the appropriate response actions for their roles.

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

Contents

1: INCIDENT HANDLING PROCEDURES

1.1: INCIDENT REPORTING

Reporting an Information Security Incident

All persons accessing and using the OHS's Information Technology resources have a responsibility to immediately report any possible security incidents.

All suspected incidents outside of the normal hours of operations (07:00 – 20:00 EST with Exception to Holidays) must be reported to the IT Help Desk

IT Help Desk
INSERT EMAIL/PHONE HERE

Outside normal hours of operations, report potential cyber incidents to the communications center

INSERT PHONE NUMBERS HERE

Emergency Contact of Authorities

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

Coordination with Law Enforcement Agencies

The IT Security Manager will oversee coordination with external law enforcement agencies when, and where, necessary. The IT Security Manager, either directly or as directed through cyber resources within the EOC or operations center, will be responsible for notifying the appropriate federal and/or state agencies including law enforcement when appropriate upon determination of confirmed breach. The IT Security Manager will report and coordinate with Federal and/or State Cyber-security Agencies for all incidents of level 3 or greater severity.

Reference: 1.2 Contact Directory.

1.2 Contact Directory

Organization	Contact Role	Contact Information	Contact Condition (s)
OHS	IT Security Manager	INSERT NAME & EMAIL/PHONE HERE	Primary incident handler
OHS	IT Director	INSERT NAME & EMAIL/PHONE HERE	Primary incident handler
OHS	Tier 1 Support	INSERT NAME & EMAIL/PHONE HERE	Report cyber incident during normal hours of operations. 07:00 – 20:00 EST with Exception to Holidays
OHS	Communications Center	INSERT NAME & EMAIL/PHONE HERE	Report potential cyber incident outside of normal operating hours.
OHS	Public Information Officer	INSERT NAME & EMAIL/PHONE HERE	Notification is required to the public as a result of an incident.
OHS	Legal Counsel	INSERT NAME & EMAIL/PHONE HERE	Legal support is required for communications or actions taken during incident management.
OHS	Security	INSERT NAME & EMAIL/PHONE HERE	Executive support for incident management decisions and emergency budget.
OHS	Finance Director	INSERT NAME & EMAIL/PHONE HERE	Executive support for incident management budget, emergency, and non-emergency.
OHS	Department of Administration	INSERT NAME & EMAIL/PHONE HERE	Non-emergency submission of incident management budget requests.
Hawai'i	Risk Manager	INSERT NAME & EMAIL/PHONE HERE	Support in coordination with cyber insurer.
Specialty Insurance Company	Cyber Insurer	SELF INSURED [OR PROVIDE INFORMATION OF PROVIDER] Emergency: **1-800-XXX-XXXX**	Filing a claim or engaging with support services.

		Non-Emergency: Hyperlink to insurance carrier **Policy Number:**	
Federal	FBI	INSERT NAME & EMAIL/PHONE HERE	Determination of impact to criminal investigations is required prior to making notice of an event. Assistance in forensic evidence collection is required.
MS-ISAC	The MS-ISAC Security Operations Center (SOC)	866-787-4722 soc@msisac.org	Investigative and monitoring support regarding Albert events and network communication traffic is required. Must report events of level 3 or greater severity, may report events of level 2 or less severity.
Hawai'i	Hawai'i Department of Law Enforcement	INSERT NAME & EMAIL/PHONE HERE	Determination of impact to criminal investigations is required prior to making notice of an event. Assistance in forensic evidence collection is required.
Hawai'i	Cybercrime Office Department of Law	INSERT NAME & EMAIL/PHONE HERE	Must report events of level 3 or greater severity, may report events of level 2 or less severity.
Hawai'i	Hawai'i Digital Services	INSERT NAME & EMAIL/PHONE HERE	
Hawai'i	Department of Legal Affairs	INSERT NAME & EMAIL/PHONE HERE	Breach of personal information as defined by 501.171 Security of confidential personal information.

Transunion	Major Consumer Reporting Agency	Transunion Data Breach Reporting Hotline https://thirdpartyissue.webline.saiglobal.com/ 1-800-680-7289 www.transunion.com.	Notice required in cases of breaches of over 1,000 records of personal information as defined by 501.171 Security of confidential personal information.
Experian	Major Consumer Reporting Agency	Data Breach Support 1-866-751-1323 www.experian.com/fraud	Notice required in cases of breaches of over 1,000 records of personal information as defined by 501.171 Security of confidential personal information.
Equifax	Major Consumer Reporting Agency	1-800-525-6285 www.equifax.com	Notice required in cases of breaches of over 1,000 records of personal information as defined by 501.171 Security of confidential personal information.
Municipal and Cities Cyber Security Incident Reporting	Outside agencies report to OHS	INSERT NAME & EMAIL/PHONE HERE	282.3185(5)(b)1. Local Government and Municipal Cyber-security issue(s) as defined by 1.4.10 Notification by Local Governments to Sate Cyber-security Agencies

1.3 Response Role Quick Tables

These tables provide a brief outline of the procedural tasks required to be performed by each role with links to relevant procedures.

1.3.1 Incident Reporter (All)

Procedure	Phase	Triggers
General		
1.4.7 Internal Incident Reporting	Detection and Notification	Notice or suspicion of a cyber incident.
Malware		
1.5.3 Initial Personnel Response	Mitigation	Presented with a ransomware or other suspicious pop-up box. Otherwise, suspect or confirm the presence of malware on a system.

1.3.2 Incident Handlers

Procedure	Phase	Triggers
General		
1.4.13 Breach Handling	Detection and Notification	A breach of data as defined by state breach law is suspected.
1.4.14 General Investigation	Investigation	Response to Alerts and incident reports and indicators of compromise
14.19 Mitigation of Potentially Compromised Accounts	Mitigation	Investigation of events determines potential impact of access credentials
1.4.25 System Recovery	Recovery and Monitoring	System is untrusted or unrecoverable following a cyber event
1.4.28 Incident Tracking	Reporting	Throughout Incident Lifecycle
Malware		
1.5.2 Malware Investigation	Investigation	System suspected to be actively infected with malware.
1.5.4 Isolate Affected Systems	Mitigation	Suspect or confirm the presence of active malware on a system
1.5.5 Isolate Affected Networks	Mitigation	Review of malicious activity trends, or notification of active events involving command and control servers or other inbound/outbound malicious communications.

1.5.6 Ransomware	Mitigation	A ransomware incident occurs.

1.3.3 IT Security Manager

Procedure	Phase	Triggers
General		
1.4.1 Configuration of Logs, Alerts and Cyber-security Reports	Pre-Incident	Configuration of alerting and report sources
1.4.2 Coordination with MSISAC	Pre-Incident	Pre-Incident
1.4.3 Co-ordination with Law Enforcement	Pre-Incident	Pre-Incident
1.4.4 Coordination with Communications Center	Pre-Incident	Pre-Incident
1.4.5 Coordination with Third-Party Agents	Pre-Incident	Pre-Incident
1.4.8 Notification to Personnel	Detection and Notification	Cyber event causes a disruption requiring notice to personnel.
1.4.9 Notification to the Public	Detection and Notification	Cyber event causing disruption or breach of information requires notice be made to the public.
1.4.10 Notification by Local Governments to Sate Cyber-security Agencies	Detection and Notification	Ransomware or Cyber-security Incident
1.4.11 Notification to Authorities Resulting from Breach	Detection and Notification	Information breach defined by state breach laws require notice made to state authorities
1.4.13 Breach Handling	Detection and Notification	A breach of data as defined by state breach law is suspected.
1.4.14 General Investigation	Investigation	Response to Alerts and incident reports and indicators of compromise
1.4.15 Formation of IRT	Investigation	Response to an event requires additional resources beyond initial incident handler capabilities.
1.4.16 Coordination of Criminal Investigation	Investigation	Suspected criminal activity, or event requiring notice to the public.
1.4.17 Forensic Collection of Evidence	Investigation	Forensic evidence related to an event needs to be collected.
1.4.18 Escalation with MSISAC	Investigation	Additional technical support is required for investigation of an event. Albert alerts, network communications logs or aid with monitoring for indicators of compromise during and event
1.4.19 Mitigation of Insecure User Activities	Mitigation	Monitoring/review of events, logs and alert heuristics indicate events generated due to insecure user activities.

1.4.21 Executive Sponsorship for Incident Management Activities	Mitigation	Enlisted for decision and resource support from Incident Handlers/IRT Leaders
1.4.22 Emergency Incident Expense Approval	Mitigation	Level 3 or greater event requiring emergency financial investment to mitigate impact or recover
1.4.23 Monitoring	Recovery and Monitoring	General Monitoring
1.4.24 Weekly Cyber Event Data Review	Recovery and Monitoring	Weekly
1.4.26 Handling of Reported Cyber Events	Reporting	A breach at a government agency within jurisdiction is reported to the OHS.
1.4.27 Handling of Breach Related Artifacts	Reporting	Throughout Breach Incident Lifecycle.
1.4.28 Incident Tracking	Reporting	Throughout Incident Lifecycle
1.4.29 Incident Post-Mortem	Reporting	Resolved incident, submission of incident report. Within three days of close of incident.
Malware		
1.5.6 Ransomware	Mitigation	A ransomware incident occurs.

1.3.4 IT Director

Procedure	Phase	Triggers
General		
1.4.1 Configuration of Logs, Alerts and Cyber-security Reports	Pre-Incident	Configuration of alerting and report sources
1.4.6 Ticket System Configuration	Pre-Incident	Pre-Incident
1.4.14 General Investigation	Investigation	Response to Alerts and incident reports and indicators of compromise
1.4.15 Formation of IRT	Investigation	Response to an event requires additional resources beyond initial incident handlers
1.4.23 Monitoring	Recovery and Monitoring	General Monitoring
1.4.29 Incident Post-Mortem	Reporting	Resolved incident, submission of incident report. Within three days of close of incident.

1.3.5 Communications Center

Procedure	Phase	Triggers
General		
1.4.7 Internal Incident Reporting	Detection and Notification	Notice or suspicion of a cyber incident.

1.3.6 Support Manager

Procedure	Phase	Triggers
Malware		
1.5.3 Initial Personnel Response	Mitigation	Incident report received.

1.3.7 Field Technician

Procedure	Phase	Triggers
Malware		
1.5.3 Initial Personnel Response	Mitigation	Assigned to retrieval of affected workstation.

1.3.8 Risk Manager

Procedure	Phase	Triggers
General		
1.4.9 Notification to the Public	Detection and Notification	Cyber event causing disruption or breach of information requires notice be made to the public.
1.4,11 Notification to Insurer	Detection and Notification	An insurance claim needs to filed, or vendors used to support response of an incident where a claim will be filed need to be approved by the insurer.
1.4.13 Breach Handling	Detection and Notification	A breach of data as defined by state breach law is suspected.
1.4.15 Formation of IRT	Investigation	Response to an event requires additional resources beyond initial incident handlers

1.3.9 Legal Counsel

Procedure	Phase	Triggers
General		
1.4.8 Notification to Personnel	Detection and Notification	Request made by Incident Response Team for legal support in communications content or response actions
1.4.9 Notification to the Public	Detection and Notification	Request made by Incident Response Team for legal support in communications content or response actions
1.4.11 Notification to Authorities Resulting from Breach	Detection and Notification	Request made by Incident Response Team for legal support in communications content or response actions
1.4.13 Breach Handling	Detection and Notification	Request made by Incident Response Team for legal support in communications content or response actions
1.4.15 Formation of IRT	Investigation	Request made by Incident Response Team for legal support in communications content or response actions

1.3.10 Public Information Officer

Procedure	Phase	Triggers
General		
1.4.9 Notification to the Public	Detection and Notification	Communications required to the public.
1.4.13 Breach Handling	Detection and Notification	Communications required to the public

1.3.11 Access Account Holders

Procedure	Phase	Triggers
General		
14.19 Mitigation of Potentially Compromised Accounts	Mitigation	Investigation of events determines potential impact of access credentials

		Potential for account compromise extends to use of third-party or cloud applications outside of the OHS IT Department administration.

1.3.12 Finance Director

Procedure	Phase	Triggers
General		
1.4.21 Executive Sponsorship for Incident Management Activities	Mitigation	Enlisted for decision and resource support from Incident Handlers/IRT Leaders
1.4.22 Emergency Incident Expense Approval	Mitigation	Level 3 or greater event requiring emergency financial investment to mitigate impact or recover

1.3.13 Department of Administration

Procedure	Phase	Triggers
General		
1.4.21 Executive Sponsorship for Incident Management Activities	Mitigation	Enlisted for decision and resource support from Incident Handlers/IRT Leaders

1.3.14 Post-Mortem Team

Procedure	Phase	Triggers
General		
1.4.29 Incident Post-Mortem	Reporting	Resolved incident, submission of incident report. Within three days of close of incident.

1.3.15 IT Technician

Procedure	Phase	Triggers
General		
1.5.1 Endpoint Agent Configuration	Pre-Incident	New workstation or server is deployed.

