# Comprehensive Information Security Plan

This Information Security Plan will be reviewed annually and updated as needed to address operational, technological, and regulatory changes.

## 1. Purpose

The Angeles College (AC) is committed to protecting the confidentiality, integrity, and availability of sensitive and nonpublic information. This **Information Security Plan (ISP)** establishes the safeguards necessary to prevent unauthorized access, disclosure, misuse, or destruction of institutional data.

This plan applies to all AC employees, contractors, vendors, systems, and third-party service providers that access, process, store, or transmit sensitive information.

The **ISP** supports:

- Risk identification and management
- Security controls and monitoring
- Incident response procedures
- Security awareness and training
- Third-party risk management

---

## 2. Scope

This ISP applies to all sensitive and nonpublic information handled by AC, including:

- Financial and student aid records
- Personally Identifiable Information (PII)
- Protected health information covered under HIPAA
- Academic and employee records
- Proprietary or institutional data

---

## 3. Roles and Responsibilities

### 3.1 Information Security Officer (ISO)

The ISO oversees the implementation and enforcement of this ISP, including risk assessments, compliance monitoring, and incident response coordination.

### 3.2 GLBA Compliance Coordinator

The GLBA Compliance Coordinator ensures compliance with the Gramm-Leach-Bliley Act and works with the ISO to safeguard financial information.

### 3.3 Information Technology Department

The IT Department manages technical safeguards such as network security, system monitoring, access control, and software updates.

### 3.4 Data Stewards

Departments handling sensitive information must designate Data Stewards responsible for ensuring data is managed in accordance with AC policies.

---

## 4. Risk Assessment and Management

AC will conduct periodic risk assessments to identify and address threats to sensitive information.

### 4.1 Risk Identification

Risks may include:

- Unauthorized access to systems or data
- Cyberattacks, malware, or phishing
- Insider misuse or human error
- Equipment failure or theft
- Natural disasters or environmental events

### 4.2 Risk Mitigation

AC will implement appropriate administrative, technical, and physical safeguards to reduce identified risks.

---

## 5. Administrative Safeguards

### 5.1 Policies and Procedures

AC will maintain and regularly review information security policies governing the use, storage, transmission, and disposal of sensitive information.

### 5.2 Security Awareness Training

Employees, contractors, and authorized third parties must complete security awareness training appropriate to their job responsibilities. Training must include, at a minimum, the following topics:

- Phishing and social engineering
- Secure data handling and disposal
- Password management and MFA
- Incident reporting procedures

### 5.3 Access Control

Access to sensitive information will be limited to authorized individuals based on business need and the principle of least privilege.

---

## 6. Technical Safeguards

### 6.1 Encryption

Sensitive data transmitted electronically must be encrypted using industry-standard methods. Encryption at rest will be implemented where feasible.

### 6.2 Network Security

AC will maintain network protections including:

- Firewalls
- Intrusion detection and prevention systems (IDS/IPS)
- VPN and MFA for remote access

### 6.3 Endpoint Protection

Institution-owned devices must use approved antivirus and endpoint protection software with current updates applied.

### 6.4 Backup and Recovery

Critical systems and data will be backed up regularly and tested periodically to ensure recovery capabilities.

### 6.5 Patch Management

Systems and software will be updated regularly to address security vulnerabilities.

---

## 7. Physical Safeguards

### 7.1 Facility Security

Access to sensitive areas such as server rooms and records storage locations will be restricted using locks, access badges, or surveillance systems.

### 7.2 Paper Records

Sensitive paper documents must be securely stored and shredded before disposal.

### 7.3 Device Security

Institutional devices must be protected against theft and unauthorized access through password protection and physical security measures.

---

## 8. Incident Response

AC maintains an Incident Response Plan (IRP) to address and contain security incidents.

### 8.1 Incident Reporting

Employees and contractors must promptly report suspected security incidents or data breaches to the Information Security Officer.

### 8.2 Response and Containment

The ISO and IT Department will investigate incidents and take appropriate containment actions.

### 8.3 Notification Requirements

AC will provide required notifications following a confirmed data breach in accordance with applicable laws.

### 8.4 Post-Incident Review

After an incident, AC will review the cause and implement corrective actions to prevent recurrence.

---

# 9. Monitoring and Improvement

## 9.1 Security Monitoring

AC will monitor systems and networks for suspicious activity and vulnerabilities.

## 9.2 Testing and Assessments

Periodic vulnerability assessments and penetration testing will be conducted to evaluate security controls.

## 9.3 Plan Review

This ISP will be reviewed annually and updated as necessary to address evolving threats and regulatory changes.

---

# 10. Third-Party Risk Management

## 10.1 Vendor Due Diligence

AC will assess the security practices of vendors that access or process sensitive information.

## 10.2 Contract Requirements

Vendor agreements will include information security and confidentiality requirements consistent with AC standards and applicable laws.

## 10.3 Ongoing Oversight

AC may periodically review vendor security practices and require remediation of identified issues.

---

# 11. Compliance

AC will comply with all applicable federal, state, and local laws and regulations, including:

- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Family Educational Rights and Privacy Act (FERPA)
- Applicable state data breach notification laws

---