ELEVATE
SOLUTIONS

TEMPLATE · COMPLIANCE & RISK

IT Security Policy Template Pack

6 policies, NIST-aligned

Six foundational security policies ready to customize: acceptable use, access control, device security, data handling, incident reporting, and remote work. Replace the bracketed fields, run legal review, approve, and attest annually.

01 — ACCEPTABLE USE

How to adopt this pack, then Policy 1

Written policies are the first thing auditors, cyber insurance carriers, and client security questionnaires ask for — and the first thing regulators request after an incident. These six templates give you a defensible baseline. They only count if they describe what your firm actually does.

Each policy follows the same structure: Purpose, Scope, numbered Policy Statements, Enforcement, and Review Cadence, plus a one-line mapping to the NIST Cybersecurity Framework so you can show alignment without buying a consulting engagement. Most of the breaches these policies prevent involve people, not exotic exploits — the human element is involved in 60% of breaches. Verizon DBIR 2025

- [ ] **Replace every bracketed field** 1
  [Company], contacts, systems, and timeframes. Every bracket is a decision, not a blank — pick numbers your team can actually meet.
- [ ] **Cut anything you will not enforce** 2
  An unenforced clause is worse than no clause: it documents a control you claim to have and don't. Auditors and opposing counsel both notice.
- [ ] **Route through legal and compliance review** 3
  Monitoring notices, sanctions language, and retention rules vary by jurisdiction and regulator — HIPAA, state bar rules, FTC Safeguards, CCPA/CPRA.
- [ ] **Approve formally** 4
  Management signature, version number, effective date. Unapproved drafts carry no weight in an audit or a dispute.
- [ ] **Distribute and collect signed attestations** 5
  From every workforce member, including contractors and temps. Keep the attestations — they are your evidence.
- [ ] **Re-attest annually and on material change** 6
  Recirculate after any significant revision, merger, platform change, or incident. Track completion to 100%.

> DRAFTING CONVENTION
>
> In these templates, **must / must not** means mandatory, **may** means permitted, and bracketed text **[like this]** is a field you replace. There is deliberately no "should" — auditable policy states requirements, not suggestions.

Policy 1 — Acceptable Use Policy

NIST CSF 2.0 mapping: **Govern (GV)** — organizational cybersecurity policy (GV.PO), with workforce awareness outcomes under Protect (PR.AT).

Policy owner _____ **Effective date** _____ **Next review** _____

1. PURPOSE

This policy defines acceptable use of [Company] information systems, accounts, and data. It protects [Company], its clients, and its workforce from legal, regulatory, and security harm arising from misuse of technology.

2. SCOPE

All employees, contractors, temporary staff, and interns ("workforce members"), on all systems owned, leased, or managed by [Company], including company accounts accessed from personal devices.

3. POLICY STATEMENTS

3.1 **Ownership and monitoring.** [Company] systems, accounts, and the data on them are [Company] property. Activity on company systems may be logged, monitored, and reviewed for security, legal, and operational purposes to the extent permitted by law. Workforce members have no expectation of privacy in company systems.

3.2 **Authorized use only.** Workforce members must use company systems only for authorized business purposes and only with the access assigned to them. Attempting to access systems or data beyond one's authorization is prohibited.

3.3 **Prohibited activities.** Workforce members must not: (a) use company systems for unlawful activity or to harass, threaten, or discriminate; (b) install software not present in the [Approved Software Register]; © disable, bypass, or tamper with security controls, including antivirus/EDR, encryption, web filtering, and update mechanisms; (d) share credentials or use another person's account; (e) store company data in personal cloud storage, personal email, or unapproved messaging apps; (f) connect unauthorized hardware, including personal USB storage, to company systems; (g) use company systems to operate a personal business; (h) copy or remove company or client data except as required by an assigned task.

3.4 **Email conduct.** Business email must be conducted through [Company] email accounts. Automatic forwarding of company email to external addresses is prohibited. Workforce members must report suspicious messages using [the report button / IT contact] and must not reply to, click, or forward them.

3.5 **Web conduct.** Web access through company systems is filtered. Workforce members must not use proxies, VPNs, or other means to circumvent filtering, and must not access content that is illegal or violates [Company] workplace conduct policies.