Malware		
1.4.1 Configuration of Logs, Alerts and Cyber-security Reports	Pre-Incident	Configuration of alerting and report sources

1.4: General Incident Handling Procedures

Procedure	Phase	Triggers	Audience	Notes
1.4.1 Configuration of Logs, Alerts and Cyber-security Reports	Pre-Incident	Configuration of alerting and report sources	♦ IT Director ♦ IT Security Manager ♦ IT Technician	
1.4.2 Coordination with MSISAC	Pre-Incident	Pre-Incident	IT Security Manager	
1.4.3 Co-ordination with Law Enforcement	Pre-Incident	Pre-Incident	IT Security Manager	
1.4.4 Coordination with Communications Center	Pre-Incident	Pre-Incident	IT Security Manager	
1.4.5 Coordination with Third-Party Agents	Pre-Incident	Pre-Incident	IT Security Manager	
1.4.6 Ticket System Configuration	Pre-Incident	Pre-Incident	IT Director	
1.4.7 Internal Incident Reporting	Detection and Notification	Notice or suspicion of a cyber incident.	♦ Incident Reporters (All) ♦ Communications Center	Incorporate regular awareness training content. Communications center requires training on initial response actions and triage of potential event severity for reported incidents.
1.4.8 Notification to Personnel	Detection and Notification	Cyber event causes a disruption requiring notice to personnel.	♦ IT Security Manager ♦ Legal Counsel	Rule out suspicions of criminal activity or active investigation prior to giving notice. (1.4.16 Coordination of Criminal Investigation)
1.4.9 Notification to the Public	Detection and Notification	Cyber event causing disruption or breach of information requires notice be made to the public.	♦ IT Security Manager ♦ Risk Manager ♦ Public Information Officer (PIO) ♦ Legal Counsel	Rule out suspicions of criminal activity or active investigation prior to giving notice. (1.4.16 Coordination of

				Criminal Investigation)
1.4.10 Notification by Local Governments to Sate Cyber-security Agencies	Detection and Notification	Ransomware or Cyber-security Incident	IT Security Manager	Required for Compliance to Local Government Cyber-security Act
1.4.11 Notification to Authorities Resulting from Breach	Detection and Notification	Information breach defined by state breach laws require notice made to state authorities	♦ IT Security Manager ♦ Legal Counsel	
1.4,11 Notification to Insurer	Detection and Notification	An insurance claim needs to filed, or vendors used to support response of an incident where a claim will be filed need to be approved by the insurer.	Risk Manager	
1.4.13 Breach Handling	Detection and Notification	A breach of data as defined by state breach law is suspected.	♦ Incident Handlers ♦ IT Security Manager ♦ Risk Manager ♦ Legal Counsel ♦ Public Information Officer	
1.4.14 General Investigation	Investigation	Response to Alerts and incident reports and indicators of compromise	♦ IT Security Manager ♦ IT Director ♦ Incident Handlers	
1.4.15 Formation of IRT	Investigation	Response to an event requires additional resources beyond initial incident handlers	♦ IT Security Manager ♦ IT Director ♦ Risk Manager ♦ Legal Counsel	
1.4.16 Coordination of Criminal Investigation	Investigation	Suspected criminal activity, or event requiring notice to the public.	IT Security Manager	
1.4.17 Forensic Collection of Evidence	Investigation	Forensic evidence related to an event needs to be collected.	IT Security Manager	
1.4.18 Escalation with MSISAC	Investigation	Additional technical support is required for investigation of an event. Albert alerts, network communications logs or aid with monitoring for indicators of compromise during and event	IT Security Manager	
1.4.19 Mitigation of Insecure User Activities	Mitigation	Monitoring/review of events, logs and alert heuristics indicate events	IT Security Manager	

		generated due to insecure user activities.		
14.19 Mitigation of Potentially Compromised Accounts	Mitigation	Investigation of events determines potential impact of access credentials Potential for account compromise extends to use of third-party or cloud applications outside of the OHS IT Department administration.	♦ Incident Handlers ♦ Access Account Holders	Incorporate to general awareness.
1.4.21 Executive Sponsorship for Incident Management Activities	Mitigation	Enlisted for decision and resource support from Incident Handlers/IRT Leaders	♦ IT Security Manager ♦ Finance Director ♦ Department of Administration	
1.4.22 Emergency Incident Expense Approval	Mitigation	Level 3 or greater event requiring emergency financial investment to mitigate impact or recover	♦ IT Security Manager ♦ Finance Director	
1.4.23 Monitoring	Recovery and Monitoring	General Monitoring	♦ IT Security Manager ♦ IT Director	
1.4.24 Weekly Cyber Event Data Review	Recovery and Monitoring	Weekly	IT Security Manager	
1.4.25 System Recovery	Recovery and Monitoring	System is untrusted or unrecoverable following a cyber event	♦ Incident Handlers	
1.4.26 Handling of Reported Cyber Events	Reporting	A breach at a government agency within jurisdiction is reported to the OHS.	IT Security Manager	
1.4.27 Handling of Breach Related Artifacts	Reporting	Throughout Breach Incident Lifecycle.	IT Security Manager	
1.4.28 Incident Tracking	Reporting	Throughout Incident Lifecycle	♦Incident Handlers ♦IT Security Manager	
1.4.29 Incident Post-Mortem	Reporting	Resolved incident, submission of incident report. Within three days of close of incident.	♦IT Security Manager ♦IT Director ♦Post-mortem Team	

Pre-Incident

1.4.1 Configuration of Logs, Alerts and Cyber-security Reports

Step	Responsible Party	Trigger	Result
1.0	IT Security Manager	Prior to incidents, all alerting sources should be properly configured.	Configure alerting sources to send information security events to [email] In all possible cases, alerts should auto-generate tickets within the ticketing systems with the category of "Security Event" (reference: 1.4.6 Ticket System Configuration).
2.0	IT Security Manager	Information security monitoring controls should be configured to generate periodic reports of activity for review.	Configure all automated cyber-security reports to be delivered to [email]
3.0	IT Security Manager	Deployment of information systems.	Information systems should all be configured to use a standard consistent NTP time source. Time-skew between systems must be minimized to support time correlation between event sources.
4.0	IT Security Manager	Configuration of log storage and correlation sources is required.	Log storage and correlation engines should be configured to provide 60 days of live log for review. One year of log data should be accessible.
5.0	IT Technician	Deployment of workstations or servers.	The Splunk logging agent must be installed on all supported workstations and servers.
6.0	IT Technician	Deployment of devices, operating systems, services, and applications with SNMP logging support.	SNMP logs must be configured to be sent to the Splunk SNMP log storage and correlation. A minimum of SNMPv2 must be used.
7.0	IT Security Manager	Event logs should be configured for centralized storage, correlation, and monitoring for indicators of compromise from multiple sources.	Ensure system, application and device logs should be configured to centralized log stage, correlation, and monitoring sources.
8.0	IT Security Manager	Configuration definition, update, and review.	Ensure configuration standards for logging, alerting, and reporting satisfy need for monitoring and timely and effective response. Periodically audit configuration to ensure alerting and reporting mechanisms are configured in accordance to response requirements.

Back to Top -^

1.4.2 Coordination with MS-ISAC

Step	Responsible Party	Trigger	Result
1.0	IT Director	Pre-Incident	The IT Director will maintain contact information for MS-ISAC and procedures for escalation of cyber incident details to MS-ISAC when engaging for incident support.

Back to Top -^

1.4.3 Coordination with Law Enforcement

Step	Responsible Party	Trigger	Result
1.0	IT Director	Pre-Incident	The IT Director will maintain contact information for The Hawai'i Department of Law Enforcement (FDLE), Cyber-security Operations Center and the Cybercrime Office of the Department of Law Enforcement, and FBI along with procedures for escalating cyber-security incident events and reports to appropriate agencies.

Back to Top -^

1.4.4 Coordination with Communications Center

Step	Responsible Party	Trigger	Result
1.0	IT Director	Pre-Incident	The IT Director ensures the communications center is provided adequate training to identify reports of cyber-security incidents enabling them to advise on appropriate initial response actions required by the end-user as well as appropriately determine requirements incident severities requiring urgent escalation.

Back to Top -^

1.4.5 Coordination with Third-Party Agents

Step	Responsible Party	Trigger	Result
1.0	IT Director	Pre-Incident	The IT Director ensures any agreements with third party agencies that may have access to personal information as defined in 501.171 security of confidential personal information requires notice be made to the IT Security Manager within 10 days of a

			noticed breach. The IT Director ensures third-party agencies are provided clear instruction on requirements and means to report breaches

Back to Top -^

1.4.6 Ticket System Configuration

Step	Responsible Party	Trigger	Result
1.0	IT Director	Pre-Incident	The Ticketing system should be configured to support standard ticket categories, priorities, classifications, and approval processes. The following configurations must be in place for management cyber-security event tickets; • Tickets and their associated data must be accessible for up to five years from creation. • A category of “Security Event” must be created and assigned to all tickets automatically generated from alerting sources and e-mails sent to [email] • All tickets generated with the category of “Security Event” must generate automated notice of the even to the IT Director and IT Security Manager along with any other primary incident handlers assigned on staff. • Level 1, 2, 3, 4 and 5 priority definitions for security events must be created in accordance to 2.2 Incident Impact • Workflow processes must be implemented that require all “Security Event” tickets to be reviewed by the IT Director prior to final “closing” or “re-categorization” to provide final validation and approval for the resolved event. A ticket status of “Security Review” must be created and used to trigger final review and approval of resolved cyber-security events. • Reporting capabilities must be implemented to support periodic query and review of “Security Event” category tickets.

Back to Top -^

Detection and Notification

1.4.7 Internal Incident Reporting

Step	Responsible Party	Trigger	Result
1.0	Incident Reporters (All)	Suspected or known level 3, 4 or 5 event or breach of personal information.	Contact the Security Manager and IT Director. Incident report should include the time of the incident, a summary of the incident activity being reported, contact details for the incident reporter, and a summary of the potentially affected scope including but not limited to, user accounts, information systems, applications and networks.
2.0	Incident Reporters (All)	Suspected or known level 1 or 2 cyber-security incidents.	Call or E-mail Tier 1 IT Support or the Communications center outside of normal hours of operations (07:00 – 20:00 EST with exception to Holidays). Reference: 1.2 Contact Directory.
3.0	Communications Center	Reported cyber-security event.	Provide guidance on appropriate initial response for the event type. Document information related to the incident. Incident report should include the time of the incident, a summary of the incident activity being reported, contact details for the incident reporter, and a summary of the potentially affected scope including but not limited to, user accounts, information systems, applications and networks. A determination must be made if the report warrants a level 3 or greater severity event.
4.0	Communications Center	Reported cyber-security event determined to be level 3 or greater severity.	Escalate immediate contact to the IT Security Manager and IT Director.

Back to Top -^

1.4.8 Notification to Personnel

Step	Responsible Party	Trigger	Result
1.0	IT Director	Disruption of services due to a cyber event require notice of disruption to internal personnel. Criminal activity, or information breach is suspected.	Ensure coordination with law enforcement in accordance with 1.4.16 Coordination of Criminal Investigation.

2.0	IT Director	Disruption of services due to a cyber event require notice of disruption to internal personnel.	Determine need to delay notice due to impact to criminal investigation 1.4.16 Coordination of Criminal Investigation. General notification should be drafted to employees providing generic technology causes for downtime and/or activity. The intent is to provide cause to quell concerns while keeping details of the nature and scope of the incident to a "need to know" status. This draft may be provided to Legal Counsel for additional input.
3.0	Legal Counsel	Support is requested in generating communications in response to a cyber-event.	Provide legal counsel in assistance in drafting internal communications.

Back to Top -^

1.4.9 Notification to the Public

Step	Responsible Party	Trigger	Result
1.0	IT Director	A breach of information is determined that requires notification be made to the public.	Ensure coordination with Public Information Officer and law enforcement in accordance to 1.4.16 Determination of Criminal Investigation.
2.0	Risk Manager	Notified by the IT Director of a privacy or other cyber-event that may require a claim made to the insurer or support of additional incident handling services.	The Risk Manager will determine the financial impact of the event and appropriateness of filing an insurance claim. The Risk Manager will Initiate contact with the insurer per 1.4.12 Notification to Insurer. The Risk Manager will determine if services provided by the insurer to aid in a breach event satisfy implementation of the communication plan and will coordinate services delivery if determined appropriate.
3.0	Public Information Officer	Notified by the Risk Manager of a potential data breach or cyber-security event requiring contact be made to the affected public.	The Public Information Officer will establish an event communication plan in coordination with the Risk Manager and Legal Counsel in accordance with 501.171 Security of confidential personal information. This may take the form of written or e-mail n notice, or use of media in the cases contact information is unknown, or notification costs would exceed $250,000.
4.0	Legal Counsel	Support is requested in generating communications in response to a cyber-event.	Provide legal Counsel regarding appropriate communication content and requirements.
5.0	Public Information Officer	Notification plan is ready to be enacted.	Ensure all communications are made in accordance with communication plan.

Back to Top -^

1.4.10 Notification by Local Governments to State Cyber-security Agencies

Step	Responsible Party		Trigger	Result
1.0	IT Director		A cyber event of Level 3, 4 or 5 is determined to have occurred.	Shall report the event Cyber-security Operations Center and the Cybercrime Office of the Department of Law Enforcement as soon as possible but no later than 48 hours after discovery of the cyber-security incident and no later than 12 hours after discovery of the ransomware incident. The notification must include, at a minimum, the following information: 1. A summary of the facts surrounding the cyber-security incident or ransomware incident. 2. The date on which the local government most recently backed up its data, the physical location of the backup, if the backup was affected, and if the backup was created using cloud computing. 3. The types of data compromised by the cyber-security incident or ransomware incident. 4. The estimated fiscal impact of the cyber-security incident or ransomware incident. 5. In the case of a ransomware incident, the details of the ransom demanded. 6. A statement requesting or declining assistance from the Cyber-security Operations Center, the Cybercrime Office of the Department of Law Enforcement, or the sheriff who has jurisdiction over the local government.
2.0	IT Security Manager		A cyber event of Level 1, or 2 is determined to have occurred.	A local government may report a cyber-security incident determined by the local government to be of severity level 1 or 2 as provided in s. 282.318(3)(c) to the Cyber-security Operations Center, the Cybercrime Office of the

				Department of Law Enforcement, and the Sheriff who has jurisdiction over the local government. Refer to 1.2 Contact Directory for contact information.

Back to Top -^

1.4.11 Notification to Authorities Resulting from Breach

Step	Responsible Party	Trigger	Result
1.0	IT Security Manager	Investigation reasonably determines a breach of personal information will not result in financial harm or identity theft.	Written determination and supporting documentation must be submitted in writing to the Department of Legal Affairs within 30 days of determination.
2.0	IT Director	A data breach is known to impact 500 or more records of personal information as defined by 501.171 Security of confidential personal information	Provide notice to the Department of Legal Affairs in accordance with 501.171 Security of confidential personal information. Notice must be made in writing or for Judicial branch, post to an internal agency-managed website may be used.
3.0	IT Director	1000 or more records of personal information are affected in a data breach.	Notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. s. 1681a(p), of the timing, distribution, and content of the notices.
4.0	Legal Counsel	Support is requested in generating communications in response to a cyber-event.	Provide legal Counsel regarding appropriate communication content.

