Procedure - Operations Security

Purpose
The purpose of this procedure is to ensure the integrity of information processing facilities and operating systems.

Information Processing Facility
This is defined as any equipment, operating systems, or infrastructure that are necessary or facilitate to process data completely, accurately, and effectively, such as IT equipment, applications, computer network systems, procedures, or information processing areas, etc. It only applies to information that is processed at ESD facilities, and not applications that are hosted as software-as-a-service, unless developed and maintained by ESD.

Documented Operations Practices
The operating practices as identified by this security procedure will be documented and maintained. Operating practices will be treated as formal documents and changes authorized by management.

The operating practices will specify the instructions for the detailed execution of each facility including:

- Processing and handling of information
- Scheduling requirements, including interdependencies with other systems
- Instructions for handling errors or other exceptional conditions, including restrictions on the use of system utilities
- Support contacts in the event of unexpected operational or technical difficulties
- System restart and recovery procedures for use in the event of system failure

Documented procedures will also be prepared for system housekeeping activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, back-up, equipment maintenance, computer room and mail handling management and safety.

IT will develop, implement, and review documentation for this.

Operational Change Control
Formal management responsibilities and procedures will be in place to ensure satisfactory control of all changes to equipment, software or procedures. Maintaining system integrity is the responsibility of the development group to whom the application system or software belongs with ESD oversight.

Operational programs must be subject to change control. When programs are changed, an audit log containing all relevant information must be retained. Wherever practicable, operational and application change control procedures will be integrated. The change control process will cover the following items:

- Identification and recording of significant changes
- Assessment of the potential impact of such changes
- Formal approval procedure for proposed changes
- Communication of change details to all relevant persons
- Procedures identifying responsibilities for aborting and recovering from unsuccessful changes
- Scheduling of changes (e.g., periodic change control windows)

Capacity Planning
To limit disruption to the network, applications, and business functions, ESD will monitor system capacity and plan for future capacity needs in sufficient time to procure system resources prudently. This will ensure adequate resources are available and reduce the possibility of system overload.

System owners shall monitor their equipment for current uses and projected capacity.

Separation of Development and Operational Facilities
Separating development, test and operational facilities is important to achieve segregation of the roles involved. Rules for the transfer of software from development to operational status must be defined and documented.

Development and testing activities may cause unintended changes to software and information if they share the same computing environment. Separating development, test and operational facilities is therefore desirable to reduce the risk of accidental change or unauthorized access to operational software and business data. The following controls must be implemented:

- Development and operational software will, where possible, run on different computer processors, or in different domains or directories
- Development and testing activities will be separated as far as possible
- Compilers, editors and other system utilities will not be accessible from operational systems when not required
- Different log-on procedures will be used for operational and test systems, to reduce the risk of error. Users will be encouraged to use different passwords for these systems, and menus will display appropriate identification messages.
- Development staff will only have access to operational passwords where controls are in place for issuing passwords for the support of operational systems. Controls will ensure that such passwords are changed after use.

Protection Against Malicious Software
ESD shall implement procedures, user awareness, and change controls to detect and prevent the introduction of malicious software into the organization's computing environment.

The ESD shall comply with the requirements of software licenses. No unauthorized or illegal software will be used.

Information Backup
Back-up copies of essential business information and software will be taken regularly. Adequate back-up facilities will be provided to ensure that all essential business information and software

can be recovered following a disaster or media failure. Back-up arrangements for individual systems will be regularly tested to ensure that they meet the requirements of business continuity plans.

- A minimum level of back-up information, together with accurate and complete records of the back-up copies and documented restoration procedures, will be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. At least three generations or cycles of back-up information will be retained for important business applications.
- Back-up information will be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site. The controls applied to media at the main site will be extended to cover the back-up site.
- Back-up media will be regularly tested, where practicable, to ensure that they can be relied upon for emergency use when necessary
- Restoration procedures will be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery. The retention period for essential business information, and also any requirement for archive copies to be permanently retained, will be determined.

Retention schedules will be adhered to for all information as defined in RCW 40.14.

User Computer Data Backup
To protect ESD's information resources from loss or damage, users are responsible for regularly backing up the information on their computers to cloud locations as specified and directed by IT.

Event Logging
ESD will log all security-relevant events or exceptions.

IT will be responsible for maintaining event logs.

Event logs will be retained for at least one year with at least 3 months of on-line retention.

The Designated Information Security Officer will monitor event logs at periodic intervals as determined based on data type. Automated log analysis and alerting will suffice for this provision.

Event logs will contain:

- User IDs used in logons
- Dates and times for logon and logoff for each user
- Terminal identity (system name and network address)
- Successful and rejected access attempts
- Successful or rejected data access attempts
- Use of elevated privileges through 'su' or 'run as'
- Any access to cardholder data (credit card numbers)

ESD will monitor the use of information processing facilities to detect unauthorized activities and ensure that users are only performing the functions and gaining access to information to which they are authorized.

Areas eligible for monitoring include:

- Authorized access:
    - User IDs
    - Date and time of key events
    - Types of events
    - Files accessed
    - Programs and utilities used
- Privileged operations:
    - Use of supervisor accounts
    - Use of other privileged accounts (i.e., administrator)
    - System start-up and stop
    - Devise attachment and removal
- Unauthorized attempts:
    - Failed attempts for access
    - Access policy violations and notifications for network gateways and firewalls
    - Alerts from proprietary intrusion detection systems
- System alerts or failures:
    - Console alerts or messages
    - System log exceptions
    - Network management alarms
- All access to cardholder data, including root/administration access

Monitoring results shall be retained in accordance with retention schedules for potential evidence.

Clock Synchronization
ESD will use a common method to ensure that all system clocks are synchronized. This will ensure the accuracy of the audit logs and protect the integrity and credibility of any logs that might need to be used as future evidence.

All computers with real-time clocks shall be set on ESD's local standard time (US/Pacific with DST), the employee's location's local standard time, or UTC.

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.