INFORMATION SECURITY - INCIDENT RESPONSE AND TECHNOLOGY DISPOSAL

CS
(REGULATION)

OVERVIEW	This Policy governs College of the Mainland's detection, response, documentation, and reporting of Incidents affecting Information Resources. Incidents include, but are not limited to, unauthorized access, theft, intrusion, misuse of data, other activities contrary to College of the Mainland's Acceptable Use Policy, denial of service, corruption of software, computer, and electronic communication based events.
PURPOSE	This Policy is established to protect the integrity, availability and confidentiality of information, prevent loss of service, and comply with legal requirements. This Policy establishes an Incident Response Team and the process for identifying and reporting an Incident, initial investigation, risk classification, documentation and communication of Incidents, responder procedures, Incident reporting, and training.
SCOPE	This Policy applies to all individuals who manage and are responsible for College of the Mainland's Information Resources.
POLICY	Under the direction and supervision of the Chief Information Officer (CIO) the Information Security Officer (ISO) shall ensure: • Procedures and processes identify and respond to suspected or known Incidents, mitigate them to the extent practicable, measure harmful effects of known Incidents, document Incidents and their outcomes, collect evidence, and provide appropriate reporting to the CIO. • Incident response procedures list examples of security Incidents and the appropriate responses for each. • An Incident Response Team has been assembled to receive notice of Incidents and manage the process of investigating, responding to, and reporting of the Incident. <u>Establishment of an Incident Response Team</u> The ISO is responsible for Incident detection and remediation of Information Resources. The ISO will

consult with the CIO and key representatives of College of the Mainland's IT, Human Resources, Legal or other departments as warranted to establish an Incident Response Team appropriate to respond to a specific Incident.

As necessary, the ISO and Incident Response Team shall assign Staff to manage specific security Incidents:

1. Initial Investigations. An Incident Response Plan (Plan) shall provide a quick and orderly response to Incidents. The Plan will identify steps to be followed for the initial reporting of events and subsequent investigations. Where appropriate, Staff will be on call to handle Incidents reported outside of standard business hours.
2. Risk Classification. The initial investigations will identify the Incident severity level and classify the risk to the organization according to the guidelines contained in the Risk Assessment Classification section of this Policy.
3. Documentation and Communications. The initial investigations staff will inform the ISO of the Incident and the preliminary risk classification. The ISO shall follow the guidelines identified in the Documentation and Communication of Incidents section of this Policy.
4. Responder Procedures. The ISO shall identify the appropriate procedures and Staff to address the specific Incident. Responders will attempt to identify as much information about the event so as to limit additional adverse effects. Responders and appropriate Staff will evaluate and recommend to the ISO appropriate actions to be taken.
5. Special Situations/Exceptions. The ISO shall identify and document procedures that address special situations and exceptions.

6. Incident Reporting. The ISO shall keep the CIO informed on the status of current Incidents. A post Incident report shall be created.
7. Training and Testing. The ISO shall ensure Staff have the proper training to fulfill their Incident response roles and responsibilities.

Identifying and Reporting Incidents

The Incident Response Team shall work with College of the Mainland departments to establish proactive monitoring systems that can identify potential Incidents. In addition, any College of the Mainland Staff may refer an activity or concern to the CIO.

Once an Incident has been reported, the Incident Response Team will log and track Incidents and, working with others as appropriate, take steps to investigate, escalate, remediate, refer to others, or otherwise address as outlined in the remainder of this Policy.

In addition to reporting Incidents, Staff shall report to the CIO any weaknesses or deficiencies in Information Resources.

Risk Assessment Classification

The ISO will establish an internal risk assessment classification to focus the response to each Incident, and to establish the appropriate team participants to respond. This classification matrix will correspond to an “escalation” of contacts and will indicate which personnel at College of the Mainland to involve and which procedure would be applicable for each class of Incident.

In general, Incidents are assigned to one of the following classifications:

- Unauthorized access – a person, process, or program is granted unauthorized physical or logical access to Information Resources. This classification includes a breach of sensitive data and should be reported to ISO as soon as the Incident is detected.

- Denial of service (DoS) – an attack that overloads an Information Resource to prevent it from performing its normal function. Distributed Denial of Service (DDos) attacks are large-scale attacks from multiple sources.
- Malicious software (malware) – infects an operating system or application and prevents the software from performing its intended operation. In addition, the malware may delete software and data, compromise the integrity of information, and disclose sensitive information to unauthorized personnel.
- Improper use – a person, process, or program that violates acceptable use policies. Examples include a disgruntled Staff member who ignores policies and procedures, a network administrator who circumvents log files, and a Staff member who extracts customer lists.
- Scans/probes/attempted access – a person, process, or program that attempts to identify vulnerabilities through the use of vulnerability scanning, network mapping, and penetration testing tools.
- Other – this classification includes other types of Incidents not described above. For example, unconfirmed Incidents, potentially malicious events, or other activity that warrants additional review.

<u>Documentation and Communication of Incidents</u>
The ISO will ensure that Incidents are appropriately logged and archived. Any Incidents involving sensitive information will be identified so the appropriate security procedures can be followed. Incident reporting will be provided by the ISO to College of the Mainland Chief Information Officer.

Wherever possible, documentation of such Incidents will cross-reference other event databases such as IT help desk ticket and network monitoring systems. Any Incidents involving systems that are tracked in

the inventory database will be cross-referenced in that database with the ISO Incident tracking log.