Back to Top -^

1.4.12 Notification to Insurer

Step	Responsible Party	Trigger	Result
1.0	Risk Manager	Emergency support required from insurer for claims, incident response, PR, or legal consulting.	Self-insured
2.0	Risk Manager	Non-emergency claims incident response, public relations and Legal consulting services are required from insurer.	Self-insured

Back to Top -^

1.4.13 Breach Handling

Step	Responsible Party	Trigger	Result

1.0	Incident Handlers	A breach of data as defined by state breach law is suspected. This should be suspected possible in all cases until investigation determines otherwise as all employees may have access to data within these categories.	14.13 General Investigation of resident data on affected systems in scope and access logs for affected access accounts should be conducted to determine potential for exposure of sensitive data during an event. Additional investigative resources may be engaged per 1.4.15 Formation of IRT.
2.0	IT Security Manager	Reasonable determination through investigation can be made that no data was breached during the event.	Generate and maintain documentation in support of written notice per 1.4.11 Notification to Authorities Resulting from Breach
3.0	IT Security Manager	A breach of data as defined by state breach law is confirmed.	Generate and maintain documentation in support of written notice per 1.4.11 Notification to Authorities Resulting from Breach Report the incident to State Cyber-security Agencies per 1.4.10 Notification by Local Governments to State Cyber-security Agencies. Maintain records related to the breach and response per 1.4.27 Handling of Breach Related Artifacts.
4.0	IT Security Manager	A breach of data as defined by state breach law exceeding 500 records is confirmed.	Establish a breach management team consisting of the Risk Manager, Sherriff, Public Information Officer (PIO) and Legal Counsel.
5.0	IT Director	Notice to OHS members, public or third parties may be required as a result of the data breach.	Coordinate Criminal investigation to determine requirements for delay of notice in accordance with 1.4.16 Coordination of Criminal Investigation
6.0	Risk Manager	Breach will result in a claim to the insurance. Assistance from external providers is required in response to a breach.	Coordinate services with insurer in accordance with 1.4.12 Notification to Insurer
7.0	Legal Counsel	Assistance is requested in drafting notice or in post-breach actions.	Provide Legal Council on response actions and content of notices and communications.
8.0	Public Information Officer	Notice to the public is required	Ensure notification is made to the public in accordance to 1.4.9 Notification to Public

Back to Top -^

Investigation

1.4.14 General Investigation

Step	Responsible Party	Trigger	Result
1.0	♦ IT Security Manager ♦ IT Director	Alerts from all sources will be investigated and coordinated to determine the scope and nature of the incident and define mitigating actions.	Review of alerts and other indicators of compromise present within logs and system events will be reviewed from all relevant sources to help determine the

	♦ Incident Handlers		nature and scope of the breach. Scope, nature, and incident impact severity as defined in section 2.2 Incident Impact must be defined throughout the course of the incident. Ensure a ticket is created for documentation and tracking of the incident if one is not already present. Details of the incident should be updated and tracked throughout the incident within the ticket. (reference 1.4.6 Ticket System Configuration) Incident tickets will maintain a definition of the incident, including: • Whether a Breach of information has occurred. • The nature, scope, and severity of the incident. Use incident impact levels in alignment with (reference: 2.2 Incident Impact) • The possible sources of the incident. • Actions taken or required in response to the incident. • Summary of notifications made to involved parties during the incident. • Post-mortem determinations and reference to associable action items as a result of post-mortem. • Links to data storage location containing artifacts related to the response.
2.0	♦ IT Security Manager ♦ IT Director ♦ Incident Handlers	Evidence or other artifacts (screenshots, logs, installation files, etc.) are encountered during response.	Ensure evidence is collected, documented, and maintained for further investigation, review or archival with the incident details. Content maintained throughout investigation should be adequate to satisfy notification requirements of 1.4.10 Notification by Local Governments to Cyber-security Agencies.
3.0	Incident Handlers	Potential for compromise of access credentials resulting from cyber event.	Investigation during the incident must involve review of user account login activity heuristics to determine potential compromise of access accounts. If an account compromise is determined, or highly suspected without determination

			1.4.20 Mitigation of Potentially Compromised Access Credentials.
4.0	Incident Handlers	Resolution of a security event.	Tickets must be changes to a status of "security review."
5.0	IT Director	Security event tickets in a "security review" status.	Confirm the event has been adequately resolved prior to close and trigger of any necessary post-mortem.
6.0	♦ IT Security Manager ♦ IT Director	Investigative, mitigating or recovery activities related to an incident requires authorized approval.	1.4.21 Executive Sponsorship for Response Actions
7.0	♦ IT Security Manager ♦ IT Director	Additional resources and agencies are required for response	1.4.15 Formation of IRT
8.0	IT Security Manager	Suspected criminal activity	1.4.16 Coordination of Criminal Investigation
9.0	IT Security Manager	Suspected Breach	1.4.13 Breach Handling
10.0	IT Security Manager	Forensic evidence collection is required.	1.4.17 Forensic Collection of Evidence
11.0	IT Security Manager	Throughout Life of Incident	Ensure incidents are tracked and documented 1.4.27 Incident Tracking

Back to Top -^

1.4.15 Formation of IRT

Step	Responsible Party	Trigger	Result
1.0	♦ IT Director ♦ IT Security Manager	Triage of incoming cyber-security incidents or indicators.	The IT Director and/or the IT Security Manager will delegate response task activity amongst members of the OHS technology staff.
2.0	♦ IT Director ♦ IT Security Manager	A breach is possible, or an event of severity level 3 or greater.	Communications will be sent out notifying the Town Manager, Risk Manager and Legal Counsel.
3.0	IT Security Manager	A breach is determined.	Establish a Breach Communication Team consisting of responsible members outlined in 1.4.13 Breach Handling.
4.0	IT Security Manager	Suspected internal criminal or malicious activity	Engage with chain of command to report suspicions of activity.
5.0	IT Security Manager	Additional investigation assistance or assistance, network communication logs or assistance with Albert alert data is required.	Engage MSISAC for investigative support and collection of network communication logs where appropriate.
6.0	IT Security Manager	Forensic collection of evidence or additional incident investigative	1.4.17 Forensic Collection of Evidence

		support is required to determine scope and nature of incident.	
7.0	♦ IT Security Manager ♦ IT Director	Executive sponsorship of activities, or notice as a result of a breach, or to internal personnel is required.	1.4.18 Executive Sponsorship for Response Actions
8.0	Risk Manager	Additional resources for investigation or post-event recovery as offered by insurer provider insurance claim is required.	1.4.10 Notification to Insurer
9.0	IT Security Manager	Emergency incident management expenses are required to investigate, mitigate, or recover.	Provide financial consultation support for requested resource allocations. 1.4.19 Emergency Mitigation Expense Approval
10.0	Legal Counsel	Legal support is required in response to a cyber event.	Engage with the incident response team to provide legal counsel.

Back to Top -^

1.4.16 Coordination of Criminal Investigation

Step	Responsible Party	Trigger	Result
1.0	IT Security Manager	Event is suspected to be perpetrated intentionally by malicious actors or otherwise indicative of criminal activity. Breach event requires notice to public or internal personnel	Report the suspicion of criminal activity through standard chain of command reporting procedures.
2.0	IT Security Manager	A breach or incident requires notice to be made to staff or the public.	Coordinate with the FBI and Hawai'i Department of Law Enforcement to determine impact of notice on criminal investigation and need for a delay of notice.
2.1	♦FBI ♦FDLE ♦MS-ISAC ♦Other Legal Agencies	Coordination of criminal activity is required for an event.	Determine if notification of the event will affect any current investigations. Requirements to delay notice, or "all-clear" statuses must be communicated to the IT Security Manager and provided in writing to the OHS.
3.0	♦IT Director ♦IT Security Manager	Filing of police reports, or receipt of notices or investigative reports from investigative agencies.	Documentation must be maintained with the incident details. Copies of police reports must be provided when reporting breaches 1.4.11 Notification to Authorities Resulting from Breach

Back to Top -^

1.4.17 Forensic Collection of Evidence

Step	Responsible Party	Trigger	Result
1.0	IT Security Manager	Forensic evidence collection is required during a cyber event that may result in a claim filed with the insurer	Coordinate with Digital Forensics Unit (DFU) For evidence collection assistance. Coordinate with the FBI or Hawai'i Department of Law Enforcement for evidence collection assistance.

Back to Top -^

1.4.18 Escalation with MS-ISAC

Step	Responsible Party	Trigger	Result
1.0	IT Security Manager	Additional technical support is required for investigation of an event. Splunk event logs, network security system logs, or aid with monitoring for indicators of compromise during an event.	Engage with MS-ISAC for investigative support.

Back to Top -^

Mitigation

1.4.19 Mitigation of Insecure User Activities

Step	Responsible Party	Trigger	Result
1.0	IT Security Manager	Monitoring/review of events, logs and alert heuristics indicate events generated due to insecure user activities.	Contact will be made to the employee(s) to determine if misuse is the cause of repeat cyber events or indicators of events. False positive indicators should be addressed through tuning of logging, monitoring, and alerting capabilities. In cases where insecure user actions are determined to be causes of events, mitigating actions will be planned and enacted. Mitigating actions may involve creation or modification to policy, work procedures or specific security or technology education that may be necessary for affected staff.
2.0	IT Security Manager	Repetitive insecure user activity through misuse following implementation of mitigating policy, procedures, and education.	Report repetitive violations of use through OHS chain of command reporting procedures.

Back to Top -^

1.4.20 Mitigation of Potentially Compromised Access Accounts

Step	Responsible Party	Trigger	Result

1.0	Incident Handlers	Investigation of events determines potential impact of access credentials	Accounts should be temporarily disabled if untrusted until investigation determines the account was not compromised. Account passwords must be reset to secure temporary passwords from a known "trusted" system. Account passwords are securely provided to the end user after mitigation resolves the potential for re-compromise of credentials. Temporary account passwords following reset are required to be changed on initial login.
2.0	Affected Account Holders (all)	Potential for account compromise extends to use of third-party or cloud applications outside of the OHS IT Department administration.	The affected account holders must ensure all passwords for all services are changed to a new secure password. Changes to the passwords must be made from a "trusted" system.

Back to Top -^

1.4.21 Executive Sponsorship for Incident Management Activities

Step	Responsible Party	Trigger	Result
1.0	IT Security Manager	Enlisted for decision and resource support from Incident Handlers/IRT Leaders	Provide timely decisions and resources required to support response activity in accordance to relevant policies, procedures, laws, and regulations.
2.0	IT Director	Response decisions have impact to varying departments or stakeholders	Communicate and coordinate the potential impact of the activity with the affected stakeholders.
3.0	IT Director	Emergency funding is required for mitigation, recovery, investigation or other incident support for level 3 or greater events.	Engage with the Finance Director to establish emergency budget approval.
4.0	IT Director	Non-emergency funding is required for incident management or for post-mortem improvements to incident management capabilities.	Provide a change proposal to the Finance Director. The Department of Administration will be notified.
4.1	♦ Finance Director ♦ Department of Administration	Change proposal is provided by the IT Director, requiring funding for incident management.	Generate a financial proposal for the necessary budget. Follow standard budget submission procedures.
5.0	IT Director	Emergency funding is required for incident management.	1.4.22 Emergency Incident Management Expense Approval

Back to Top -^

1.4.22 Emergency Incident Expense Approval

Step	Responsible Party	Trigger	Result
1.0	IT Director	Level 3 or greater event requiring emergency financial investment to mitigate impact or recover	Engage with the Finance Director to establish funding.
2.0	Finance Director	Request for emergency incident expense approval received from the IT Director	Establish appropriate resources to incident management needs.

Back to Top -^

Recovery and Monitoring

1.4.23 Monitoring

Step	Responsible Party	Trigger	Result
1.0	♦ IT Security Manager ♦ IT Director	Normal Operating Hours	Regularly monitor alerts generated from detection software or reports of potential cyber events from personnel.
2.0	♦ IT Security Manager ♦ IT Director	Outside normal operating hours.	Regularly monitor for level 3 or higher severity event escalation from the communications center and alert sources.

Back to Top -^

1.4.24 Weekly Cyber Event Data Review

Step	Responsible Party	Trigger	Result
1.0	IT Security Manager	Weekly	All logs, events, alerts, incident tickets and security reports will be reviewed with IT Director for anomalies and general heuristics for indicators of undetected events, or improvements required to information security capabilities.
2.0	IT Security Manager	Monitoring/review of events, logs and alert heuristics indicate events generated due to insecure user activities.	1.4.19 Mitigation of insecure user activities

Back to Top -^

1.4.25 System Recovery

Step	Responsible Party	Trigger	Result
1.0	♦ Incident Handlers	System is untrusted or unrecoverable following a cyber event	Nubeva software can detect ransomware encryption and immediately capture copies of the encryption keys. With keys in hand, Nubeva provides the fastest and easiest path to complete recovery with limited data loss.

			Times of events and trusted restoration points will be determined, and the system restored from a trusted backup.