3.6 **AI tools.** Workforce members may use only AI tools listed in the [Approved Software Register], under company accounts. Client data, personal information, regulated data (including PHI), privileged material, and [Company] confidential information must not be entered into unapproved AI tools.

3.7 **Personal use.** Incidental personal use of company systems is permitted if it is brief, lawful, does not interfere with work or others, does not consume material resources, and does not involve storing personal files, media libraries, or backups on company systems.

3.8 **Credentials.** Workforce members must use unique passwords for company accounts, store them only in the [approved password manager], and complete multi-factor authentication prompts only for sign-ins they initiated. Unexpected MFA prompts must be denied and reported.

3.9 **Duty to report.** Workforce members must report suspected violations of this policy and suspected security incidents to [IT Contact] as described in the Incident Reporting Policy.

4. ENFORCEMENT

Violations are subject to disciplinary action up to and including termination of employment, consistent with [Company] HR procedures. For contractors, violations may result in termination of the engagement. Suspected unlawful activity will be referred to counsel and, where appropriate, law enforcement. [IT Contact] may suspend access immediately to contain risk pending review.

5. REVIEW CADENCE

[Policy Owner] reviews this policy at least annually and after any material incident, organizational change, or regulatory change. All workforce members re-attest at hire and annually thereafter.

02 — ACCESS CONTROL

Policy 2 — Access Control Policy

Access control is the policy auditors test hardest, because it produces evidence: tickets, approval records, and review sign-offs. Set timeframes you can prove, then prove them.

NIST CSF 2.0 mapping: **Protect (PR)** — Identity Management, Authentication, and Access Control (PR.AA).

Policy owner _____ **Effective date** _____ **Next review** _____

1. PURPOSE

This policy governs how access to [Company] systems and data is requested, granted, changed, reviewed, and removed, so that each workforce member holds only the access required for their role.

2. SCOPE

All accounts on all [Company] systems and applications, including employee, contractor, vendor, service, and administrative accounts, whether hosted on-premises or in cloud services.

3. POLICY STATEMENTS

3.1 **Least privilege.** Access is granted at the minimum level required to perform assigned duties. Convenience, seniority, and "just in case" are not justifications for access.

3.2 **Role-based access.** [Company] maintains a documented catalog of roles and the system entitlements each role carries. Access is assigned by role wherever the system supports it; individual exceptions require documented approval by the [system owner].

3.3 **Provisioning.** Access is created only from a documented request approved by the workforce member's manager and the system owner. New-hire access is provisioned no earlier than [2 business days] before the start date and activated on day one.

3.4 **Deprovisioning.** On voluntary departure, all accounts are disabled within [4 business hours] of the final work hour. For involuntary terminations, accounts are disabled before or at the moment of notification. HR must notify [IT Contact] of all departures the same business day.

3.5 **Role changes.** When a workforce member transfers roles, the receiving manager and [IT Contact] re-baseline access within [5 business days]. Prior-role entitlements are removed, not accumulated.

3.6 **Multi-factor authentication.** MFA is required for all user accounts on email, remote access, and cloud applications, with no exceptions for executives. Administrative accounts must use phishing-resistant MFA (FIDO2 security key or platform passkey) where the system supports it.

3.7 **Privileged accounts.** Administrative privileges require a separate, named admin account distinct from the user's daily account. Admin accounts must not be used for email or web browsing, must be inventoried, and their credentials must be stored in the [approved vault]. Standing global-admin rights are limited to [2] named individuals plus one emergency access account with sealed credentials.

3.8 **Service accounts.** Every service account has a documented owner, purpose, and scope; interactive logon is disabled; credentials are rotated on owner change and at least every [12 months].

3.9 **Shared and vendor accounts.** Shared accounts are prohibited unless the system cannot support individual accounts, in which case use requires a documented exception with a compensating control. Vendor and third-party access must be sponsored by an employee, time-bound, limited to named systems, and disabled at engagement end.

3.10 **Access reviews.** System owners review and certify all access to in-scope systems quarterly, and all privileged access monthly. Review results, removals, and sign-offs are retained as audit evidence for [3 years].

4. ENFORCEMENT

Access granted outside this process will be revoked on discovery and the grant investigated. Managers who approve access without business justification, and administrators who provision without an approved request, are subject to disciplinary action under [Company] HR procedures. Quarterly review completion is reported to [management/ownership].

