# California Health Sciences University

UNIVERSITY

INFORMATION TECHNOLOGY (IT) POLICY

**PURPOSE**

This policy establishes the governance structures, decision making processes, and accountability mechanisms that guide the management of information technology at the University. It is structured so that all technology investments, operations, and services support the University's mission in teaching, research, and administration.

**SCOPE**

This policy applies to:

- All IT units and personnel
- All academic, administrative, and research departments using IT resources
- All technology related decisions, systems, data, and services
- All employees, students, contractors, consultants, and affiliates with access to University systems

**POLICY STATEMENT**

The University is committed to the secure, efficient, and strategic use of information technology. All IT activities must align with institutional goals, comply with legal and regulatory requirements, and support high quality academic and administrative operations.

**DEFINITIONS**

A. **IT Resources:** All University owned or managed hardware, software, networks, data, and digital services.
B. **Data Owner:** The department or unit responsible for the accuracy, use, and stewardship of specific data sets.

C. **Confidential/Restricted Data**: Information requiring protection due to legal, regulatory, or institutional requirements.
D. **Incident:** Any event that compromises the confidentiality, integrity, or availability of IT systems or data.
E. **End Users:** Any individual granted access to University IT resources.

## RELATED INFORMATION AND PROCEDURES

A. **Governance Structure**

- **Vice President (VP) of Operations**
  The VP Operations provides executive leadership and is accountable for institutional IT strategy, policy, and performance.
- **President's Executive Council**
- **IT Committee (ITC)**

**Purpose:** Provide strategic oversight, security governance, and risk management.

**Responsibilities:**

- Approve IT strategy and major technology investments
- Prioritize enterprise-level projects
- Review IT performance, risk, and compliance reports
- Approve security policies
- Review risk assessments and incident reports
- Ensure regulatory compliance

B. **AI committee**

**Purpose:** Provide strategic oversight and guidance for the responsible, ethical, and effective adoption of artificial intelligence technologies in support of the University's academic, administrative, research, and operational goals.

**Responsibilities:**

- Develop and recommend institutional policies, standards, and guidelines related to the use of AI technologies.
- Evaluate and recommend AI tools and platforms that support teaching, learning, research, student services, and operational efficiency.
- Promote the ethical, secure, and compliant use of AI, including considerations related to privacy, bias, protection of intellectual property, and compliance with regulatory requirements.
- Identify opportunities for innovation and continuous improvement through the use of AI across the University.
- Support faculty and staff development by providing guidance, resources, and training on emerging AI technologies and best practices.
- Review and assess potential risks associated with AI adoption and recommend appropriate governance and mitigation strategies.
- Foster cross-functional collaboration among academic, administrative, and technology stakeholders to ensure alignment with institutional priorities.
- Monitor developments in AI and advise University leadership on emerging trends, opportunities, and challenges.

C. **IT Management**

The Director of IT and IT managers are responsible for implementing governance decisions, managing IT operations, and ensuring compliance with this policy. The IT managers generally report to the Director of IT, but if the Director of IT is not available, the IT managers report to the VP of Operations

D. **Roles & Responsibilities**

- Set institutional IT priorities
- Approve major policies and investments

**Executive Leadership**

- Set institutional IT priorities
- Approve major policies and investments

**IT Department**

- Implement security controls
- Maintain systems and infrastructure
- Provide support services
- Conduct risk assessments

**Departments & Data Owners**

- Safeguard data they own
- Ensure appropriate access and use to the data they own
- Participate in IT policy reviews
- Comply with IT Policy and guidance from IT Department

**End Users (CHSU employees and Students)**

- Follow all IT policies and procedures
- Protect credentials and sensitive data
- Report incidents promptly

E. **Policy Requirements**

**Acceptable Use**

End Users must follow CHSU IT Acceptable use policies. Employees are required to follow the acceptable use policy for employees, whereas Students must follow the acceptable use policy applicable to students. (CHSU Acceptable Use of Technology Policy for Employees, CHSU Acceptable Use of Technology Policy for Students). Misuse may result in disciplinary action up to and including termination or dismissal.

**Information Security**

The University requires:

- Multi-factor authentication
- Encryption of sensitive data
- Network segmentation
- Regular patching and vulnerability scanning
- Immediate reporting of security incidents

**Data Governance**

All CHSU employees must follow the CHSU Data Governance Policy

**Technology Procurement**

- Prior to purchase, all IT equipment and software must be reviewed by the IT department for security, compatibility, and licensing.
- Cloud services require security and privacy assessments.
- Vendors handling sensitive data must sign data protection agreements.

**IT Service Management**

The IT Service Catalog includes network services, email, classroom technology, help desk support, application hosting, and research computing. Service Level Agreements (SLAs) define response times, resolution times, availability targets, and support hours.

**Change Management**

All changes to production systems are required to have:

- Impact assessment
- Testing
- Approval
- Communication to individuals affected by change
- Documentation

**Business Continuity & Disaster Recovery**

- Critical systems must be identified and prioritized.
- Backup schedules, RTOs, and RPOs must be defined.
- Disaster recovery plans must be tested annually.

F. **Compliance**

All users must comply with this policy and related regulations. Violations may result in disciplinary action, loss of access, or legal consequences. The University may conduct audits to ensure compliance.

G. **Monitoring & Review**

- IT performance will be monitored using KPIs such as uptime, incident response times, project delivery metrics, and security compliance rates.
- This policy will be reviewed annually by VP Operations and IT Committee (ITC).

H. **Related Documents**

- Acceptable Use Employee and Student Policies
- Data Governance Policy
- Generative AI Use in the Workplace
- Incident Response Plan
- Business Continuity & Disaster Recovery Plan

---

**RESPONSIBILITIES**

A. Director of Information Technology (IT)

**HISTORY (R*)**

Approval Date:

08/12/2026

Revision Date(s):

07/22/2026

Reviewed Date(s):

07/22/2026

**RACI –**

**R**: Director of Information Technology

**A**: Director of Information Technology, Vice President of Operations

**C**: Vice President of Operations, Legal Affairs

**I**: CHSU Community