

System and Communications Protection Policy

Purpose

Network boundaries, segmentation, and cryptography are the technical backbone that keeps Your Organization's systems and data protected in transit and at rest. This policy defines the requirements Your Organization applies to boundary protection, network architecture, and encryption across its information systems.

Scope

This policy applies to all Your Organization networks, network devices, cloud environments, and application boundaries that carry or store company or customer data, and to the Engineering and IT Operations teams that design and operate them.

Boundary protection

- Your Organization maintains defined network boundaries between trusted internal networks, less-trusted zones (e.g., guest networks, DMZs), and the public internet, enforced by firewalls or equivalent boundary controls.
- Network traffic is denied by default and permitted only by documented exception ("deny-all, allow-by-exception"), with firewall rule sets reviewed at least annually to remove stale or overly broad rules.
- Publicly accessible systems (customer-facing applications, public APIs) are architecturally separated from internal-only systems, typically via a DMZ or equivalent segmentation pattern.

Network segmentation

- Production, staging/test, and corporate IT networks are segmented from one another so that a compromise in one does not automatically grant access to another.
- Systems processing higher-sensitivity data (per the Data Classification Policy) are placed in more restrictive network segments with tighter access controls than general-purpose systems.
- Administrative and management interfaces for network and infrastructure devices are not exposed to the public internet and are reachable only from approved management networks or via a bastion/jump host with MFA.

Encryption in transit

- All transmission of Confidential or Restricted data over untrusted networks, including the public internet, must use current, Your Organization-approved encryption protocols (e.g., TLS 1.2 or higher).
- Deprecated protocols and weak cipher suites are disabled on Your Organization-managed systems.
- Remote access to Your Organization networks uses encrypted VPN or equivalent zero-trust access with MFA, per the Access Control Policy.

Encryption at rest

- Confidential and Restricted data at rest — in databases, object storage, backups, and on endpoints — is encrypted using Your Organization-approved algorithms and key lengths.
- Encryption keys are managed through an approved key management solution, with defined ownership, rotation schedule, and restricted access to key material.

Cryptographic key management

Cryptographic keys are generated, distributed, stored, rotated, and destroyed following a documented key lifecycle. Private keys and secrets are never stored in source code repositories; they are held in an approved secrets management or KMS solution.

Session and application-level protections

- Sessions to sensitive systems are authenticated, encrypted, and time out after a defined period of inactivity.
- Mobile code (browser scripts, executable content from untrusted sources) and collaborative computing tools (video, screen-share, chat) are configured according to Your Organization-approved baselines to prevent unauthorized data exposure.
- Voice-over-IP and other real-time communications carrying sensitive discussions use encrypted transport where technically supported.

Architecture and design review

Material changes to network architecture or the introduction of new externally facing services undergo a security architecture review before deployment, assessing boundary placement, segmentation, and encryption requirements.

Roles and responsibilities

- **Engineering.** Designs application-level boundary and encryption controls into the systems it builds.
- **IT and Network Operations.** Owns network architecture, firewall rule management, and boundary device configuration.
- **Information Security.** Reviews architecture changes, sets cryptographic standards, and audits boundary configurations.

Review cadence

This policy is reviewed annually by Information Security and IT Operations, or sooner following a significant architecture change or a cryptographic standard deprecation (e.g., a TLS version or cipher suite reaching end of support).

Effective date: [the date this policy takes effect]