Back to Top -^

Reporting

1.4.26 Handling of Reported Cyber Events

Step	Responsible Party	Trigger	Result
1.0	IT Security Manager	A breach at a government agency within jurisdiction is reported to the OHS IT Department.	Maintain all provided documentation and communications along with dates and times of interactions in a manner that can be easily retrieved for the Department of Legal Affairs if requested.
2.0	IT Security Manager	A breach at a government agency within jurisdiction is reported to the OHS IT Department.	A reported incident should initiate investigation for potential impact to OHS information systems as a result of the reported breach.
3.0	IT Security Manager	A breach at a government agency within jurisdiction is reported to the OHS IT Department.	May provide further support for the affected agencies in coordinating with law enforcement agencies (reference 1.4.3 Coordination with Law Enforcement)

Back to Top -^

1.4.27 Handling of Breach Related Artifacts

Step	Responsible Party	Trigger	Result
1.0	IT Security Manager	Investigation and handling of a breach of personal information	Police reports, forensic reports, incident reports, logs, alerts, and other discoverable content along with documentation on the incident handling must be stored and maintained for discovery requests from the Department of Legal Affairs.
2.0	IT Security Manager	Investigation reasonably determines no risk of identity theft or financial harm due to breach of personal information.	Written reports regarding the determination must be maintained in writing for 5 years.

Back to Top -^

1.4.28 Incident Tracking

Step	Responsible Party	Trigger	Result
1.0	Incident Handlers	During Incidents	Must maintain accurate incident definitions, log of actions taken, and take steps to

			preserve evidence and other artifacts related to the incident. Information for the incident must be maintained and available to incident handlers for purpose of tracking and communicating the incident within the ticketing system. Reports of events to the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government requires the following information 1. A summary of the facts surrounding the cyber-security incident or ransomware incident. 2. The date on which the local government most recently backed up its data, the physical location of the backup, if the backup was affected, and if the backup was created using cloud computing. 3. The types of data compromised by the cyber-security incident or ransomware incident. 4. The estimated fiscal impact of the cyber-security incident or ransomware incident. 5. In the case of a ransomware incident, the details of the ransom demanded. 6. A statement requesting or declining assistance from the Cyber-security Operations Center, the Cybercrime Office of the Department of Law Enforcement, or the sheriff who has jurisdiction over the local government.
2.0	IT Security Manager	Conclusion of a confirmed cyber-security incident.	Must Generate a Cyber Incident Report and schedule a post-mortem 1.4.29 Incident Post-Mortem
3.0	IT Security Manager	Submission of incident report	Must ensure incident reports are maintained for the purposes of post-mortem, and inclusion in functional risk assessment and cyber-security planning exercises. Ensure post-mortem leader is identified and post-mortem process is performed per 1.4.29 Incident Post-Mortem

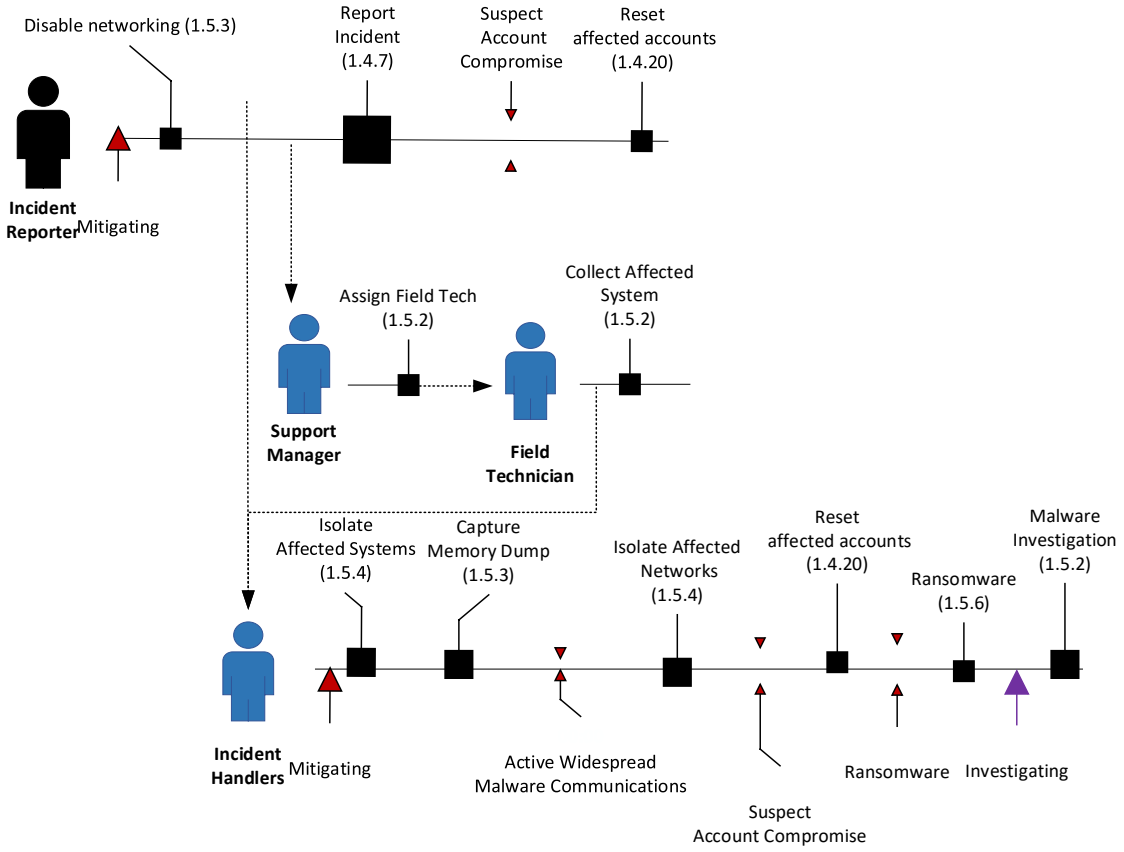
Back to Top -^

1.4.29 Incident Post-Mortem

Step	Responsible Party	Trigger	Result
1.0	IT Security Manager	Resolved incident, submission of incident report.	Review incident report and schedule post-mortem conference within one week of close.
2.0	IT Security Manager	Within three days of close of incident.	Conduct post-mortem meeting/conference with participating incident handlers and stakeholders of interest to the incident.
3.0	Post-mortem Team	Post-mortem meeting	Provide evidence and details related to the incident to the post-mortem leader. Collectively work to complete the incident After-Action report by identifying root cause problems and plans for improving information security and response.
4.0	IT Security Manager	Conclusion of post-mortem meeting	Store After-Action Reports and establish directive and resources to meet cyber-security improvements. Ensure After-Action reports are archived and available for future tracking and review of security plan status. Generate change proposals for budget and submit per 1.4.22 Executive Sponsorship for Incident Management Activities
5.0	IT Security Manager	Within one week of close of incident.	Submit to the Hawai'i Digital Service, within 1 week after the remediation of a cyber-security incident or ransomware incident, an after-action report that summarizes the incident, the incident's resolution, and any insights gained as a result of the incident. Submission of completed incident and After-Action reports will satisfy communications requirements.
6.0	IT Director	After Action Report Generated	Must review all after action reports and establish appropriate priority, resources, and approval for implementation through the appropriate chain of command.

Back to Top -^

1.5 Malware



Go to Appendix E: Incident Type Procedures Diagram Legend

Procedure	Phase(s)	Triggers	Audience	Notes
1.5.1 Endpoint Agent Configuration	Pre-Incident	New workstation or server deployed.	IT Technician	
1.5.2 Malware Investigation	Investigation	System suspected to be actively infected with malware.	Incident Handlers	
1.5.3 Initial Personnel Response	Mitigation	Presented with a ransomware or other suspicious pop-up box. Otherwise suspect or confirm the presence of malware on a system.	♦ Incident Reporters (all) ♦ Support Manager ♦ Field Technician	Incorporate to general awareness training.
1.5.4 Isolate Affected Systems	Mitigation	Suspect or confirm the presence of active malware on a system	Incident Handlers	
1.5.5 Isolate Affected Networks	Mitigation	Review of malicious activity trends, or notification of active events involving command and control servers or other inbound/outbound malicious communications.	Incident Handlers	
1.5.6 Ransomware	Mitigation	A ransomware incident occurs.	♦ Incident Handlers ♦ IT Security Manager	

Pre-Incident

1.5.1 Endpoint Agent Configuration

Step	Responsible Party	Trigger	Result
1.0	IT Technician	New workstation or server is deployed.	Ensure Endpoint Security agent is installed, and components are configured to allow for isolation and forensic memory collection from potentially infected hosts.

Back to Top -^

Investigation

1.5.2 Malware Investigation

Step	Responsible Party	Trigger	Result
1.0	Incident Handlers	System suspected to be actively infected with malware.	Affected systems must be investigated in isolation per 1.5.4 Isolate Affected Systems prior Refer to 1.4.14 General Investigation
2.0	Incident Handlers	System determined to be actively infected with malware.	Generate and save a dump of live system memory for forensic purposes using Endpoint Security.
3.0	IT Security Manager Incident Handlers	Ransomware is determined to have destroyed data or systems and rendered it unrecoverable.	1.5.6 Ransomware

Back to Top -^

Mitigation

1.5.3 Initial Personnel Response

Step	Responsible Party	Trigger	Result
1.0	Incident Reporters (all)	Presented with a ransomware or other suspicious pop-up box. Suspect or confirm the presence of malware on a system.	Disconnect networking cables or disable Wi-Fi if it is laptop. Report the incident in accordance to General Handling 1.4.7 Internal Incident Reporting. If possible, resume work on an available workstation.
2.0	Incident Reporters (all)	access account holder suspects credentials may be compromised.	Ensure account details are included in the summary of the report. Reset account passwords from a “trusted system” per 1.4.20 Mitigation of Potentially Compromised Access Accounts

3.0	Support Manager	Incident report received	Assign a Field Technician to collect the affected system.
4.0	Field Technician	Assigned to retrieval of affected workstation.	Affected systems must be investigated in isolation per 1.5.4 Isolate Affected Systems prior . Ensure memory forensics are collected before powering off the system.

Back to Top -^

1.5.4 Isolate Affected Systems

Step	Responsible Party	Trigger	Result
1.0	Incident Handlers	Suspect or confirm the presence of active malware on a system.	To help mitigate potential spread of a malware attack, Endpoint Security should be used to isolate potentially affected systems from the network prior to investigation. Investigation should be conducted in isolation from unaffected systems. Physical workstations and devices should be investigated locally until a determination is made to the state of the system. The system may be re-connected to networks when the event is determined false or fully mitigated and resolved.
2.0	Incident Handlers	Isolation is required for a critical production server.	1.4.21 Executive Sponsorship for Incident Management Activities to ensure notice is made and approval established prior to isolation. Disconnect networking cables or disable networking to isolate the server. In a level 3 or greater severity event with active malware, handlers may isolate systems to quickly by disabling networking links to mitigate the event prior to following communications in 1.4.21 Executive Sponsorship for Incident Management Activities.
3.0	Incident Handlers	Review of malicious activity trends, or notification of active events involving command and control servers or other inbound/outbound malicious communications.	Review network traffic from affected hosts and identify the malicious endpoints that traffic is being directed to. Implement firewall controls to prevent communications to/from the suspected host In severe cases of level 3 or greater severity impact 1.5.5 Isolate Affected Networks

Back to Top -^

1.5.5 Isolate Affected Networks

Step	Responsible Party	Trigger	Result
1.0	Incident Handlers	Review of malicious activity trends, or notification of active events involving command and control servers or other inbound/outbound malicious communications.	1.4.21 Executive Sponsorship for Incident Management Activities.to ensure notice is made and approval established prior to isolation. Disconnect networking cables or disable logical ports to isolate the required network segments. In a level 3 or greater severity event with active malware, handlers may isolate Networks by disconnecting networking cables to quickly mitigate the event prior to following communications in 1.4.21 Executive Sponsorship for Incident Management Activities.

Back to Top -^

1.5.6 Ransomware

Step	Responsible Party	Trigger	Result
1.0	Incident Handlers	A ransomware incident occurs.	In compliance to the Local Governments Cyber-security Act, OHS is prohibited from complying with ransomware events. Where possible attempt recovery of the system 1.4.25 System Recovery
2.0	IT Director	A ransomware incident occurs	Ensure reporting to state agencies in accordance to 1.4.10 Notification by Local Governments to State Cyber-security Agencies.

Back to Top -^

2: Roles and Responsibilities

All – A general designation for all persons involved in and/or potentially impacted by an incident.

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

Incident Handler – Incident Handlers are members of the OHS's staff or enlisted third-party agents 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 possible incident or as a member of the Incident Response Team as required.

IT Security Manager – Manages information security for the OHS. Acts as a primary incident handler and incident response team leader. Identifies and coordinates resources needed for response. Fills leadership roles for response activities and ensures communication is made to IT Director during an incident.

IT Director – Manages information technology implementation including configuration for monitoring and alerting mechanisms for the OHS. Acts as a primary incident handler and incident response team leader. Identifies and coordinates resources needed for response. Fills leadership roles for response activities and ensures communication is made to required parties during an incident.

Communications Center – Responds to potential cyber incidents after hours. Instructs incident reporters on required initial steps to be taken. Identifies potential events of severity 3 or greater and escalates in those cases to the IT Security Manager and IT Director.

Support Manager – May delegate response tasks to OHS Information Technology support staff such as field technicians.

Field Technician – May conduct on-site response activity such as retrieval of compromised systems

IT Technician – General designation for OHS IT Support personnel.

Access Account Holder – Persons maintain authorized user access accounts with access to OHS information resources.

Incident Response Team (IRT) – Refers to the collection of persons and third-party agents engaged in response to an incident. 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 IRT.

Incident Response Team Leader – The IT Security Manager or IT Director is responsible for formation and coordination of the Incident Response Team. The Incident Response Team Leader is responsible for notifying the

Breach Communication Team of breaches and coordination of other communications and resources required by the Incident Response Team.

Digital Forensic Unit (DFU) – Participants in an incident response and associated stakeholders responsible for conducting digital evidence collection, examination, analysis, and reporting of incident.

Post-mortem Team – Participants in an incident response and associated stakeholders responsible for conducting post-mortem review of incident details.

Post-mortem Leader – Individual or committee designated responsibility to lead post-mortem review of incidents. This appointment may vary based on nature of the incident and involved parties.

Breach Communication Team - The breach communication team consists of the Risk Manager, Public Information Officer, and Legal Counsel and is responsible for appropriate breach notification as required by state or regulatory laws in response to a confirmed breach.