5. REVIEW CADENCE

[Policy Owner] reviews this policy annually and whenever a major system is added or replaced. The quarterly and monthly access reviews in clause 3.10 operate as standing controls under this policy, not as substitutes for the annual policy review.

Policy 3 — Device Security · Policy 4 — Data Handling

Two policies share this section because they fail together: an unencrypted laptop is a data-handling incident the moment it leaves the office. Adopt both or neither.

Policy 3 — Device Security Policy

NIST CSF 2.0 mapping: **Protect (PR)** — Platform Security (PR.PS), with device inventory under Identify (ID.AM).

Policy owner _____ **Effective date** _____ **Next review** _____

1. PURPOSE

This policy sets minimum security requirements for endpoints that access [Company] systems or data, so that a lost, stolen, or compromised device does not become a reportable data breach.

2. SCOPE

All laptops, desktops, tablets, and smartphones that access [Company] data — company-owned and, where permitted under clause 3.7, personally owned.

3. POLICY STATEMENTS

3.1 **Management and inventory.** Company devices must be enrolled in [Company]'s device management platform before first use and remain enrolled for their service life. [IT Contact] maintains an inventory of all managed devices, including assigned user and disposition.

3.2 **Encryption.** Full-disk encryption (BitLocker on Windows, FileVault on macOS, platform encryption on mobile) must be enabled on every device, with recovery keys escrowed to the management platform — never stored by the user alone.

3.3 **Screen lock.** Devices must lock automatically after no more than [10] minutes of inactivity and require authentication to resume. Workforce members must lock devices manually when stepping away.

3.4 **Patching.** Operating system and application updates are deployed through the management platform. Critical security updates must be installed within [7 days] of release; all other security updates within [30 days]. Users must not defer mandated restarts beyond [48 hours]. Devices running operating systems past end-of-support must not access company data.

3.5 **Endpoint protection.** [Company]'s endpoint detection and response agent must be installed, running, and reporting on every managed device. Disabling or tampering with the agent is prohibited and generates an alert.

3.6 **Local privileges.** Workforce members do not hold local administrator rights on company devices. Software installation and elevation requests go through [IT Contact].

3.7 **Personal devices.** Personally owned devices may access only [email/approved collaboration apps], only through [Company]'s mobile application management profile, which enforces encryption, PIN, and the ability to remove company data without touching personal data. Jailbroken or rooted devices are prohibited.

3.8 **Loss or theft.** A lost or stolen device must be reported to [IT Contact] immediately and in no case later than [4 hours] after discovery, at any hour. [IT Contact] will remotely lock or wipe the device and record the event under the Incident Reporting Policy. Prompt reporting is a defense, not an offense — see the no-blame clause in Policy 5.

3.9 **Disposal.** Devices leaving service must have storage sanitized using methods aligned with NIST SP 800-88 (cryptographic erase or destruction) and the disposition recorded in the inventory before resale, recycling, or donation.

4. ENFORCEMENT

Non-compliant devices are blocked from company resources automatically by conditional access where supported, and manually otherwise. Repeated or willful violations — particularly disabling protections or failing to report a lost device — are handled under [Company] disciplinary procedures.

5. REVIEW CADENCE

[Policy Owner] reviews this policy annually and after any change of device platform, management tooling, or operating system support status.

Policy 4 — Data Handling Policy

NIST CSF 2.0 mapping: **Identify (ID) + Protect (PR)** — Asset Management (ID.AM) and Data Security (PR.DS).

Policy owner _____ **Effective date** _____ **Next review** _____

1. PURPOSE

This policy classifies [Company] data and sets handling rules for storage, sharing, retention, and disposal, so that protection matches sensitivity and regulated data is handled to the standard regulators expect.

2. SCOPE

All data created, received, or processed by [Company] in any form — electronic, paper, and spoken — across all systems and locations.

3. POLICY STATEMENTS

3.1 **Classification tiers.** All data is classified into one of four tiers. Data of unknown classification is treated as Internal until classified; when in doubt between two tiers, the higher tier applies.

