

## **PM 2021-05 [Supersedes PM 2016-01]**

Thomas A. Parham, Ph.D.

10/29/2021

# **INFORMATION SECURITY AND PRIVACY POLICY**

## **1.0. POLICY**

Consistent with published [CSU Information Security Policies and Standards](#), this policy outlines the roles and responsibilities of the University in information security and privacy. This policy is further supported by related IT standards and guidelines that facilitate University compliance with the recommendations, audit requirements, actions, and safeguards necessary to mitigate risks, protect information assets, and user data.

## **2.0. PURPOSE**

California State University, Dominguez Hills (CSUDH) establishes this Information Security and Privacy Program in compliance with the CSU Information Security Policy, "Establishing an Information Security and Privacy Program." CSUDH recognizes the importance of protecting University technology resources and user data.

This Information Security and Privacy Policy defines and communicates appropriate and reasonable administrative, technical, and physical safeguards by:

- Documenting roles and responsibilities for the information security and privacy program.
- Securing the confidentiality, integrity, and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g., paper or electronic).
- Complying with all applicable federal and state laws and regulations, CSU Information Security Policy, and applicable CSUDH policies, procedures, standards, and guidelines.

The CSUDH Information Security and Privacy Policy and supporting IT standards and guidelines are not intended to prevent, prohibit or inhibit the permitted use of information assets required to meet University academic and administrative goals.

## **3.0. SCOPE**

All constituents within the University share responsibility for protecting information resources, information assets, and user data. A collaborative and unified approach provides the most robust defense against system unavailability, service interruptions, identity theft, and fraud, among other concerns.

The CSUDH Information Security and Privacy Policy applies to the following:

- A. Centrally managed and department-managed systems and information assets and user data.
- B. All users employed by CSUDH, university auxiliary organizations, third-party service providers, and any other person, accessing the CSUDH network resources, information assets, and/or user data. This includes non-University-owned and non-University-housed computing, storage, cloud storage, or mobile devices that may store University data.
- C. CSUDH information assets and data, including but not limited to student and employee data and byproduct, in which the information asset is held or transmitted (e.g., physical or electronic).
- D. Information technology facilities, hardware systems, network resources, and applications are owned by CSUDH. This includes third-party service providers' systems that access or store CSUDH protected data, transmit protected data over communication lines, or process credit card payments.

#### **4.0. GENERAL PROGRAM INFORMATION**

##### **4.1. INFORMATION SECURITY MANAGEMENT TEAM**

The President has designated responsibility for the University information security program to the following individuals:

##### **Information Security Officer (ISO) – AVP, Security & Compliance**

Coordinates and oversees University compliance with the Information Security and Privacy Policy; develops and administers all information security and privacy standards and guidelines; directs and supports the information security risk management process; performs independent information security and privacy audits; manages security awareness; conducts computer forensic evaluations; leads the CSUDH-CSIRT team and serves as the University representative on the CSU Information Security Advisory Committee (ISAC). Provides oversight in investigations involving employees and students suspected of violating the CSUDH Information Security and Privacy Policy or federal and state laws and regulations.

##### **Vice President for Information Technology/CIO**

The Chief Information Officer (CIO) is the senior campus information technology executive and represents the campus on all information technology issues and overall coordination for all aspects of campus information technology resources.

## **Information Practices– University Counsel**

Provides guidance regarding all legal matters involving information assets and privacy regulations; acts as the University's designated agent with the U.S. Copyright Office to receive and act upon copyright infringement notifications.

### **Vice Presidents**

In consultation with the ISO and the University Counsel, oversee risk assessment, mitigation, and acceptance for their respective division; ensure compliance with state and federal statutes and regulations in accordance with published IT standards and user guidelines; ensure compliance with information security and privacy policy pertaining to their respective divisions; maintain a disaster recovery plan for decentralized systems within their division, and maintain a divisional technology and data related business continuity plan.

### **President**

Oversee all efforts regarding information security and privacy policy and designated responsibility for the University Information Security and Privacy Program.

#### **4.2. GOVERNANCE**

Oversight for Information Technology is provided by the Vice President/CIO. The ISO chairs the Technology Risk, Privacy, Security, and Compliance Governance committee.

#### **4.3. REVIEW OF THE INFORMATION SECURITY AND PRIVACY POLICY**

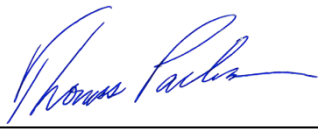
The information security and privacy policy is reviewed at least annually by the information security officer (ISO) and the University Counsel and may be updated as required. The policy may be evaluated and adjusted at any time in light of relevant circumstances, including changes in the University's business arrangements or operations, federal or state regulatory changes.

#### **4.4. ACCESS TO THE PLAN**

Information Technology (I.T.) is responsible for the online publication of the Information Security and Privacy Policy for California State University, Dominguez Hills. The printed document is maintained by the AVP of IT Security & Compliance/ISO.

#### **5.0. REFERENCE**

- CSU Data Classification Policy
- CSU Information Security Policy
- CSU Access Control Policy
- CSU Retention Policy

Approved:   
 \_\_\_\_\_  
 Thomas A. Parham, Ph.D.  
 President

Date: 10/29/2021

<b>Policy Category</b>	Information Technology
<b>Policy Owner</b>	Sara Hariri
<b>Policy Approver(s)</b>	Dr. Thomas Parham
<b>Related Policies</b>	CSU Information Security Policy
<b>Related Procedures</b>	
<b>Effective Date</b>	October 18, 2021
<b>Next Review Date</b>	Annual

### Revision History

Version	Revision Date	Revised By	Summary of Revisions	Date of Change
1.0	Jan 20, 2021	Sara Hariri	Privacy Policy added, new structure added.	Jan 21 <sup>st</sup> 2021
1.1	Feb 20, 2021	Faculty and Students Comm Working Group	Update on procedures	March 25 <sup>th</sup> , 2021
1.2	April 20, 2021	Faculty and Students Comm Working Group	Update on content	May 10 <sup>th</sup> , 2021
2.0	June 7 <sup>th</sup> , 2021	John Walsh	Final Draft	June 7 <sup>th</sup> , 2021

### Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
June 7 <sup>th</sup> 2021	Sara Hariri	Approved