California State University | Division Of TECHNOLOGY & INNOVATION | CHANNEL ISLANDS

| | | | |
|---|---|---|---|
| **Process Number:** | BP-05-006.01 | **Effective Date:** | 03/12/2013 |
| **Approved By:** | A. Michael Berman<br>VP for Technology & Innovation | | **Page 1 of 4** |

# Business Practice for Information Technology Security

# Mobile Device Access

## *PURPOSE:*

Provide support of ICSUAM Policy 8045.400 for mobile device data storage.

## *BACKGROUND:*

To support ICSUAM policy 8045.400, CI must develop and implement controls for securing protected data stored on mobile devices. Protected data must not be stored on mobile devices unless effective security controls have been implemented to protect the data. Campuses must use encryption, or equally effective measures, on all mobile devices that store level 1 data as defined in the CSU Data Classification Standard. Alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by a designated campus official. Other effective measures include physical protection that ensures only authorized access to protected data.

## *BUSINESS PRACTICE:*

### *Accountability:*

Vice President for Technology & Innovation
Information Security Officer

### Applicability:

Anyone with access to Channel Islands computer systems

### Definitions:

1. **Protected Data** – Data classification as prescribed in recognized campus data classification standard.
2. **ISO** – Information Security Officer
3. **ICSUAM** – Integrated CSU Administrative Manual

# Business Practice for Information Technology Security

# Mobile Device Access

## Text:

### *General*

Having adequate levels of controls in place to protect data stored on mobile devices is paramount to the security of CI's information assets. To validate that appropriate levels of access are in place, and in support of the CSU's ICSUAM policy 8045.400 for mobile devices, Channel Islands maintains standards for requesting the use of mobile storage devices. Mobile storage devices include but are not limited to unattached storage drives of any size or format, thumb drives, SD cards, CD's, DVD's, or any other storage device/media that is not a part of the design and manufacture of a University assigned computer.

**Acceptable Use for Mobile Device Storage**

Storage of University data on mobile devices may be acceptable only if all of the following conditions have been met:

1. There is a documented business need for the data to be stored outside of University systems.
2. The devices identified for storage of University data utilize strong encryption.
3. Approval has been given in writing by the ISO and a Divisional Vice President to store University data on a mobile device.

**Requesting Approval for Mobile Data Storage**

The following outlines the steps needed to request approval for mobile data storage:

Email the following information to the Information Security Officer (infosec@csuci.edu):

1. Requester Name
2. Requester Employee ID
3. Requester Division
4. Requester Department
5. Requester Immediate Manager
6. Business Reason for Requiring Mobile Storage
7. Description of Data to be stored on this Device

Once received, the ISO will review the request, and contact the Division Vice President for their approval and discuss purchasing options for approved storage devices.

# Business Practice for Information Technology Security

## Mobile Device Access

**Assessment of Mobile Device Storage**
Regular assessments shall occur to review current mobile storage of University data, and to determine if that data storage is still applicable. If applicable, approval renewal shall occur at assessment time.

Information gathered at assessment will include the following:

1. Name of the party storing University data
2. Device(s) identification data is being stored on
3. Date of assessment
4. Name and department of the resource performing the assessment
5. Description of the data being stored

Assessment results will be kept on record in the office of the Vice President for Technology & Innovation for a period of five years.

**Compliance**
The University reserves the right to temporarily or permanently suspend, block, or restrict access to information assets when it reasonably appears necessary to do so to protect the confidentiality, integrity, availability, or functionality of those assets.

Any disciplinary action resulting from violations of this business practice or program supporting policies, standards or procedures shall be administered in a manner consistent with the terms of the applicable collective bargaining agreement and/or the applicable provisions of the California Education Code. Student infractions of this business practice or supporting policies, standards or procedures may be referred to the Office of Student Judicial Affairs. Third party service providers who do not comply with established information security policies, business practices, standards or procedures may be subject to appropriate actions as defined in contractual agreements.

# Business Practice for Information Technology Security

# Mobile Device Access

## *Assessment Requirements*

Assessment requirements and history are listed in the grid below.

| Description | Frequency | Role Assigned |
|---|---|---|
| Review business practice | Annual | ISO |
| Review list of acceptable storage devices | Annual | Mgr, User Services<br>ISO |
| Assessment of approved mobile data storage users | Bi-annual | ISO |

## *Revision History*

| | | | | | |
|---|---|---|---|---|---|
| **BP Nbr:** | BP-05-006 | **Enacted Date:** | 03/12/2013 | | |
| **Revision Nbr:** | 001 | **Revision Date:** | 02/02/2017 | **Revised By:** | NFisch |