TIER	EXAMPLES	CORE HANDLING RULE
Public	Marketing material, published filings	May be shared without restriction once approved for release by [owner].
Internal	Procedures, org charts, internal email	Stays inside [Company] systems; external sharing requires manager approval.
Confidential	Client files, contracts, financials, HR records	Access on need-to-know; external sharing only via approved encrypted channels with a business reason.
Restricted	PHI, SSNs, payment card data, privileged matter files	Named-access only; stored solely in [approved systems of record]; every external disclosure logged and, where required, covered by a BAA or equivalent agreement.

3.2 **Approved storage.** Company data must reside only in [Company]-approved systems listed in the [Approved Systems Register]. Storage of Confidential or Restricted data on personal devices, personal cloud accounts, personal email, or unencrypted removable media is prohibited.

3.3 **Sharing.** Confidential and Restricted data sent externally must use [approved secure-sharing method] with encryption in transit, recipient verification, and link expiration of no more than [14 days]. Open "anyone with the link" sharing is prohibited for these tiers.

3.4 **Removable media.** Use of removable media for Confidential or Restricted data requires documented approval from [IT Contact] and hardware or software encryption of the media.

3.5 **Regulated data.** PHI, consumer personal information, and cardholder data are handled per [Company]'s obligations under applicable law and contracts (HIPAA, CCPA/CPRA, GLBA/FTC Safeguards, PCI DSS as applicable). Where this policy and a regulation differ, the stricter requirement applies.

3.6 **Retention.** Data is retained per the [Company] Retention Schedule and no longer. Workforce members must not maintain private "shadow archives" of company or client data outside the systems of record. Legal holds issued by counsel suspend disposal for the data they cover.

3.7 **Disposal.** Electronic data is deleted from the system of record and any synchronized copies at end of retention; storage media follow Policy 3 clause 3.9. Paper containing Internal-or-higher data is cross-cut shredded or placed in locked shred bins — never general trash or open recycling.

3.8 **Mis-sent and mishandled data.** Sending data to the wrong recipient, or discovering data stored or shared in violation of this policy, must be reported under the Incident Reporting Policy the same day it is discovered.

4. ENFORCEMENT

[IT Contact] may remove improperly stored data, revoke shares, and disable external sharing for repeat violators. Violations involving Restricted data are escalated to [Compliance Officer/Counsel] for notification analysis. Disciplinary measures follow [Company] HR procedures.

5. REVIEW CADENCE

[Policy Owner] reviews this policy annually, when the Retention Schedule changes, and when a new regulation or client contractual requirement takes effect.

Policy 5 — Incident Reporting · Policy 6 — Remote Work

Speed of reporting determines breach cost more than almost anything a policy can control: breaches contained in under 200 days averaged $3.61M vs $5.49M for those over 200 days. IBM Cost of a Data Breach Report 2025 Your workforce only reports fast if the policy makes reporting safe.

Policy 5 — Incident Reporting Policy

NIST CSF 2.0 mapping: **Detect (DE) + Respond (RS)** — Adverse Event Analysis (DE.AE) and Incident Management (RS.MA).

Policy owner _____ **Effective date** _____ **Next review** _____

1. PURPOSE

This policy defines what workforce members must report, how fast, and through which channels, so that [Company] detects incidents early, preserves evidence, and meets legal and contractual notification duties.

2. SCOPE

All workforce members. This policy covers reporting and initial escalation; detailed response actions live in [Company]'s incident response plan.

3. POLICY STATEMENTS

3.1 **Reportable events.** Workforce members must report: a clicked phishing link or opened suspicious attachment; entry of credentials on a suspicious page; an unexpected MFA prompt; a lost or stolen device; a malware or EDR alert; suspected unauthorized access or account behavior; data sent to the wrong recipient; a ransom note or file-encryption symptoms; a breach notice from any vendor; and anything that seems wrong even if it fits no category.

3.2 **Timeframes.** Events suggesting an active compromise — ransomware symptoms, credential entry on a fake page, unauthorized access in progress — must be reported immediately, and in no case later than [1 hour] after discovery. All other reportable events must be reported the same business day.

3.3 **Channels.** Reports go to [IT Contact] via [phone number] or [reporting channel]. If company email or chat may be compromised, report by phone or in person — not through the suspect system. After-hours reports use [on-call number].

