Stanford | University IT

Information Security

Minimum Security Standards

Stanford is committed to protecting the privacy of its students, alumni, faculty, and staff, as well as protecting the confidentiality, integrity, and availability of information important to the university's mission.

Endpoints

Servers

Applications

SaaS/PaaS

IaaS

IoT

Research

Definitions

Cookbooks

FAQ

Inquiries

These standards are intended to reflect the minimum level of care necessary for Stanford's sensitive data. They do not relieve Stanford or its employees, partners, consultants, or vendors of further obligations that may be imposed by law, regulation, or contract. University schools, departments, or organizations may impose more restrictive requirements.

Stanford expects all partners, consultants, and vendors to abide by Stanford's information security policies. If non-public information is to be accessed or shared with these third parties, they should be bound by contract to abide by Stanford's information security policies.

You are encouraged to begin adopting these standards, prioritizing your systems by risk level. As cybersecurity is a rapidly evolving field that continuously presents us with new challenges, these standards will be revised and updated accordingly.

> **Special note to Stanford researchers:** See Research Policy Handbook Section 1.10 for information security practices and guidelines specific to research computing systems.

Minimum Security Standards: Endpoints

An endpoint is defined as any laptop, desktop, or mobile device.

1. Determine the risk level by reviewing the data, server, and application risk classification examples and selecting the highest applicable risk designation across all. For example, an endpoint storing Low Risk Data but utilized to access a High Risk application is designated as High Risk.
2. Follow the minimum security standards in the table below to safeguard your endpoints.

Standard	Recurring Task	What to do	Low Risk	Moderate Risk	High Risk
Patching	↻	Apply security patches within seven days of publish. BigFix is recommended. Use a supported OS version.	✓	✓	✓
Whole Disk Encryption		Enable FileVault2 for Mac, BitLocker for Windows. SDR is recommended. Install MDM on mobile devices.	✓	✓	✓
Malware Protection		Install antivirus (Recommended: CrowdStrike or Microsoft Defender for Windows, Crowdstrike for Mac).	✓	✓	✓
Backups		Back up user data at least daily. University IT CrashPlan is recommended (option to set personal password). Encrypt backup data in transit and at rest.	✓	✓	✓
Inventory	↻	Review and update NetDB records quarterly. Maximum of one node per NetDB record.	✓	✓	✓
Configuration Management		Install BigFix , Jamf and SDR.			✓
Regulated Data Security Controls		Implement PCI DSS, HIPAA, or export controls as applicable.			✓

Minimum Security Standards: Servers

A server is defined as a host that provides a network accessible service.

1. Determine the risk level by reviewing the data, server, and application risk classification examples and selecting the highest applicable risk designation across all. For example, a server running a Low Risk application but storing High Risk Data is designated as High Risk.
2. Follow the minimum security standards in the table below to safeguard your servers.

Standard	Recurring Task	What to do	Low Risk	Moderate Risk	High Risk
Patching	🔄	Based on National Vulnerability Database (NVD) ratings, apply high severity security patches within seven days of publish and all other security patches within 90 days. Use a supported OS version.	✓	✓	✓
Vulnerability Management	🔄	Perform a monthly Qualys scan. Remediate severity 4 and 5 vulnerabilities within seven days of discovery and severity 3 vulnerabilities within 90 days.	✓	✓	✓
Inventory	🔄	Review and update NetDB, SUSI, and department/MinSec inventory records quarterly. Maximum of one node per NetDB record.	✓	✓	✓
Firewall		Enable host-based firewall in default deny mode and permit the minimum necessary services.	✓	✓	✓
Credentials and Access Control	🔄	Review existing accounts and privileges quarterly. Enforce password complexity. Logins with SUNet credentials via Kerberos recommended.	✓	✓	✓
Two-Step Authentication		Require Duo two-step authentication for all user and administrator logins.		✓	✓
Centralized Logging		Forward logs to a remote log server. University IT Splunk service recommended.		✓	✓
Sysadmin Training	🔄	Attend at least one Stanford Information Security Academy training course annually.		✓	✓
Malware Protection	🔄	Deploy Crowdstrike. Review alerts as they are received.		✓	✓
Intrusion Detection	🔄	Deploy OSSEC or Tripwire. Review alerts as they are received.		✓	✓
Physical Protection		Place system hardware in a data center.		✓	✓

Standard	Recurring Task	What to do	Low Risk	Moderate Risk	High Risk
Secure Admin Workstation		Access administrative accounts only through a Privileged Access Workstation (PAW) or Cardinal Protect workstation. A PAW is required for ring0 access.			✓
Security, Privacy, and Legal Review		Follow the Data Risk Assessment process and implement recommendations prior to deployment.			✓
Regulated Data Security Controls		Implement PCI DSS, HIPAA, or export controls as applicable.			✓

Minimum Security Standards: Applications

An application is defined as software running on a server that is remotely accessible, including mobile applications.

