

Cybersecurity Checklist for 2026

General security

- ☐ Set up security@ email address (forward to developers group)
- ☐ Perform regular system vulnerability sweeps
- ☐ Create a set of security policies and document them, holding them in a specific folder, either digitally or on paper.

Incident Response Plan

- ☐ Prepare for ransomware attack (establish a response team, emergency contact list, consider cybersecurity liability insurance, determine the limit you're willing to pay)
- ☐ Create an incident response plan that outlines responsibilities and steps for detecting, reporting, and responding to an incident
- ☐ Set up a process for regularly reviewing, updating, and communicating this plan
- ☐ Use automation and AI to detect and respond to incidents faster

Pentesting

- ☐ Start bug bounty program (e.g., Hacker One, Bugcrowd)
- ☐ Use a third-party tool (e.g., Cobalt, Securisea)

Intrusion Detection

- ☐ Monitor dark web for a data breach (e.g., PhishLabs)
- ☐ Host-based IDS (e.g., OSSEC, Wuzah, Tripwire, rkhunter)
- ☐ Network-based IDS (e.g., Suricata, Snort, Bro)

Personnel

- ☐ Onboarding (for employees and contractors):
 - ☐ Complete background checks
 - ☐ Ensure access provisioning has necessary approvals and is tracked
 - ☐ Complete NDAs as necessary

Risk and Vulnerability Management

- ☐ Conduct continuous risk assessments
- ☐ Regular vulnerability scanning and remediation

Communication and Collaboration

- ☐ Increase visibility through collaborative risk assessments, cross-departmental cybersecurity committees, and joint training exercises
- ☐ Build feedback mechanisms where personnel can report potential security issues

Configuring for least functionality

- ☐ Firewall rules
- ☐ Close unnecessary ports and block unnecessary protocols and services
- ☐ Segment functions such as APIs, admin privileges, etc.

Device security

- ☐ Encrypt all devices, such as laptops and hard drives (e.g., FileVault on Mac)
- ☐ Apply device restrictions (stop backups to personal cloud storage, etc.)
- ☐ Consider providing employees with mobile devices for business purposes with remote wipe
- ☐ Block potentially dangerous apps and websites
- ☐ Prevent users from installing software
- ☐ Turn on endpoint verification

Software security

- ☐ List current system security software (e.g., firewalls, AV, SIEM tools, etc.)
- ☐ Consider data loss protection software
- ☐ Require MFA for all third-party services
 - ☐ Slack
 - ☐ GitHub
 - ☐ Heroku
 - ☐ AWS
 - ☐ Others:
- ☐ Set up a team password manager (e.g., 1Password)
- ☐ Check all software and operating systems are fully patched and updated to the latest versions. Consider an inventory management/patch management tool (e.g., FleetSmith)
- ☐ Domain names
 - ☐ Auto-renew on
 - ☐ Buy primary domains for 5-10 years (optional)
 - ☐ Transfer lock enabled (default for most services)

Application Security

- ☐ Scan website (e.g., Mozilla Observatory)
 - ☐ Everything should pass except Content Security Policy
- ☐ Code analysis
 - ☐ No credentials in code
 - ☐ Scan dependencies for vulnerabilities (e.g., GitHub, bundle-audit, npm audit, yarn audit, CodeClimate)
 - ☐ Static code analysis (e.g., Brakeman, CodeClimate, others)
- ☐ Secure password hashing (e.g., bcrypt, Argon2)
- ☐ Require MFA for admin accounts (e.g., Google Authenticator)
- ☐ Add rate-limiting
- ☐ Notify users of email and password changes (sent to old email)
- ☐ Record login attempts
- ☐ Protect against account takeovers
 - ☐ Lock accounts after too many attempts
 - ☐ Lock accounts after successful login from credential stuffing IP

Email Security

- ☐ Sender Policy Framework (SPF)
- ☐ Domain Keys Internet Mail (DKIM)
- ☐ Domain-based message authentication reporting & conformance (DMARC)
- ☐ For inactive domains, create a null SPF record: “v=spf1 -all”

Data storage & processing security

- ☐ Create an employee offboarding checklist to disable all accounts (or automate it)
- ☐ Enforce encryption for all data transmissions

Data Storage

- ☐ Create a list of personal data, where it's stored, and sensitivity level
 - ☐ Database fields (and other data stores)
 - ☐ Files
 - ☐ Third-party services
- ☐ Data at rest
 - ☐ Storage level encryption
 - ☐ Database
 - ☐ Elasticsearch
 - ☐ S3
 - ☐ Application-level encryption
 - ☐ Database fields
 - ☐ File uploads
 - ☐ Use authenticated encryption (e.g., AES-GCM or Libsodium)

Data access & processing

- ☐ Data in transit
 - ☐ External
 - ☐ HTTPS everywhere (including subdomains)
 - ☐ HSTS header
 - ☐ HSTS preload list (if possible)
 - ☐ Secure ciphers
 - ☐ SSL certificates not expiring soon
 - ☐ Internal
 - ☐ Postgres (sslmode=verify-full)
 - ☐ Elasticsearch (HTTPS)
 - ☐ Redis (SSL)
- ☐ Database users
 - ☐ Password greater than 32 characters
 - ☐ Use separate roles for migrations, app, and analytics

- ☐ Business Intelligence tools
 - ☐ Personal data not accessible
 - ☐ Auditing/logging
- ☐ Check for data leakage
 - ☐ Logs
 - ☐ Error reporting
 - ☐ App instrumentation
 - ☐ Third-party analytics
 - ☐ Cache stores
 - ☐ Email inboxes

End-user security

User Management

- ☐ Every 3 months (put it on your calendar):
 - ☐ Verify list of admins for all services
 - ☐ Verify list of users for all services
 - ☐ Remove inactive accounts

Internal Threats

- ☐ User activity logged
 - ☐ SSH/console logins
 - ☐ SSH/console commands
 - ☐ Separate admin privileges among multiple personnel/teams or implement approval gates

Physical & environmental security

- ☐ Lock server rooms and limit physical access to servers
- ☐ Establish a logbook or video surveillance to monitor physical access
- ☐ Document security access levels for personnel and review access periodically
- ☐ Log employee badges and keys and terminate access for departing employees
- ☐ Disable means for connecting external drives and devices
- ☐ Monitor temperature and humidity and set alerting thresholds
- ☐ Monitor water detection
- ☐ Have backup power, lighting, and fire suppression systems in place in case of emergencies
- ☐ Account for natural disasters such as earthquakes and flooding in the building design

Automated security

- ☐ Use automation and AI to streamline routine security tasks and compliance requirements
 - ☐ Continuous monitoring
 - ☐ Evidence collection

- ☐ Employee onboarding and offboarding
- ☐ Cloud remediation
- ☐ Risk assessment process
- ☐ Writing and updating security policies
- ☐ Mapping controls across framework requirements and tests
- ☐ Responding to RFPs and security questionnaires
- ☐ Assigning, tracking, and reporting on required training