Procedure - Information Security Incident Management

Purpose
This procedure defines the requirements for reporting and responding to incidents related to ESD information systems and operations.

Requirements
The following items specify the incident management plan requirements. These requirements shall be in compliance with relevant laws.

The ESD management shall ensure that:

1. Incidents are detected as soon as possible and properly reported.
2. Incidents are handled by appropriate authorized personnel with skilled alternates as required.
3. Incidents are properly recorded.
4. All evidence is gathered, recorded and maintained to withstand internal and external scrutiny.
5. The full extent and implications relating to an incident are understood.
6. Incidents are dealt with in a timely manner and service(s) restored as soon as possible.
7. Similar incidents will likely not recur.
8. Any weaknesses in procedures or operating practices are identified and addressed.
9. The risk to ESD's reputation through negative exposure is minimized.
10. All incidents shall be analyzed and reported to the designated officer(s).

Incident Response Plan
ESD must maintain a documented Incident Response Plan to provide a well-defined and organized approach for handling any potential threat to systems and informational assets. The Incident Response Plan must ensure that appropriate leadership from organization entities (business owners, system owners, HR, physical security, legal, operations, procurement, risk executives, and others) and technical resources are established to coordinate incident response activities. Incident response activities that include Preparation, Identification (detection and analysis), Containment, Eradication, Recovery, and Lessons learned (post-incident activity) (PICERL). The incident response plan shall be reviewed and updated on an annual basis, as changes arise in the environment, and/or as lessons are learned from real-world incidents and training exercises.

The Incident Response Plan must establish, maintain, and follow documented incident management procedures to ensure rapid, effective, and consistent response to security incidents. The plan must include relevant topics including:

- Incident response planning and preparation
- Monitoring, detecting, analyzing, and reporting of information security events and incidents
- Establish an incident tracking system

- Logging incident management activities with an established place and way to store these (encrypted)
- Handling of forensic evidence; Establish a place and way to store evidence (encrypted)
- Maintain a prioritization and severity rating for various events and incident types. Establish performance measures (SLA) for each
- Maintain pre-defined incident response actions for events and incidents; review at least annually but this should be a living document that is updated regularly
- Maintain an internal contact roster
- Establish and maintain an incident communications plan for use during an incident
- Establish hardware and software requirements for analyzing incidents and review annually
- Remediation runbooks of common security incident types
- Post-mortem and root cause analysis of the incident
- Maintain a roles and responsibilities matrix, including the definition of a designated Information Security Incident Response Team (CIRT) led by the Designated Information Security Officer (ISO)
- Training requirements and frequency for each role. This should include any training for average users to identify suspicious behaviors and anomalous events
- Maintain a list of external authorities (local law enforcement, FBI, Office of the Washington State Auditor, special interest groups, or forums that handle the issues related to information security incidents) who can assist in an incident and when contacting / notifying these authorities is appropriate.

Event Detection
An event is any observable occurrence on the network. Events can be detected in several ways such as loss of productivity, alarms & alerts from systems, notifications from other organizations, or results from various assessments. All security events must be investigated to determine if they are a security incident using the incident triage and response processes. This includes automated alerts and employee-reported suspicious or anomalous events.

Event Reporting
Employees and contractors detecting any anomalous or suspicious events are required to immediately report those events to the Help Center or a manager. Confirmed suspicious events must be reported to the Information Security team or the ISO. Individuals reporting a suspected security event should be provided feedback on its resolution whenever possible.

Analyze and Triage Events
Establish a plan to analyze, triage, and prioritize (rate) events. This plan should contain a priority and rating scheme to support a quick resolution to events and if necessary, declare an incident. Once triage determines the priority of an event, the appropriate pre-planned response should be taken. Low priority or low impact events should result in closure of the event and no actions taken. High priority events should result in declaring an incident and the appropriate incident response plan activated.

Develop Responses to Incidents
Pre-approved response actions and procedures that the incident responders can take without having to seek approval will improve incident response times. Pre-approved response actions and

procedures to various incidents will be developed and made part of the incident response plan. New responses and procedures will be added/updated at least annually as new types of incidents become known and technologies change.

Track, Document, and Report Incidents
Documenting incidents creates the information necessary for evaluating incidents in detail, conducting forensics, evaluating trends, and updating incident response plans. Proper planning for secure communication, documentation transmission, and document storage is essential. A secure out-of-band communications plan and secure out-of-band central document repository will be established and maintained in a ready to use state in case an incident occurs. Tracking and documenting system security incidents includes maintaining records of each incident, documenting actions taken, and incident status.

Incident information can be obtained from a variety of sources including incident reports, IR teams, log monitoring, network monitoring, physical access monitoring, and user/administrator reports. This relevant information should be communicated and stored securely in a central repository for later examination and review.

Formal incident reporting requirements must be pre-defined for both internal (such as execs., affected business units, and other stake holders) and external (such as law enforcement, EO, directives, regulations, and policies) requirements. This should include the types of security incidents, who it should be reported to, level of content, and timelines for reporting.

Incident Root Cause Analysis
A post-incident review using root-cause analysis will be conducted within ten (10) working days following the closure of a security incident. This will include a formal examination of the causes of the incident and the responses to it. This examination will evaluate administrative, technical, and physical control weaknesses that may have allowed the incident to occur. Consideration of other processes that may have contributed should also be given (such as change management and configuration management).

After completion of the post incident analysis, the CIRT must develop an action plan that will reduce the likelihood of the incident's reoccurrence and improve organizational response capabilities. Actions to be taken may include:

- Updating response and recovery plans, policies, processes, and/or procedures
- Updating 3rd party tools
- New or modified technical controls or configurations
- Employee training and awareness topics

Incident Response Testing Requirements
Incident response exercises test incident response capabilities and help determine the effectiveness of incident response plans and help identify potential weaknesses or deficiencies. Incident response exercises should:

- Follow the appropriate incident response plan and any associated run books
- Address what happens during an incident
- Exercise as many roles and responsibilities as possible

- Include a debrief and feedback session
- End with updating the IR plans and procedures.

Incident Response testing exercises will be performed at least annually to validate organizational preparedness to carry out the Incident Response Plan. Testing exercises should include representatives from as many stakeholder groups as possible, including senior management, legal, communications, and IT. Exercises can tabletop exercises or technical exercises of various incident response techniques. Participation can be company internal or externally hosted exercises such as an industry sponsored exercise. Exercise scenarios should be derived from real-world attack scenarios and lessons learned from exercises should result in updates to the incident response plan and procedures.

Timeline for Implementation of Procedure

Given the required changes to ESD processes to fully implement this procedure, new technology systems will be subject to this procedure immediately while existing processes or systems will be reviewed as required by the procedure's periodic review. If an operating practice is needed from IT as part of the procedure, IT will develop and have implemented that process before running proposed technology system through it. Procedure to be fully implemented by September 1, 2024.