Public Information Officer (PIO) – The PIO is responsible for enacting approved communications with the public during an incident.

Legal Counsel– Provides guidance and counsel related to relevant law and regulation. Submission of relevant legal documentation. May be involved in evidence collection and handling.

Risk Manager – Maintains contact with and enlists support from the insurer.

Sheriff - Provides executive support and resource acquisition for incident management actions and emergency budget requirements.

Finance Director – Provides resource support for emergency incident management budget. Submits budget requests for incident management improvements.

Department of Administration – Works with Finance Director to submit budget request for improvements to incident management capabilities.

Third-Party – Some response activities and roles may be dependent on the cooperative plan execution by third-party service and support providers. The extent of reliance on third and first-party response activities will be subject to change overtime as technologies and roles evolve within the OHS. As such any defined roles in this section may be partially or wholly reliant on a third party for execution. These role assignments are noted as "Third-party" prior to the role name, for example "Third-party Incident Handler" or "Third-Party Breach Communication Team."

Appendix A: Definitions

Anomaly - An unusual or atypical event (in a system or network).

Attack Scanner - A tool used to remotely connect to systems and determine security vulnerabilities that have not been fixed.

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 5.2 Breach Communication Laws of this policy document.

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

Cracker - A person who obtains or attempts to obtain unauthorized access to computer resources for specific, premeditated crimes. (See also Hacker)

Checksum - Value computed, via some parity or hashing algorithm, on information requiring protection against error or manipulation.

Code - A system of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length.

Cracking Utilities - Programs planted in systems by attackers for a variety of purposes such as elevating privileges, obtaining passwords, and disguising the attacker's presence.

Cryptographic - A checksum that is generated using a checksum cryptographic means. It is used to detect accidental or deliberate modification of data.

Disruption of service - Occurs when an intruder uses malicious code to disrupt computer services, including erasing a critical program, “mail spamming” i.e., flooding a user account with electronic mail, or altering system functionality by installing a Trojan horse program.

Encryption - Using encryption renders information unintelligible in a manner that allows the information to be decrypted into its original form - the process of transforming plain text into cipher text.

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

Firewall - Used to control access to or from a protected network. Enforces a network access policy by forcing connections to pass through this system, where they can be examined and evaluated. The system can be a router, a personal computer, a host, or a collection of hosts, set up specifically to shield a site or subnet from protocols and services that can be abused from hosts outside the subnets.

Hacker - A person who obtains or attempts to obtain unauthorized access to a computer for reasons of thrill or challenge. (See also Cracker)

Hoax - A hoax occurs when false stories, fictitious incidents or vulnerabilities are spread (e.g., virus warnings that do not exist).

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, violations of information technology policy, and lost or stolen computer equipment and /or intelligent devices.

Integrity - (1) A sub-goal of computer security which pertains to ensuring that data continues to be a proper representation of information, and that information processing resources continue to perform correct processing operations. (2) A sub-goal of computer security which pertains to ensuring that information retains its original level of accuracy. Data integrity is that attribute of data relating to the preservation of:

(a) its meaning and completeness,

(b) the consistency of its representation(s), and

(c) correspondence to what it represents.

Intrusion - Unauthorized access to a system or network

IRT - Incident response Team

Misuse - Misuse occurs when someone uses a computing system for other than official or authorized purposes.

Sniffer - A device or program that captures packets transmitted over a network.

Social engineering - "Conning" unsuspecting people into sharing information about computing systems (e.g., passwords) that should not be shared for the sake of security.

Threat - Capabilities, intentions, and attack methods of adversaries to exploit any circumstance or event with the potential to cause harm to information or an information system.

Trigger – An event or incident definition that requires an action is taken in response.

Trusted – System, account or other information asset that is uncompromised and in a verifiable known good security state.

Ransomware – Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.

Trojan horse - Computer program containing an apparent or actual useful function that contains additional (hidden) functions that allows unauthorized collection, falsification or destruction of data.

Unauthorized access - Unauthorized access encompasses a range of incidents from improperly logging into a user's account (e.g., when a hacker logs in to a legitimate user's account) to obtaining unauthorized access to files and directories possibly by obtaining "super-user" privileges. Unauthorized access also includes access to network data

gained by planting an unauthorized "sniffer" program (or some such device) to capture all packets traversing the network at a particular point.

Virus - Self-replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no external signs of its presence.

Vulnerability - A weakness in an information system, cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited to violate system security policy.

Worm - An independent program that replicates from machine to machine across network connections often clogging networks and computer systems as it spreads.

APPENDIX B: INCIDENT DEFINITIONS

Incidents are classified by common definition. This allows for appropriate response decisions to be easily made by the appropriate persons. Incident handling phases, participants and decision-making scopes of authority may be in part dictated by the incident definition.

The incident definition is comprised of the incident type, scope, and severity. Incident definition may be subject to change during incident handling as investigation may uncover more components of the incident which extends or reduces the scope, level or involved incident types. It is the job of the Incident Handlers to maintain and communicate appropriate incident definitions within all incident handling communications.

Type

This generally deals with a classification of attack like "Malware," or "Social Engineering." Types are outlined in section 6, "Incident Type Handling Procedures". Incident types dictate specific handling procedures. 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.

Scope

The scope of the incident is the extent of the incident's impact, which could be broad, moderate, or narrow. This must be determined by the Incident Handlers and may relate to affected applications, systems, departments, or networks and should contain an inventory of the affected accounts, applications, and information systems, operational processes along with potentially affected data.

Severity

An incident severity is defined by 1) the confidence in the validity of the incident, 2) the potential impact, and 3) an additional indicator signifying a risk of breach.

The remainder of this section deals with establishing common definitions of severity.

2.1 Incident Confidence

Incident confidence provides differentiation between possible, confirmed, and false incidents.

Possible

Possible 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 possible Incidents which have been proven through evidence reviewed first-hand by the Department to involve a loss or compromise of data or the loss of functionality of information systems, applications, or business operations.

False

False Incidents (aka False Positives) are Possible Incidents which upon further review do not involve a loss or compromise of data or the loss of functionality of information systems, applications, or business operations.

2.2 Incident Effect

Incident Effect severity levels help communicate the amount of potential damage. Incident impact definitions are aligned to the definitions within the NIST Cyber-security Framework (CSF) and NIST 800-61 guidance OR guidance provided by the Department of Homeland Security (DHS) Cyber-security & infrastructure Security Agency (CISA).

Level 5: EMERGENCY

Level 5 is an EMERGENCY-level incident within the specified jurisdiction that poses an imminent threat to the provision of wide-scale critical infrastructure services; national, state, or local government security; or the lives of the country's, state's, or local government's residents.

Level 4: SEVERE

Level 4 is a SEVERE-level incident that is likely to result in a significant impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; or civil liberties.

Level 3: HIGH

Level 3 is a HIGH-level incident that is likely to result in a demonstrable impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

Level 2: MEDIUM

Level 2 is a MEDIUM-level incident that may impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

Level 1: LOW

Level 1 is a LOW-level incident that is unlikely to impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

2.3 Breach Definition

A breach level definition is added to the incident level if the compromised applications or information systems are suspected to hold private information in accordance with Hawai'i Law. Breach status indication may only be removed if it can be adequately determined and proven that no unencrypted "Personal Information" was acquired by unauthorized parties because of the incident. Breaches are classified as a breach or large breach on the basis of the number of personal information records potentially affected.

Personal Information Definition.

1. **"**Personal information" means either of the following:

a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

(I) A social security number;

(II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

(III) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;

(IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

(V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

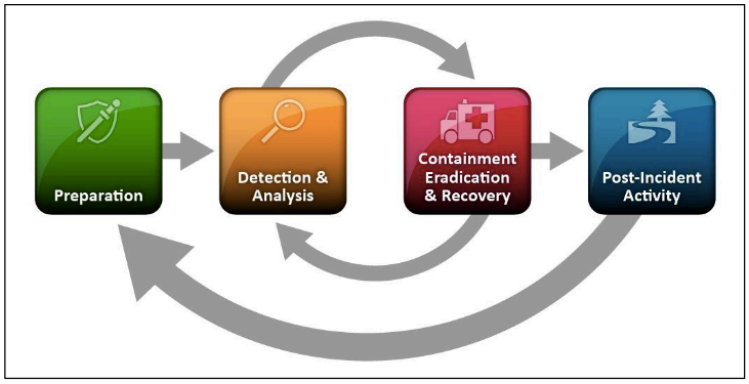
b. A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

2. The term does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

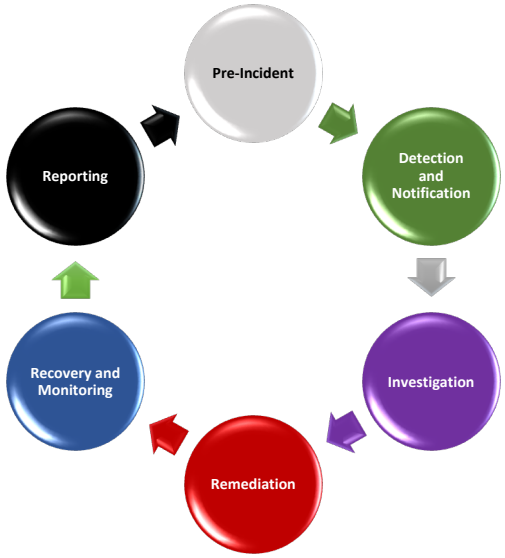
Large Breach

1,000+ records affected. Large breaches must be reported to consumer reporting agencies.

APPENDIX C: INCIDENT HANDLING PHASES



NIST 800-61 provides standardized incident response guidance to be utilized by any Entity/Organization's cyber-security personnel supporting cyber incident response. 800-61 breaks the process into four phases (as shown in the graphic above. That being said, the document requires a specific level of cyber-security history or expertise in order to be digestible.



The incident handling phases (from the graphic above) described herein are an expanded definition beyond that provided in NIST 800-61. While maintaining the consistency of process and lexicon from 800-61, they provided expanded guidance and information to enable this same consistency for a workforce with a wide and diverse experience set in cyber incidents. This helps to provide consistency from novice to expert.

3.1: PRE-INCIDENT

To ensure response capabilities are adequate if not optimally functional, some tasks need to be regularly accomplished prior to an incident occurring. Operationally, the pre-incident phase is also known as STEADY STATE (normal operations).

3.2: DETECTION AND NOTIFICATION

Detection relates to the processes and technologies used for the collection and review of alerts, with the intent to establish timely and relevant notifications to warn the Department about potential attacks and indicators of compromise.

Notification of a possible incident can come from any persons, software monitoring and alerts, anomalous activity, or other technical indicators of compromise. Upon notification of a possible incident an Incident Handler must be assigned to begin investigation into the incident.

3.3: Investigation

Incident investigation is the responsibility of the Incident Handlers operating alone or in conjunction with the IRT. 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 aid in determining appropriate actions for mitigation, recovery, and reporting.

3.2.1 Incident Response Team

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 IT Security Manager or IT Director to act as Incident Response Team Leader to form an Incident Response Team (IRT). The IRT 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 IRT as required during incident handling by the IRT Leader. IRT members may also include or be led by third parties. An IRT must be established along with formation of a Breach Notification Team when the incident definition indicates a breach. An IRT may include persons or entities not already identified within this document – as necessary to achieve resolution – as authorized by the IT Security Manager or Director.

3.3: Remediation

Remediation actions are the responsibility of the Incident Handlers and IRT and are actions taken to

a) Contain the incident.
b) Remove active threats from the environment as it pertains to the incident following adequate investigation.
c) Prevent future recurrence of the incident by remediation of used attack vectors.

3.4: 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 IRT and focuses on;

a) Restoring normal business operations from a failed state
b) Restoring 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 confirm an incident has been successfully contained and mitigated as well as continually monitor for recurrence of problems.

3.5: 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, or state agencies in cases of criminal activity or breaches.

Reporting also pertains to reports required by state authorities and persons whose information has been breached in accordance to relevant state laws.

3.5.1 Incident Tracking

Communications, analysis results, evidence and other artifacts related to the incident will be maintained by incident handlers throughout the course of the incident. This data may be invaluable to the response and shared amongst the team during handling of the incident. Incident handlers, or IRT Leaders if an IRT is formed, must submit a completed cyber incident report (Appendix B.) to the Executive Leadership Team upon conclusion of the incident. All data related to the incident and its response actions must be stored by handlers and made available for collection and review during incident post-mortem. It will be the responsibility of the person conducting post-mortem to ensure all data related to the response is centrally collected, analyzed, and archived along with the results of incident post-mortem review. This data should be stored minimally for five years with the consideration it may provide context for potential future incidents.

Incident Tracking should be executed using a Case Number process. Case Numbers provide a single point of reference under which all collected data, coordinated decisions, and actions taken may be centralized. A Case Number is uniquely assigned for each confirmed case – though not for pre-incident research that concludes with an incident not being confirmed. For the purposes of this template, the Case Number process will be based upon the following nomenclature:

ENTITY INITIALS-DATE/TIME GROUP-NUMBER

EXAMPLE: HI-MAY2024-001

This Case Number nomenclature provides a simple, repeatable, and easily searched tag (Case Number) for quickly referring to or researching previous or current cases.

3.5.2 Incident Post-Mortem

All confirmed incidents will require execution of a "post-mortem" review within three days of incident resolution. The IT Security Manager will be responsible for conducting post-mortem. Persons responsible for conducting the post-mortem are responsible for collection of details and evidence related to the incident, analysis of the problem, and submission of an Incident After-Action Report (Appendix C.). The IT Security Manager may delegate incident post-mortems. The IT Director must review all generated After-Action Reports and coordinate results and necessary resources for implementation with the appropriate chain of command.

