Division Of TECHNOLOGY & COMMUNICATION
California State University CHANNEL ISLANDS

Process Number:	BP-05-002	**Effective Date:**	01/25/2017
Approved By:	A. Michael Berman VP for Technology & Innovation		**Page 1 of 6**

Business Practice for Use of Monitoring Technologies

PURPOSE:

Document the responsibilities and expectations concerning data security, security monitoring, and data privacy.

BACKGROUND:

The University must take steps to protect the confidentiality, integrity, and availability of the information assets entrusted to it by students, faculty and staff. To this end, T&I operates cyber security systems on CSU Channel Islands' network to help mitigate and investigate any incidents that may occur. Intrusion detection/prevention systems (IDS/IPS), and firewalls, are examples of such systems designed to monitor network traffic and serve as a record of suspected intrusion events to support T&I incident investigations and quality assurance.

BUSINESS PRACTICE:

Accountability:

Information Security Officer

Applicability:

All users of CI's network system.

Definitions:

***IDS* – Intrusion Detection System**: An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms.

Business Practice for Use of Monitoring Technologies

IPS – **Intrusion Prevention System**: Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, report it and attempt to block or stop it
Firewall – a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules
NGFW – **Next Generation Firewall**: A Next-Generation Firewall (NGFW) is an integrated network platform that is a part of the third generation of firewall technology, combining a traditional firewall with other network device filtering functionalities, such as an application firewall using in-line deep packet inspection (DPI), and intrusion prevention system (IPS).
Computing and Communications -- These terms include voice, data, and video networks, switches, routers, and storage devices and any and all forms of computer-related equipment, tools, and intellectual property, including computer/communications systems, personal computers, and all forms of software, firmware, operating software, and application software which is owned by the University or is in the University's possession, custody, or control.
Electronic Communications -- This term refers to the use of computers and communications facilities in the communicating or posting of information or material by way of electronic mail, bulletin boards, or other such electronic tools.

Text:

General

Legal Basis

Use of the university's computing and communications facilities and resources is governed by all applicable CSU and CSU Channel Islands system and university policies and procedures, as well as by all applicable federal, state, and local laws and statutes. Users are subject to the California State University and CENIC Acceptable Use Policy. CENIC provides access to the network infrastructure that interconnects CSU campuses and other sites to information and communication resources worldwide.

Material accessible to the Channel Islands community through networks and material disseminated from Channel Islands shall not be restricted on the basis of its content (with the exception of content otherwise prohibited by law) nor because of the origin, background, or views of those contributing to its

creation. University administrators, faculty, and staff should challenge any attempts to censor electronic information resources.

Privacy and Ownership (Disclaimers)

Monitoring of the University network by T&I employees to ensure quality of service, and to protect information assets, is permitted under Federal and state law, and required by the Integrated California State University Administrative Manual (ICSUAM), Policy 8045.500.

The University supports each individual's right to private communication and will take reasonable steps to ensure security of network communications. However, messages on university computing resources are potentially accessible to others through normal system administration activities, in response to subpoenas or other court orders, and to the public through public records laws. Furthermore, while the University endeavors to protect the security of network communications, the possibility of unauthorized access always exists. Hence, the University cannot guarantee absolute privacy of electronic communication.

The University supports each individual's right to privacy of personal files. However, in the normal course of system administration, information technology staff may have to examine user files to gather information to diagnose and correct problems. Any information incidentally obtained in the process of system administration will be kept confidential, unless its release is required by law or campus policy. Additionally, with reasonable cause for suspicion and appropriate administrative authority, files may be examined by system personnel to determine if a user is acting in violation of the policies set forth in this document, other T&I business practices and university policies, or state or federal statutes.

The University will normally treat all e-mail messages, personal files, and personal data as private and confidential and will normally examine or disclose the contents only when authorized by the affected computer user(s). Requests for access to private messages/data for any other purpose than technical problem resolution must be approved jointly by the senior divisional officer or their designee and by the Vice President for Technology & Innovation, except as necessary to protect the integrity, security, and effective operation of the university's computing and communications facilities or as required by local, state, or federal law.

To protect the integrity, security, confidentiality, and effective operations of the university's computing and communications facilities and the users thereof against unauthorized or improper use of these

facilities, the University reserves the right, without notice, to limit or restrict any individual's use of any computing and communications facility or resource and to inspect, copy, remove, or otherwise alter any data, file, or system resource which may undermine security, integrity, confidentiality, or the effective operation of the university's computing and communications facilities. The University disclaims responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of computing and communications facilities.

Caution: Having open access to computing and communications facilities implies some risk. The University cherishes the diversity of values and perspectives endemic in an academic institution and is respectful of freedom of expression. Therefore, it does not condone censorship nor does it endorse the inspection of files other than on an exceptional basis. As a result, the University cannot protect individuals against the existence or receipt of material that may be offensive to them. Reasonable expectations of privacy are diminished once electronic communications are sent to other users or posted on public systems.

University-purchased, -owned, or -maintained software for individual workstations and site licenses, data, and custom applications programs are the exclusive property of the University and shall be used by faculty, staff, and registered students only in the conduct of university business or for incidental use as permitted under the California State University Appropriate Use Policy.

Use and Disposal of System Log Files (Metadata)

Some of the systems operated by Technology & Innovation capture and record information about University network traffic. This information, generally referred to as metadata, records the movement of network traffic and normally does not include any personal data. However, because of the potential of the use of metadata to track the activities of individual users, the following policies will apply:

1. Metadata will be available to technical staff on a strict “need to know” basis and will be kept confidential to the extent possible.
2. Metadata will not be disclosed without appropriate safeguards.
3. All log files containing metadata will be securely and fully deleted within 120 days of collection.

User Responsibilities

Business Practice for Use of Monitoring Technologies

Each faculty, staff, and student user of CSU Channel Islands' computer communications systems is responsible for the material that he or she chooses to send or display using the campus computing/communications resources. All personal data processed is considered sensitive and/or confidential. Anyone utilizing/accessing university computer systems, related data files, and information shares the responsibility for the security, integrity, and confidentiality of information.

Business Practice for Use of Monitoring Technologies

Assessment Requirements

Assessment requirements and history are listed in the grid below.

Description	Frequency	Role Assigned
General review of this business practice	Annually	Information Security Officer

Revision History

BP Nbr:	BP-05~~0~~-002~~0~~	**Enacted Date:**	01/25/2017		
Revision Nbr:	999	**Revision Date:**	99/99/9999	**Revised By:**	