1. Determine the risk level by reviewing the data, server, and application risk classification examples and selecting the highest applicable risk designation across all. For example, an application providing access to Low Risk Data but running on a High Risk server is designated as High Risk.
2. Follow the minimum security standards in the table below to safeguard your applications.

Standard	Recurring Task	What to do	Low Risk	Moderate Risk	High Risk
Patching	↻	Based on National Vulnerability Database (NVD) ratings, apply high severity security patches within seven days of publish and all other security patches within 90 days. Use a supported version of the application.	✓	✓	✓
Vulnerability Management	↻	Perform a monthly Qualys application scan. Remediate severity 4 and 5 vulnerabilities within seven days of discovery and severity 3 vulnerabilities within 90 days.	✓	✓	✓
Inventory	↻	Review and update department/MinSec Application inventory records quarterly. Must indicate associated risk classification and data volume estimates.	✓	✓	✓

Standard	Recurring Task	What to do	Low Risk	Moderate Risk	High Risk
Firewall		Permit the minimum necessary services through the network firewall.	✓	✓	✓
Credentials and Access Control	🔄	Review existing accounts and privileges quarterly. Enforce password complexity. Logins with SUNet credentials via WebAuth/SAML recommended.	✓	✓	✓
Two-Step Authentication		Require Duo two-step authentication for all user and administrator logins.		✓	✓
Centralized Logging		Forward logs to a remote log server. University IT Splunk service recommended.		✓	✓
Secure Software Development		Include security as a design requirement. Review all code and correct identified security flaws prior to deployment. Use of static code analysis tools recommended.		✓	✓
Developer Training	🔄	Attend at least one Stanford Information Security Academy training course annually.		✓	✓
Backups		Back up application data at least weekly. Encrypt backup data in transit and at rest.		✓	✓
Secure Admin Workstation		Access administrative accounts only via a Privileged Access Workstation (PAW) or Cardinal Protect workstation. A PAW is required for ring0 access.			✓
Security, Privacy, and Legal Review		Follow the Data Risk Assessment process and implement recommendations prior to deployment.			✓
Regulated Data Security Controls		Implement PCI DSS, HIPAA, FISMA, or export controls as applicable.			✓

Definitions

Computing Equipment

Any Stanford or non-Stanford desktop or portable device or system

Masked number

(i) A credit card primary account number (PAN) has no more than the first six and the last four digits intact, and (ii) all other Prohibited or Restricted numbers have only the last four intact. See the entire PCI DSS 4.0 Standard (if you are willing to agree to some terms).

Minimum Privacy Standards (MinPriv)

The Minimum Privacy Standards are intended to reflect best practices for the collection, processing, transfer, deletion and other use of personal data at Stanford.

NIST-Approved Encryption

The National Institute of Standards and Technology (NIST) develops and promotes cryptographic standards that enable U.S. Government agencies and others to select cryptographic security functionality for protecting their data. Encryption which meets NIST-approved standards is suitable for use to protect Stanford's data if the encryption keys are properly managed. In particular, secret cryptographic keys must not be stored or transmitted along with the data they protect. Cryptographic keys have the same data classification as the most sensitive data they protect.

Payment Card Industry Data Security Standards

The practices used by the credit card industry to protect cardholder data. The Payment Card Industry Data Security Standards (PCI DSS) comprise an effective and appropriate security program for systems that process, store, or have access to Stanford's Prohibited or Restricted data. The most recent version of the PCI DSS is available here.

Protected Health Information (PHI)

All individually identifiable information that relates to the health or health care of an individual and is protected under federal or state law. For questions about whether information is considered to be PHI, contact the University Privacy Office.

Qualified Machine

A computing device located in a secure Stanford facility and with access control protections that meet the Payment Card Industry Data Security Standards.

Student Records

Information required to be maintained as non-public by the Family Educational Rights and Privacy Act (FERPA). Student Records include Stanford-held student transcripts (official and unofficial), and Stanford-held records related to (i) academic advising, (ii) health/disability, (iii) academic probation and/or suspension, (iv) conduct (including disciplinary actions), and (v) directory information maintained by the Office of the Registrar and requested to be kept confidential by the student. Applications for student admission are not considered to be Student Records unless and until the student attends Stanford.

Who do I contact for questions?

General Questions

Unit / Website	Help
Privacy Office	Submit help request
Information Security Office	Submit help request

Suspected Information Security Incident

Unit / Website	Help
Information Security Office	Submit help ticket

Report Lost or Stolen Device

Unit / Website	Help
Privacy Office	Submit report

Back to top