Post-mortem is conducted with intent to improve cyber-security through pro-active implementation of "lessons learned" as detailed in Section 3.4.1 of NIST SP800-61r2. The section establishes the following critical questions which our incident post-mortems should seek to answer:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other Departments have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

These questions, while not wholly inclusive of all possibilities, provide foundational framing for problems we should seek to identify in our cyber security implementation and response handling, but alone they do not provide a methodology for clear root cause problem analysis focused on identifying the best appropriate solutions. The Department's incident After-Action report implements a structured root cause problem analysis and resolution approach defined by six sigma as the "(**D**)efine, (**M**)easure, (**A**)nalyze, (**I**)mplement,(**C**)ontrol" methodology. This methodology was designed with the intention of identifying and resolving deficiencies and inefficiencies within a business process and aligns particularly well to improving response practices and security controls.

Define

The person responsible for conducting post-mortem will schedule a conference or meeting with all incident handlers and parties of interest to the incident with the purpose of collectively reviewing the details of the incident. This meeting must be scheduled and held within one weeks of submission of the final incident report concluding the incident. Incident handling reports and other artifacts related during the response will be collected and reviewed.

Measure

Critical response metrics, "time-to-detect" (TTD) and "time-to-resolve" (TTR) will be captured within the After-Action report to provide trending and measure on the effectiveness of response activity.
Root cause problems identified through 5y analysis must be further clarified to a quantifiable problem with supporting data analysis proving the extent of the problem.

Analyze

Collective analysis of response data and subsequent lessons learned during the post-mortem meeting will generate a list of failures and inefficiencies in both prevention and response. The post-mortem team will identify root cause for these problems through 5y analysis, which simply challenges the team to ask, “why did this problem occur?” to a depth of 5 for each stated problem. An incident After-Action report may hold analysis on multiple problems.

Implement

A plan will be drafted recommending solutions to the identified root problems. Executive leadership will conduct timely review of plans submitted and approve or reject the plan items. A plan owner will be identified, and resources, including a timeline for implementation, will be agreed upon with the plan owner. These details will be updated within the plan. An incident After-Action report may hold multiple plans.

The significance of this plan is to identify and implement lessons learned and to evolve the overall cyber-security process as a result. Lessons learned provide the necessary guidance to evolve the processes and procedures with a focus on preventing a similar or identical recurrence of the cyber incident in the future.

Control

A means to follow up and measure the success of the implementation is required when the plan is agreed upon. A plan to standardize implementation of successful controls and practices globally across the entire Entity/Organization should be enacted where sensible for the control.

Unresolved plans whether rejected, or incomplete, shall be incorporated into risk assessment and security planning functions performed by the Department. This is to ensure appropriate consideration and priority is given to existing initiatives, and previously rejected initiatives may be given fresh consideration with new information gathered during these functional exercises.

Appendix D: Breach Handling

All systems and users of the Department's system may have access to information as defined by Hawai'i Statue policy. As such potential for data breach should be considered in all cases of a confirmed compromise of a system or account. Possible or confirmed breaches must be investigated to determine the extent and nature of the breach. All incidents potentially impacting "Personal Information" as defined by Hawai'i Statute policy, shall be treated as a possible breach until due diligence in investigation is conducted to determine otherwise. Hawai'i policy extends the definition of "Covered Entity" to government entities for notification requirements detailed in subsections (3) - (6). This law requires reporting to the Department of Legal Affairs through written notice as expediently as possible but no later than within thirty (30) days of a breach of "Personal Information" affecting 500 or more records. In the case of the affected "covered entity" being a member of the judicial branch, notice of the required information may alternatively be posted on any agency-managed website. Notice to affected individuals must be made through written notice or e-mail as expediently as possible, but no later than thirty (30) days following the detection of the breach. Substitute notice may be used in lieu of direct notice if the cost of direct notice would exceed $250,000.00, or because notice affects more than five hundred thousand (500,000) records, or because the covered entity does not have the mailing or e-mail addresses of the affected persons. Substitute notice may include publication to a managed public website or use of print and broadcast media in areas where affected individuals reside. This notice should be delayed if it is determined to interfere with any criminal investigations for the length of time determined to be reasonably necessary by the law enforcement agency. If it is determined a breach will not result in identity theft or financial harm, notice to individuals is not required, but the covered entity must create a written report of the investigation and determination and save this for five (5) years. This written determination must be submitted to the Department of Legal Affairs within thirty (30) days.

If more than one thousand (1,000) records were affected, notice must be made without delay to all consumer reporting agencies as defined in the Fair Credit Reporting Act, 15 U.S.C. s. 1681a(p).

Agreements with third-parties should require notice to the OHS of any breaches that may affect the Department's information and information systems within ten (10) days of determination of a breach.

Incident Response, Public Relations and Legal Counsel support services are available through the OHS's cyber, and vendors.

Integration of cyber-insurer services into IRT response activity should be considered if a breach is possible and additional legal counsel or public relations support is required beyond the capability of an initial review by the OHS and additional external agents involved in the response.

5.2 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.

The following is content from Hawai'i Statute regarding breach communications:

INSERT BREACH COMMUNICATIONS POLICY HERE IF DIFFERENT FROM BELOW

Security of confidential personal information.

(1) DEFINITIONS

As used in this section, the term:

(a) "Breach of security" or "breach" means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

(b) "Covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. For purposes of the notice requirements in subsections (3)-(6), the term includes a governmental entity.

(c) "Customer records" means any material, regardless of the physical form, on which personal information is recorded or preserved by any means, including, but not limited to, written or spoken words, graphically depicted, printed, or electromagnetically transmitted that are provided by an individual in this state to a covered entity for the purpose of purchasing or leasing a product or obtaining a service.

(d) "Data in electronic form" means any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

(e) "Department" means the Department of Legal Affairs.

(f) "Governmental entity" means any department, division, bureau, commission, regional planning agency, board, district, authority, agency, or other instrumentality of this state that acquires, maintains, stores, or uses data in electronic form containing personal information.

(g) 1. **"**Personal information" means either of the following:

a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

(I) A social security number;

(II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

(III) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;

(IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

(V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

b. A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

2. The term does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

(h) **"**Third-party agent" means an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity or governmental entity.

(2) REQUIREMENTS FOR DATA SECURITY

Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information.

(3) NOTICE TO DEPARTMENT OF SECURITY BREACH

(a) A covered entity shall provide notice to the department of any breach of security affecting 500 or more individuals in this state. Such notice must be provided to the department as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach occurred. A covered entity may receive 15 additional days to provide notice as required in subsection (4) if good cause for delay is provided in writing to the department within 30 days after determination of the breach or reason to believe a breach occurred.

(b) The written notice to the department must include:

1. A synopsis of the events surrounding the breach at the time notice is provided.

2. The number of individuals in this state who were or potentially have been affected by the breach.

3. Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions as to how to use such services.

4. A copy of the notice required under subsection (4) or an explanation of the other actions taken pursuant to subsection (4).

5. The name, address, telephone number, and e-mail address of the employee or agent of the covered entity from whom additional information may be obtained about the breach.

(c) The covered entity must provide the following information to the department upon its request:

1. A police report, incident report, or computer forensics report.

2. A copy of the policies in place regarding breaches.

3. Steps that have been taken to rectify the breach.

(d) A covered entity may provide the department with supplemental information regarding a breach at any time.

(e) For a covered entity that is the judicial branch, the Executive Office of the Governor, the Department of Financial Services, or the Department of Agriculture and Consumer Services, in lieu of providing the written notice to the department, the covered entity may post the information described in subparagraphs (b)1.-4. on an agency-managed website.

(4) NOTICE TO INDIVIDUALS OF SECURITY BREACH

(a) A covered entity shall give notice to each individual in this state whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach. Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to a delay authorized under paragraph (b) or waiver under paragraph (c).

(b) If a federal, state, or local law enforcement agency determines that notice to individuals required under this subsection would interfere with a criminal investigation, the notice shall be delayed upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay as of a specified date or extend the period set forth in the original request made under this paragraph to a specified date if further delay is necessary.

(c) Notwithstanding paragraph (a), notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed. Such a determination must be documented in writing and maintained for at least 5 years. The covered entity shall provide the written determination to the department within 30 days after the determination.

(d) The notice to an affected individual shall be by one of the following methods:

1. Written notice sent to the mailing address of the individual in the records of the covered entity; or

2. E-mail notice sent to the e-mail address of the individual in the records of the covered entity.

(e) The notice to an individual with respect to a breach of security shall include, at a minimum:

1. The date, estimated date, or estimated date range of the breach of security.

2. A description of the personal information that was accessed or reasonably believed to have been accessed as a part of the breach of security.

3. Information that the individual can use to contact the covered entity to inquire about the breach of security and the personal information that the covered entity maintained about the individual.

(f) A covered entity required to provide notice to an individual may provide substitute notice in lieu of direct notice if such direct notice is not feasible because the cost of providing notice would exceed $250,000, because the affected individuals exceed 500,000 persons, or because the covered entity does not have an e-mail address or mailing address for the affected individuals. Such substitute notice shall include the following:

1. A conspicuous notice on the Internet website of the covered entity if the covered entity maintains a website; and

2. Notice in print and to broadcast media, including major media in urban and rural areas where the affected individuals reside.

(g) Notice provided pursuant to rules, regulations, procedures, or guidelines established by the covered entity's primary or functional federal regulator is deemed to be in compliance with the notice requirement in this subsection if the covered entity notifies affected individuals in accordance with the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security. Under this paragraph, a covered entity that timely provides a copy of such notice to the department is deemed to be in compliance with the notice requirement in subsection (3).

(5) NOTICE TO CREDIT REPORTING AGENCIES

If a covered entity discovers circumstances requiring notice pursuant to this section of more than 1,000 individuals at a single time, the covered entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. s. 1681a(p), of the timing, distribution, and content of the notices.

(6) NOTICE BY THIRD-PARTY AGENTS; DUTIES OF THIRD-PARTY AGENTS; NOTICE BY AGENTS

(a) In the event of a breach of security of a system maintained by a third-party agent, such third-party agent shall notify the covered entity of the breach of security as expeditiously as practicable, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred. Upon receiving notice from a third-party agent, a covered entity shall provide notices required

under subsections (3) and (4). A third-party agent shall provide a covered entity with all information that the covered entity needs to comply with its notice requirements.

(b) An agent may provide notice as required under subsections (3) and (4) on behalf of the covered entity; however, an agent's failure to provide proper notice shall be deemed a violation of this section against the covered entity.

(7) ANNUAL REPORT

By February 1 of each year, the department shall submit a report to the President of the Senate and the Speaker of the House of Representatives describing the nature of any reported breaches of security by governmental entities or third-party agents of governmental entities in the preceding calendar year along with recommendations for security improvements. The report shall identify any governmental entity that has violated any of the applicable requirements in subsections (2)-(6) in the preceding calendar year.

(8) REQUIREMENTS FOR DISPOSAL OF CUSTOMER RECORDS

Each covered entity or third-party agent shall take all reasonable measures to dispose, or arrange for the disposal, of customer records containing personal information within its custody or control when the records are no longer to be retained. Such disposal shall involve shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

(9) ENFORCEMENT

(a) A violation of this section shall be treated as an unfair or deceptive trade practice in any action brought by the department under s. 501.207 against a covered entity or third-party agent.

(b) In addition to the remedies provided for in paragraph (a), a covered entity that violates subsection (3) or subsection (4) shall be liable for a civil penalty not to exceed $500,000, as follows:

1. In the amount of $1,000 for each day up to the first 30 days following any violation of subsection (3) or subsection (4) and, thereafter, $50,000 for each subsequent 30-day period or portion thereof for up to 180 days.

2. If the violation continues for more than 180 days, in an amount not to exceed $500,000.

The civil penalties for failure to notify provided in this paragraph apply per breach and not per individual affected by the breach.

(c) All penalties collected pursuant to this subsection shall be deposited into the General Revenue Fund.

(10) NO PRIVATE CAUSE OF ACTION

This section does not establish a private cause of action.

(11) PUBLIC RECORDS EXEMPTION

(a) All information received by the department pursuant to a notification required by this section, or received by the department pursuant to an investigation by the department or a law enforcement agency, is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution, until such time as the investigation is completed or ceases to be active. This exemption shall be construed in conformity with s. 119.071(2)(c).

(b) During an active investigation, information made confidential and exempt pursuant to paragraph (a) may be disclosed by the department:

1. In the furtherance of its official duties and responsibilities;

2. For print, publication, or broadcast if the department determines that such release would assist in notifying the public or locating or identifying a person that the department believes to be a victim of a data breach or improper disposal of customer records, except that information made confidential and exempt by paragraph (c) may not be released pursuant to this subparagraph; or

3. To another governmental entity in the furtherance of its official duties and responsibilities.

(c) Upon completion of an investigation or once an investigation ceases to be active, the following information received by the department shall remain confidential and exempt from s. 119.07(1) and s. 24(a)**,** Art. I of the State Constitution:

1. All information to which another public records exemption applies.

2. Personal information.

3. A computer forensic report.

4. Information that would otherwise reveal weaknesses in a covered entity's data security.

5. Information that would disclose a covered entity's proprietary information.

(d) For purposes of this subsection, the term "proprietary information" means information that:

1. Is owned or controlled by the covered entity.

2. Is intended to be private and is treated by the covered entity as private because disclosure would harm the covered entity or its business operations.

3. Has not been disclosed except as required by law or a private agreement that provides that the information will not be released to the public.

4. Is not publicly available or otherwise readily as Certain able through proper means from another source in the same configuration as received by the department.

5. Includes:

a. Trade secrets as defined in s. 688.002.

b. Competitive interests, the disclosure of which would impair the competitive business of the covered entity who is the subject of the information.

History.— s. 3, ch. 2014-189; s. 1, ch. 2014-190; s. 1, ch. 2019-32.

Hawai'i Government Cyber-security Act

This bill to be entitled and enacted within the state of Hawai'i addresses need for "local government" to report to state entities ransomware and cyber-security events. Bill language was last updated in this document March 2023.

A bill to be entitled.

