



Information Technology and Information Security Policy

Symmetric Program Management LLC

SPM 05 | Version 1.0 | Prepared October 11 2026

Policy owner Dr. Thomas Jackson Founder and Chief Executive Officer

Approval signature: *Thomas Jackson* Effective date: October 11, 2026

Purpose and scope

SPM will protect the confidentiality, integrity, and availability of company and client information on company devices, approved cloud services, removable media, and authorized contractor systems. This policy applies to all users and vendors with access. It establishes required practices; implementation must be evidenced separately.

Ownership and data classification

The CEO owns security risk and approves systems, access, and exceptions. A designated IT administrator implements controls and retains evidence. Project managers identify contract restrictions before receiving data. Classify information as public, internal, confidential, or contract-restricted. Personal information, health information, federal contract information, controlled unclassified information, and classified information require their applicable additional controls.

Restricted information gate

Do not receive or process controlled unclassified information or classified information in routine company systems. Before such work, verify authorization, required environment, personnel access, contractual controls, and assessment evidence. Personal clearance does not authorize company systems to store classified material. For health information, establish authorized purposes, applicable agreements, and privacy safeguards before access.

Access and authentication

Use individual accounts, minimum necessary permissions, and multifactor authentication for email, cloud storage, administrative access, and remote access where supported. Use a password manager and unique long passwords; never share credentials. Separate routine and administrative accounts. Approve new access in writing, review it quarterly, and revoke access immediately on termination or compromise.

Device and network controls

Maintain an inventory of authorized devices and software. Require supported systems, automatic screen lock, full-disk encryption, endpoint protection, and security updates. Prioritize actively exploited vulnerabilities immediately; use internal targets of 7 days for critical and 30 days for high-risk fixes, or document compensating controls and approval. Protect network boundaries, separate public from internal services, and prohibit unauthorized remote tools.

Secure handling and acceptable use

Store work in approved repositories. Limit sharing to verified recipients and review permissions before sending links. Do not put client information in personal email, unapproved cloud accounts, or public tools. Verify unusual payment or credential requests through a known separate channel. Report suspicious messages without opening unknown attachments. Control USB use, external integrations, and public postings through documented approval.

Physical security and disposal

Restrict device and paper access, escort visitors as appropriate, and lock devices during travel. Use approved secure connections for remote work. Sanitize media before reuse or disposal and retain evidence; shred confidential paper. Report lost equipment immediately and enable remote lock or wipe where supported and authorized.

Backup and monitoring

Back up critical records daily to a protected location separate from the working copy, using offline or immutable protection where available. Cloud synchronization alone is not a recovery strategy. Test a representative restore quarterly. Enable available security and audit logs, protect them against alteration, and review alerts promptly. Document retention by data type and contract; suspend deletion for a legal hold.

Security incident response

Users report suspected compromise immediately to the CEO and IT administrator. Isolate affected devices or disable exposed accounts when safe, preserve logs and evidence, assess affected data, and record the incident timeline. Obtain qualified assistance, reset credentials through a trusted device, remove the cause, and restore verified clean data. The CEO evaluates contractual and statutory notice duties immediately; report within applicable deadlines.

Federal contract safeguards

Before award or data access, map each incorporated FAR or agency security clause to controls, responsible persons, and evidence. For federal contract information, verify the basic safeguarding measures required by FAR 52.204-21. Confirm required subcontract flowdowns and provider restrictions. Additional controlled-information or defense clauses may require separate systems and reporting. A policy document alone does not establish CMMC compliance or assessment status.

Security administration records

Register	Required fields
Assets and services	Asset or service; owner; data class; authorization; support status
Access approvals	User; role; permissions; approver; start and end dates; review
Control evidence	Requirement; implementation; evidence; test date; owner; gap
Incident record	Detection time; scope; containment; evidence; notices; recovery; lessons
Exception record	Risk; compensating controls; approver; expiry; closure

Training and review

Provide security orientation before access and annual refresher training. Review incidents and overdue controls monthly. Test the response process annually. Exceptions require CEO approval, a time limit, and compensating controls; no exception may waive law or contract. References: NIST Small Business Cybersecurity Corner, <https://www.nist.gov/itl/smallbusinesscyber>; FAR 52.204-21, <https://www.acquisition.gov/far/52.204-21>.