3.4 **No-blame clause.** A workforce member who promptly reports an incident in good faith will not face discipline for the honest error that caused it. Concealing, delaying, or minimizing an incident is itself a serious policy violation. The fastest report is always the right answer.

3.5 **Preserve, don't investigate.** Reporters must not power off affected machines, delete suspicious emails or files, run cleanup tools, or attempt their own investigation. Disconnect from the network if instructed, note the time and what was observed, and wait for [IT Contact].

3.6 **Escalation.** [IT Contact] triages every report, assigns a severity, and opens an incident record. Severity [1–2] incidents are escalated the same hour to [Incident Commander], who engages counsel and the cyber insurance carrier before remediation decisions that could affect coverage or evidence.

3.7 **Confidentiality.** Incident details are shared on need-to-know only. Workforce members must not discuss incidents with clients, media, or on social channels; external statements come only from [designated spokesperson].

3.8 **Records.** Every report — including false alarms — is logged with timestamps, reporter, and disposition, and retained for [3 years]. False alarms are never penalized; they are evidence the reporting culture works.

4. ENFORCEMENT

Failure to report a known reportable event, or interference with evidence, is handled under [Company] disciplinary procedures and weighed more seriously than the underlying error. Managers must never instruct staff to delay or withhold a report.

5. REVIEW CADENCE

[Policy Owner] reviews this policy annually and after every severity [1–2] incident as part of the lessons-learned review, updating reportable-event examples and contact details as needed.

Policy 6 — Remote Work Policy

NIST CSF 2.0 mapping: **Protect (PR)** — applies PR.AA, PR.DS, and PR.PS requirements to work performed outside [Company] facilities.

Policy owner _____ **Effective date** _____ **Next review** _____

1. PURPOSE

This policy extends [Company]'s security requirements to work performed from home, client sites, and travel, where company controls do not reach the physical environment.

2. SCOPE

All workforce members performing any work outside [Company] facilities, on any device that touches company data.

3. POLICY STATEMENTS

3.1 **Approved devices only.** Remote work is performed on company-managed devices, or on personal devices compliant with Policy 3 clause 3.7. All other devices, including family or hotel computers, are prohibited for company work.

3.2 **Home network.** Home Wi-Fi used for work must use WPA2 or WPA3 with a non-default password, and the router's administrative password must be changed from the factory default. Work devices must not join open or unknown networks at home.

3.3 **Public networks.** On public or guest Wi-Fi, company resources may be accessed only through [Company]'s VPN or zero-trust access client, or via cellular hotspot instead.

3.4 **Visual and audio privacy.** In public or shared spaces, screens must use a privacy filter or be positioned away from view, devices must be locked when unattended even briefly, and calls discussing Confidential or Restricted matters must be taken in private.

3.5 **Household separation.** Family and household members must not use work devices or view work material. Work accounts must not be signed in on shared household devices.

3.6 **Printing and paper.** Printing Confidential or Restricted material remotely requires manager approval. Printed work material must be stored out of sight and destroyed by cross-cut shredding or returned to the office for disposal — never household trash.

3.7 **Approved tools.** Remote collaboration uses only [Company]-approved tools per the Acceptable Use Policy. Personal messaging apps and personal cloud accounts are prohibited for work content regardless of convenience.

3.8 **Incidents.** The Incident Reporting Policy applies identically off-site, including the [1 hour] timeframe for active-compromise indicators and the [4 hour] lost-device timeframe.

4. ENFORCEMENT

Remote access may be suspended for devices or workforce members out of compliance with this policy until remediated. Violations follow [Company] disciplinary procedures; repeated violations may result in withdrawal of remote work eligibility.

5. REVIEW CADENCE

[Policy Owner] reviews this policy annually and when remote access technology or workforce arrangements change materially.

> **WANT THE FULL VERSION?**
>
> This is the summary policy, sized for a six-policy pack. For the complete standalone version — with home-office setup, travel, and verification controls — see Elevate's Remote Work Security Policy resource in the same library.

ELEVATE
SOLUTIONS

Elevate Solutions provides managed IT and cybersecurity for businesses that answer to regulators, clients, and courts.

Elevate Solutions

6230 Wilshire Blvd Suite 2120, Los Angeles CA 90048

(424) 400-6625 · support@elevatesolutions.io · elevatesolutions.io