The ISO or Incident Response Team representatives are responsible for communicating the Incident to appropriate personnel and maintaining contact, for the purpose of update and instruction, for the duration of the Incident.

Responder Procedures

The ISO shall maintain standard responder procedures for the response and investigation of each Incident, as well as securing the custody of any evidence obtained in the investigation. The application of these procedures shall be governed by the classification described above as well as an Incident Response Plan. Staff shall refer to the Incident Response Plan for specific information on how to manage and respond to Incidents. The procedures will specify the location, method of custody for each Incident, and if custody of evidence is required.

Special Situations/Exceptions

Any personally owned devices, such as tablets, phones, wireless devices or other electronic transmitters which have been used to store sensitive information and are determined to contribute to an Incident, may be subject to seizure and retention by College of the Mainland Staff. By using personally owned devices within the College of the Mainland network for business purposes, Staff are subject to College of the Mainland policies restricting their use.

In the event a follow-up action concerning a person or organization after an information security Incident requires legal action proper forensic procedures including chain of custody shall be required for collection, retention, and presentation of evidence to support potential legal action subject to the relevant jurisdiction.

Cloud computing controls shall be put in place to ensure privacy and automated Tenant breach formal notification upon the compromise of a Tenant's system(s).

Incident Reporting

The ISO shall provide appropriate reporting to the CIO. Such reporting to include, but is not limited to, updates to inform the CIO of relevant details, risks, current status and progress, tasks to be completed, and expected outcomes and dates. Post Incident reporting shall include appropriate details, mitigation actions and timeframes, and lessons learned.

In addition to reporting of specific incidents, the ISO shall provide annual reporting to the CIO that summarizing incidents reported and actions taken. The annual report shall identify numbers and types of incidents, impact, costs incurred, lessons learned, and other relevant factors.

Training

The ISO is responsible for ensuring that Incident response team members and related Staff have the proper training and acknowledgement of their duties and responsibilities and appropriate Incident response policies, procedures, plans and related documents. No less than annually, awareness and refresher training shall be provided to maintain Incident response readiness and competency. The ISO may also arrange Incident response exercises to test and evaluate Staff, related procedures, and the ability to respond to Incidents in a timely and effective manner.

ENFORCEMENT

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

TECHNOLOGY DISPOSAL

College of the Mainland Staff store sensitive information on computer hard drives and other forms of electronic media. As new equipment is obtained and older equipment and media are phased out, sensitive information on the old equipment and media must be properly erased or otherwise made unreadable.

College of the Mainland faces several risks related to the disposal of hard drives and other computer storage media:

- Violation of Software License Agreements - Most software is licensed for use on either a single computer system, to a single person, or to an organization. Usually these licenses are not transferable. Even when the licenses are transferable, there may be specific requirements that must be met, such as possession of the original distribution media, consent of the licensor, or payment of a transfer fee, in order to effect the transfer. Allowing a third party access to licensed software without proper transfer of the license may be a breach of the license agreement, and may subject the state or the recipient of the software to claims for damages.
- Unauthorized Release of Confidential Information - Allowing an unauthorized person access to confidential information can subject College of the Mainland and sometimes individual employees, to claims for damages.
- Unauthorized Disclosure of Trade Secrets, Copyrights, and Other Intellectual Property – College of the Mainland computer systems develop and store data, programs, designs, techniques, etc., that are or will become valuable assets of the organization as either trade secrets, copyrighted materials, patented inventions, or other intellectual property. Accidental or premature disclosure could mean a loss of secrecy under trade secrets law or constitute a publication under federal copyright law, either of which might result in loss of the asset.

This regulation applies to all College of the Mainland Staff that have access to Information Resources.

The Director of End User Support shall ensure:

- Procedures address the final disposition of sensitive information, hardware, or electronic media.
- Procedures specify the process for making sensitive information unusable and inaccessible. Procedures specify the use of a technology (e.g. software, special hardware,etc.) to make sensitive information unusable, inaccessible, and not able to be reconstructed.
- Procedures specify the personnel authorized to dispose of sensitive information or equipment containing sensitive information. Such procedures may include shredding, incinerating, or pulp of hard copy materials so that sensitive information cannot be reconstructed.

The transfer or disposition of data processing equipment, such as computers and related media, shall be controlled. Data can be present on any type of storage device, whether fixed or removable, that contains data and maintains the data after power is removed from the device. Due to the advances in computer forensics, simply deleting the data and formatting the disk will not prevent someone from restoring the data. However, sanitization of the storage media removes the information from the media in such a way that data recovery using common techniques or analysis is prevented.

Any and all computer desktops, laptops, hard drives, and portable media must be given to the IT Department for proper disposal. Paper and hard copy records should be disposed of in a secure manner as authorized by the Director of End User Support. The Director of End User Support's analysis of secure disposal processes should include, but not be limited to, shredders and storage of records in a secure area for an authorized disposal/recycling service.

Overwriting is a software procedure that replaces the data previously stored on magnetic storage

media with a predefined set of meaningless data. At a minimum, overwriting should be performed using a character, its complement, then a random character. For confidential information, additional overwriting using different characters is recommended.

Degaussing (i.e., demagnetizing) is a procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process.

Unless IT Department Staff can absolutely verify that no personal or confidential information, intellectual property, or licensed software is stored on the hard drive/storage media, the hard drive/storage media shall be sanitized or be removed and physically destroyed.

Any Staff member found to have violated this regulation may be subject to disciplinary action, up to and including termination.