An act relating to cyber-security; amending s.282.0041, F.S.; revising a definition and defining the term "ransomware incident"; amending s. 282.318, F.S. requiring the Department of Management Services, acting through the Hawai'i Digital Service, to develop and publish guidelines and processes for reporting cyber-security incidents; requiring state agencies to report ransomware incidents and Certain cyber-security incidents to Certain entities within specifies timeframes; requiring the Cyber-security Operations Center to provide Certain notifications to the Legislature within a specified timeframe; requiring the Cyber-security Operations Center to quarterly
provide Certain reports to the Legislature and the Hawai'i Cyber-security Advisory Council; requiring the department, acting through the Hawai'i Digital Service, to develop and publish guidelines and processes by a specified date for submitting after action reports and annually provide cyber-security training to Certain persons; requiring state agency heads to annually provide cyber-security awareness training to Certain persons; requiring state agencies to report cyber-security incidents and ransomware incidents in compliance with Certain procedures and timeframes; requiring state agency heads to submit Certain after-action reports to the Hawai'i Digital Service within a specified timeframe; creating s.282.3185, F.S.; providing a short title; defining the term "local government"; requiring the Hawai'i Digital Service to develop Certain cyber-security training curricula; requiring Certain persons to complete Certain cyber-security training within a specified timeframe and annually thereafter; authorizing the Hawai'i Digital Service to provide a Certain training in collaboration with Certain entities; requiring Certain local governments to adopt Certain cyber-security standards by specified dates; requiring local governments to provide a Certain notification to the Hawai'i Digital Service and Certain entities; providing notification requirements; requiring local governments to report ransomware incidents and Certain cyber-security incidents to Certain entities within specified timeframes; requiring the Cyber-security Operations Center to provide a Certain notification to the Legislature within a specified timeframe; authorizing local governments to report Certain cyber-security incidents to Certain entities; requiring the Cyber-security Operations Center to quarterly provide Certain reports to the Legislature and the Hawai'i Cyber-security Advisory Council; requiring local governments to submit after-action reports containing Certain information to the Hawai'i Digital Service within a specified timeframe; requiring the Hawai'i Digital Service to establish Certain guidelines and processes by a specified date; creating s. 282.3186, F.S.; prohibiting Certain entities from paying or otherwise complying with a ransom demand; amending s. 282.319, F.S.; revising the purpose of the Hawai'i Cyber-security Advisory Council to include advising counties and municipalities on cyber-security; requiring the council to meet at least quarterly to review Certain information and develop and make Certain recommendations; requiring the council to annually submit to the Governor and the Legislature a Certain ransomware incident report beginning on a specified date; providing requirements for the report; defining the term "state agency"; creating s. 815.062, F.S.; defining the term "governmental entity"; prohibiting Certain persons from introducing computer contaminants in order to

procure a ransom; prohibiting Certain employees or contractors from aiding or abetting another to introduce computer contaminants in order to procure a ransom; providing criminal penalties; requiring a person convicted of Certain offenses to pay a Certain fine; requiring deposit of Certain moneys in the General Revenue Fund; providing a legislative finding and declaration of an important state interest; providing an effective date.

Enacted by the Legislature of the State of Hawai'i:

Section 1.
Present subsections (28) through (37) of section 041, Hawai'i Statutes, are redesignated as subsections (29) through (38), respectively, a new subsection (28) is added to that section, and subsection (19) of that section is amended, to read:

282.0041 Definitions

As used in this chapter, the term:

(19) "Incident" means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology resources, security, policies, or practices. An imminent threat of violation refers to a situation in which the state agency, county, or municipality has a factual basis for believing that a specific incident is about to occur.

(28) "Ransomware incident" means a malicious cyber-security incident in which a person or entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable a state agency's, county's, or municipality's data and thereafter the person or entity demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software.

Section 2.
Paragraphs (c) and (g) of subsection (3) and paragraphs (i) and (j) of subsection (4) of section 282.318, Hawai'i Statutes, are amended, and paragraph (k) is added to subsection (4) of that section, to read:

282.318 Cyber-security

(3) The department, acting through the Hawai'i Digital Service, is the lead entity responsible for establishing standards and processes for assessing state agency cyber-security risks and determining appropriate security measures. Such standards and processes must be consistent with generally accepted technology best practices, including the National Institute for Standards and Technology Cyber-security Framework, for cyber-security. The department, acting through the Hawai'i Digital Service, shall adopt rules that mitigate risks; safeguard state agency digital assets, data, information, and information technology resources to ensure availability, confidentiality, and integrity; and support a security governance framework. The department, acting through the Hawai'i Digital Service, shall also:

(c) Develop and publish for use by state agencies a cyber-security governance framework that, at a minimum, includes guidelines and processes for:

1. Establishing asset management procedures to ensure that an agency's information technology resources are identified and managed consistently with their relative importance to the agency's business objectives.

2. Using a standard risk assessment methodology that includes the identification of an agency's priorities, constraints, risk tolerances, and assumptions necessary to support operational risk decisions.

3. Completing comprehensive risk assessments and cyber-security audits, which may be completed by a private sector vendor, and submitting completed assessments and audits to the department.

4. Identifying protection procedures to manage the protection of an agency's information, data, and information technology resources.

5. Establishing procedures for accessing information and data to ensure the confidentiality, integrity, and availability of such information and data.

6. Detecting threats through proactive monitoring of events, continuous security monitoring, and defined detection processes.

7. Establishing agency cyber-security incident response teams and describing their responsibilities for responding to cyber-security incidents, including breaches of personal information containing confidential or exempt data.

8. Recovering information and data in response to a Cyber-security incident. The recovery may include recommended improvements to the agency processes, policies, or guidelines.

9. Establishing a cyber-security incident reporting process that includes procedures and tiered reporting timeframes for notifying the department and the Department of Law Enforcement of cyber-security incidents. The tiered reporting timeframes shall be based upon the level of severity of the cyber-security incidents being reported.

> **a.** The level of severity of the cyber-security incident is defined by the National Cyber Incident Response Plan of the United States Department of Homeland Security as follows:
>
> > **(I)** Level 5 is an emergency-level incident within the specified jurisdiction that poses an imminent threat to the provision of wide-scale critical infrastructure services; national, state, or local government security; or the lives of the country's, state's, or local government's residents.
> >
> > **(II)** Level 4 is a severe-level incident that is likely to result in a significant impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; or civil liberties.

(III) Level 3 is a high-level incident that is likely to result in a demonstrable impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

(IV) Level 2 is a medium-level incident that may impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

(V) Level 1 is a low-level incident that is unlikely to impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

b. The cyber-security incident reporting process must specify the information that must be reported by a state agency following a cyber-security incident or ransomware incident, which, at a minimum, must include the following:

(I) A summary of the facts surrounding the cyber-security incident or ransomware incident.

(II) The date on which the state agency most recently backed up its data, the physical location of the backup, if the backup was affected, and if the backup was created using cloud computing.

(III) The types of data compromised by the cyber-security incident or ransomware incident.

(IV) The estimated fiscal impact of the cyber-security incident or ransomware incident.

(V) In the case of a ransomware incident, the details of the ransom demanded.

c. (I) A state agency shall report all ransomware incidents and any cyber-security incident determined by the state agency to be of severity level 3, 4, or 5 to the Cyber-security Operations Center and the Cybercrime Office of the Department of Law Enforcement as soon as possible but no later than 48 hours after discovery of the cyber-security incident and no later than 12 hours after discovery of the ransomware incident. The report must contain the information required in sub-subparagraph b.

(II) The Cyber-security Operations Center shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incident as soon as possible but no later than 12 hours after receiving a state agency's incident report. The notification must include a high-level description of the incident and the likely effects.

d. A state agency shall report a cyber-security incident determined by the state agency to be of severity level 1 or 2 to the Cyber-security Operations Center and the Cybercrime Office of the Department of Law Enforcement as soon as possible. The report must contain the information required in sub-subparagraph b.

e. The Cyber-security Operations Center shall provide a consolidated incident report on a quarterly basis to the President of the Senate, the Speaker of the House of Representatives, and the Hawai'i Cyber-security Advisory Council. The report provided to the Hawai'i Cyber-security Advisory Council may not contain the name of any agency, network information, or system identifying information but must contain sufficient relevant information to allow the Hawai'i Cyber-security Advisory Council to fulfill its responsibilities as required in s. 282.319(9).

10. Incorporating information obtained through detection and response activities into the agency's cyber-security incident response plans.

11. Developing agency strategic and operational cyber-security plans required pursuant to this section.

12. Establishing the managerial, operational, and technical safeguards for protecting state government data and information technology resources that align with the state agency risk management strategy and that protect the confidentiality, integrity, and availability of information and data.

13. Establishing procedures for procuring information technology commodities and services that require the commodity or service to meet the National Institute of Standards and Technology Cyber-security Framework.

14. Submitting after-action reports following a cyber-security incident or ransomware incident. Such guidelines and processes for submitting after-action reports must be developed and published by December 1, 2022.

(g) Annually provide cyber-security training to all state agency technology professionals and employees with access to highly sensitive information which develops, assesses, and documents competencies by role and skill level. The cyber-security training curriculum must include training on the identification of each cyber-security incident severity level referenced in sub-subparagraph (c) 9.a. The training may be provided in collaboration with the Cybercrime Office of the Department of Law Enforcement, a private sector entity, or an institution of the State University System.

(4) Each state agency head shall, at a minimum:

(i) Provide cyber-security awareness training to all state agency employees within the first 30 days after commencing employment, and annually thereafter, concerning cyber-security risks and the responsibility of employees to comply with policies, standards, guidelines, and operating procedures adopted by the state agency to reduce those risks. The training may be provided in collaboration with the Cybercrime Office of the Department of Law Enforcement, a private sector entity, or an institution of the State University System.

(j) Develop a process for detecting, reporting, and responding to threats, breaches, or cyber-security incidents which is consistent with the security rules, guidelines, and processes established by the department through the Hawai'i Digital Service.

1. All cyber-security incidents and ransomware breaches must be reported by state agencies. Such reports to the Hawai'i Digital Service within the department and the Cybercrime Office of the Department of Law Enforcement and must comply with the notification procedures and reporting timeframes established pursuant to paragraph (3)(c).

2. For cyber-security breaches, state agencies shall provide notice in accordance with s. 501.171.

(k) Submit to the Hawai'i Digital Service, within 1 week after the remediation of a cyber-security incident or ransomware incident, an after-action report that summarizes the incident, the incident's resolution, and any insights gained as a result of the incident.

Section 3.

Section 282.3185, Hawai'i Statutes, is created to read:

282.3185 Local government cyber-security.

(1) SHORT TITLE

This section may be cited as the "Local Government Cyber-security Act."

(2) DEFINITION

As used in this section, the term "local government" means any county or municipality.

(3) CYBER-SECURITY TRAINING.

(a) The Hawai'i Digital Service shall:

1. Develop a basic cyber-security training curriculum for local government employees. All local government employees with access to the local government's network must complete the basic cyber-security training within 30 days after commencing employment and annually thereafter.

2. Develop an advanced cyber-security training curriculum for local governments which is consistent with the cyber-security training required under s. 282.318(3)(g). All local government technology professionals and employees with access to highly sensitive information must complete the advanced cyber-security training within 30 days after commencing employment and annually thereafter.

(b) The Hawai'i Digital Service may provide the cyber-security training required by this subsection in collaboration with the Cybercrime Office of the Department of Law Enforcement, a private sector entity, or an institution of the State University System.

(4) CYBER-SECURITY STANDARDS

(a) Each local government shall adopt cyber-security standards that safeguard its data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The cyber-security standards must be consistent with generally accepted best practices for cyber-security, including the National Institute of Standards and Technology Cyber-security Framework.

(b) Each county with a population of 75,000 or more must adopt the cyber-security standards required by this subsection by January 1, 2024. Each county with a population of less than 75,000 must adopt the cyber-security standards required by this subsection by January 1, 2025.

(c) Each municipality with a population of 25,000 or more must adopt the cyber-security standards required by this subsection by January 1, 2024. Each municipality with a population of less than 25,000 must adopt the cyber-security standards required by this subsection by January 1, 2025.

(d) Each local government shall notify the Hawai'i Digital Service of its compliance with this subsection as soon as possible.

(5) INCIDENT NOTIFICATION

(a) A local government shall provide notification of a cyber-security incident or ransomware incident to the Cyber-security Operations Center, Cybercrime Office of the Department of Law Enforcement, and sheriff who has jurisdiction over the local government in accordance with paragraph (b). The notification must include, at a minimum, the following information:

1. A summary of the facts surrounding the cyber-security incident or ransomware incident.

2. The date on which the local government most recently backed up its data, the physical location of the backup, if the backup was affected, and if the backup was created using cloud computing.

3. The types of data compromised by the cyber-security incident or ransomware incident.

4. The estimated fiscal impact of the cyber-security incident or ransomware incident.

5. In the case of a ransomware incident, the details of the ransom demanded.

6. A statement requesting or declining assistance from the Cyber-security Operations Center, the Cybercrime Office of the Department of Law Enforcement, or the sheriff who has jurisdiction over the local government.

(b)1. A local government shall report all ransomware incidents and any cyber-security incident determined by the local government to be of severity level 3, 4, or 5 as provided in s. 282.318(3)(c) to the Cyber-security Operations Center, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government as soon as possible but no later than 48 hours after discovery of the cyber-security incident and no later than 12 hours after discovery of the ransomware incident. The report must contain the information required in paragraph (a).

2. The Cyber-security Operations Center shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incident as soon as possible but no later than 12 hours after receiving a local government's incident report. The notification must include a high-level description of the incident and the likely effects.

(c) A local government may report a cyber-security incident determined by the local government to be of severity level 1 or 2 as provided in s. 282.318(3)(c) to the Cyber-security Operations Center, the Cybercrime Office of the

Department of Law Enforcement, and the sheriff who has jurisdiction over the local government. The report shall contain the information required in paragraph (a).

(d) The Cyber-security Operations Center shall provide a consolidated incident report on a quarterly basis to the President of the Senate, the Speaker of the House of Representatives, and the Hawai'i Cyber-security Advisory Council. The report provided to the Hawai'i Cyber-security Advisory Council may not contain the name of any local government, network information, or system identifying information but must contain sufficient relevant information to allow the Hawai'i Cyber-security Advisory Council to fulfill its responsibilities as required in s. 282.319(9).

(6) After-Action REPORT

A local government must submit to the Hawai'i Digital Service, within 1 week after the remediation of a cyber-security incident or ransomware incident, an after-action report that summarizes the incident, the incident's resolution, and any insights gained as a result of the incident. By December 1, 2022, the Hawai'i Digital Service shall establish guidelines and processes for submitting an after-action report.

Section 4.

Section 282.3186, Hawai'i Statutes, is created to read:

282.3186 Ransomware incident compliance.

A state agency as defined in s. 282.318(2), a county, or a municipality experiencing a ransomware incident may not pay or otherwise comply with a ransom demand.

Section 5.

Subsection (2) of section 282.319, Hawai'i Statutes, is amended, paragraphs (g) and (h) are added to subsection (9) of that section, and subsections (12) and (13) are added to that section, to read:

282.319 Hawai'i Cyber-security Advisory Council.

(2) The purpose of the council is to:

(a) Assist state agencies in protecting their information technology resources from cyber-security cyber threats and incidents.

(b) Advise counties and municipalities on cyber-security, including cyber-security threats, trends, and best practices.

(9) The council shall meet at least quarterly to:

(g) Review information relating to cyber-security incidents and ransomware incidents to determine commonalities and develop best practice recommendations for state agencies, counties, and municipalities.

(h) Recommend any additional information that a county or municipality should report to the Hawai'i Digital Service as part of its cyber-security incident or ransomware incident notification pursuant to s. 282.3185.

(12) Beginning December 1, 2022, and each December 1 thereafter, the council shall submit to the Governor, the President of the Senate, and the Speaker of the House of Representatives a comprehensive report that includes data, trends, analysis, findings, and recommendations for state and local action regarding ransomware incidents. At a minimum, the report must include:

(a) Descriptive statistics including the amount of ransom requested, duration of the ransomware incident, and overall monetary cost to taxpayers of the ransomware incident.

(b) A detailed statistical analysis of the circumstances that led to the ransomware incident which does not include the name of the state agency, county, or municipality; network information; or system identifying information.

(c) A detailed statistical analysis of the level of cyber-security employee training and frequency of data backup for the state agency, county, or municipality that reported the ransomware incident.

(d) Specific issues identified with current policies, procedures, rules, or statutes and recommendations to address such issues.

(e) Any other recommendations to prevent ransomware incidents.

(13) For purposes of this section, the term "state agency" has the same meaning as provided in s. 282.318(2).

Section 6.
Section 815.062, Hawai'i Statutes, is created to read:

815.062 Offenses against governmental entities.

(1) As used in this section, the term "governmental entity" means any official, officer, commission, board, authority, council, committee, or department of the executive, judicial, or legislative branch of state government; any state university; or any county or municipality, special district, water management district, or other political subdivision of the state.

(2) A person who willfully, knowingly, and without authorization introduces a computer contaminant that gains unauthorized access to, encrypts, modifies, or otherwise renders unavailable data, programs, or supporting documentation residing or existing within a computer, computer system, computer network, or electronic device owned or operated by a governmental entity and demands a ransom to prevent the publication of or restore access to the data, programs, or supporting documentation or to otherwise remediate the impact of the computer contaminant commits a felony of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(3) An employee or contractor of a governmental entity with access to the governmental entity's network who willfully and knowingly aids or abets another in the commission of a violation of subsection (2) commits a felony of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

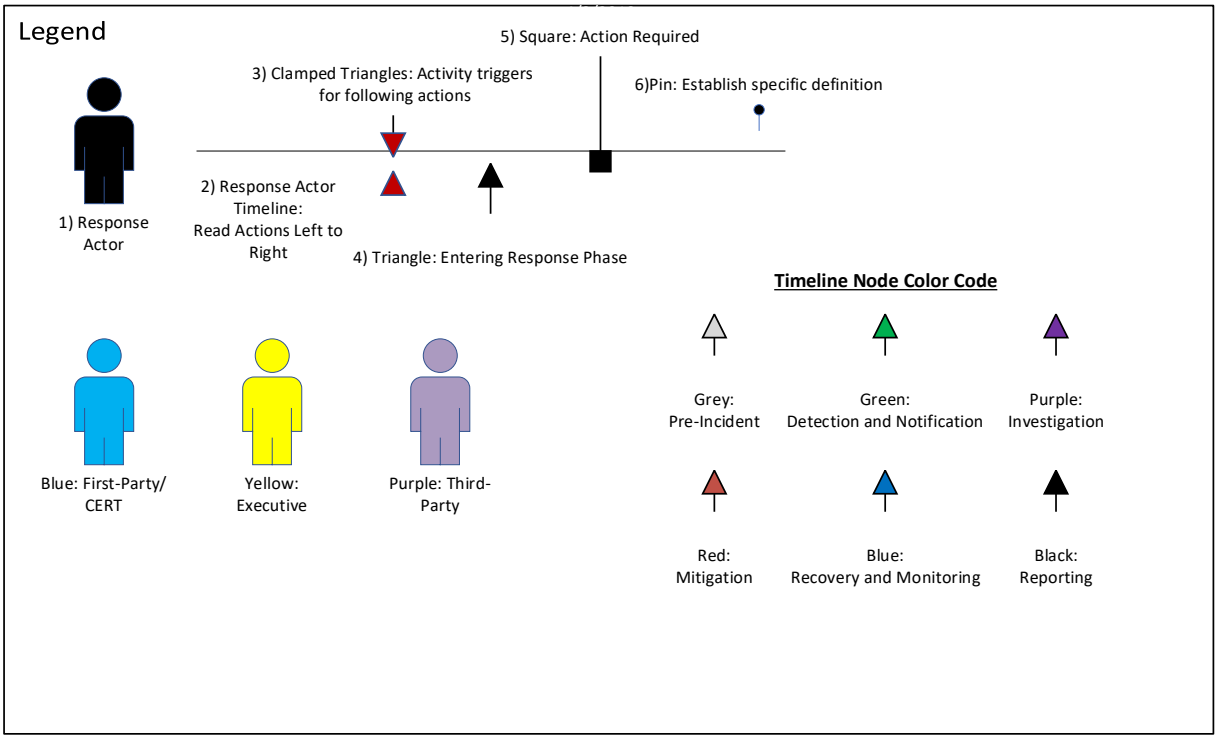
(4) In addition to any other penalty imposed, a person convicted of a violation of this section must pay a fine equal to twice the amount of the ransom demand. Moneys recovered under this subsection shall be deposited into the

General Revenue Fund.

Section 7.
The Legislature finds and declares that this act fulfills an important state interest.

Section 8.
This act shall take effect July 1, 2022

APPENDIX E: SAMPLE DIAGRAM LEGEND



1 1) Response Actor
The person who is responsible for actions on the associated timeline.

2) Response Actor Timeline
Read symbol on this line from left to right. The associated response actor is responsible for activity on this timeline.

3) Clamped Triangle
These nodes identify activity and conditions that are required to be met before proceeding to any following actions on the timeline.

4) Triangle

These nodes indicate the following action nodes occur during the indicated response phase.

5) Square

Action nodes indicate activity that must be performed by the response actor owning the timeline if the preceding conditions are met.

6) Pin

Pins denote a definition that should apply to an incident if a point of conditions is reached. This is typically an escalation or de-escalation of the incident definition in response to the conditions and actions that may pre-cede the pin on the timeline.

APPENDIX F: CYBER INCIDENT REPORT

Confidence Severity Type Breach Pick date.

Reported By:

Incident Summary:

IRT Convened? ☐
Incident Handlers:

Summary of Response Actions Taken

Investigation:

Mitigation:

Recovery and Monitoring:

Reporting:

Evidence\Key Information Collected

APPENDIX G: INCIDENT AFTER-ACTION REPORT

Confidence Severity Type Breach Pick date.

Post-Mortem Participants:

Incident Summary	Time to Detect: .Time Frame	Time to Resolve: Time Frame.

Summarize the Incident:

5y Root Analysis

Stated Problem)

Y1)

Y2)

Y3)

Y4)

Y5)

Clarify the Problem

Is quantifiably:

Is quantifiably not:

Supporting Data/Analysis

5y Root Analysis

Stated Problem)

Y1)

Y2)

Y3)

Y4)

Y5)

Clarify the Problem

Is quantifiably:

Is quantifiably not:

Supporting Data/Analysis

Security Plan Name	Approval:New	Status:New	Last Review:Pick Date.

Plan Owner:
Plan Schedule:
Required Resources:

Summarize plan details.

Plan Validation

Plan Standardization

Security Plan Name	Approval:New	Status:New	Last Review:Pick Date.

Plan Owner:
Plan Schedule:
Required Resources:

Summarize plan details.

Plan Validation

Plan Standardization

Security Plan Name	Approval:New	Status:New	Last Review:Pick Date.

Plan Owner:
Plan Schedule:
Required Resources:

Summarize plan details.

Plan Validation

Plan Standardization

Security Plan Name	Approval:New	Status:New	Last Review:Pick Date.

Plan Owner:
Plan Schedule:
Required Resources:

Summarize plan details.

Plan Validation

Plan Standardization

Security Plan Name	Approval:New	Status:New	Last Review:Pick Date.

Plan Owner:
Plan Schedule:
Required Resources:

Summarize plan details.

Plan Validation

Plan Standardization

APPENDIX H: COMMUNICATION TEMPLATES

Communications to the public or general employees during an incident should remain limited in description, and not provide indication of the ongoing incident/cyber-attack. Communications stating the true nature, impact and resolution of the incident will be generated only upon advisement by law support, the legal team and cyber-insurance carrier's post breach support.

Communications shall be crafted within the following content framework:

1. Generic statement of service disruption.
2. Estimation of outage
3. Work arounds mitigations or expectations for the recipient parties during the incident.
4. How to make contact for more information (in appropriate scenarios)
5. Where\how the recipient will receive further updates on the scenario.

Active Cyber Attack Affecting Services (Internal)

That OHS is currently experiencing technical difficulties interfering with our normal functions. By dedicating all appropriate resources to resolving these issues we expect to resume normal functions by <time>.
Until we resume normal functions, your supervisor may direct you to other duties or provide further instruction on how to continue completing your primary functions.
For more information, please contact your supervisor or our help line <###-###-#####>.
We will continue to provide further updates on this situation by e-mail until resolved.
Thank you for your patience as we work to resolve these problems.

Active Cyber Attack Affecting Services (Public Notice)

That OHS is currently experiencing technical difficulties interfering with our normal functions. By dedicating all appropriate resources to resolving these issues we expect to resume normal functions by <time>.
Until we resume normal functions, <here is what you can do>
For more information please contact visit our website at <> or contact our help line <###-###-#####>.
We will continue to provide further updates on our website at <> or follow us on social media <@>

Personal Information Breach (Affected Persons Public Notice)

The OHS recently experienced a security issue that involved a number of citizens' personal data. We want to make sure you have the facts regarding what happened, what information was affected and the actions we are taking to protect you.

What Happened?
On <Date>, we became aware <briefly describe the discovery of the data breach.> We took immediate steps to mitigate the breach by <briefly describe initial mitigation steps. Detail whether Law Enforcement

or other government contacts were alerted.>

What Information Was Involved?
Email Addresses, passwords, favorite cake recipes, number of cats in the household and their names.

What Are We Doing?
We have determined the computer system error that allowed the breach and corrected it using the system vendor's security update. We have investigated the affected systems and determined the specific accounts involved. We are using automated tools to identify and block any suspicious activity with the compromised accounts or systems. We are also actively engaging with law enforcement agencies.

What Can You Do?
<Instructions related to credit monitoring services if provided>
To prevent new accounts from being authorized in your name we recommend you lock or freeze your credit. These services are freely provided by all major credit bureaus.

Experian	https://www.experian.com/freeze/center.html
Equifax	https://www.equifax.com/personal/credit-report-services/credit-freeze/
TransUnion	https://www.transunion.com/credit-freeze

We recommend that you regularly change passwords for any online account you have with the OHS. If you use the same or similar password on other online services, we recommend you set new passwords on those accounts as well.

For More Information:
If you have further questions, please feel free to contact us through our website <web URL>

Personal Information Breach (Affected Persons Personal Notice)

To <Addressee>
Dear <person,>
The OHS recently suffered a computer data breach that included your personal information. We want to make sure you have the facts regarding what happened, what information was affected and the actions we are taking to protect you.

What Happened?
On <Date>, we became aware <briefly describe the discovery of the data breach.> We took immediate steps to mitigate the breach by <briefly describe initial mitigation steps. Detail whether Law Enforcement or other government contacts were alerted.>

What Information Was Involved?
Your email addresses passwords and Aunt Margie's Bodacious Chocolate cake recipe

What Are We Doing?
We have determined the computer system error that allowed the breach and corrected it using the system vendor's security update. We have investigated the affected systems and determined the specific

accounts involved. We are using automated tools to identify and block any suspicious activity with the compromised accounts or systems. We are also actively engaging with law enforcement agencies.

What Can You Do?

<Instructions related to credit monitoring services if provided>

To prevent new accounts from being authorized in your name we recommend you lock or freeze your credit. These services are freely provided by all major credit bureaus.

Experian	https://www.experian.com/freeze/center.html
Equifax	https://www.equifax.com/personal/credit-report-services/credit-freeze/
TransUnion	https://www.transunion.com/credit-freeze

We recommend that you regularly change passwords for any online account you have with the OHS. If you use the same or similar password on other online services, we recommend you set new passwords on those accounts as well.

Appendix I: Document Revisions

Date	Version	Comments
3/8/2023	1.0	Initial Draft In Progress (Cyberstone)