GOOEY
SMART IT. SEAMLESS EXPERIENCE.

Comprehensive Cybersecurity Checklist

Enterprise-Grade Security Assessment | August 04, 2025

🚨 Critical Security Notice

This checklist represents minimum security requirements. Your specific industry regulations may require additional measures. Regular security audits and updates are essential for maintaining protection.

Infrastructure Security

Implement HTTPS with TLS 1.3 minimum

Critical

Disable older protocols (SSL, TLS 1.0/1.1), use 2048-bit RSA or 256-bit ECC certificates

Configure HTTP Strict Transport Security (HSTS)

Critical

Set max-age to at least 31536000, include subdomains, enable preload

Deploy Web Application Firewall (WAF)

High

Configure OWASP ModSecurity Core Rule Set, custom rules for application

Implement DDoS protection

High

Rate limiting, geographic filtering, traffic analysis, auto-scaling

Configure secure DNS (DNSSEC)

Medium

Prevent DNS hijacking and cache poisoning attacks

Network segmentation and VLANs

High

Isolate critical systems, DMZ for public-facing services

Intrusion Detection/Prevention System (IDS/IPS)

High

Real-time threat detection and automated response

Access Control & Authentication

Enforce strong password policy — Critical

Minimum 14 characters, complexity requirements, password history, 90-day expiration

Implement Multi-Factor Authentication (MFA) — Critical

TOTP/hardware tokens for admin, SMS/app for users, backup codes

Role-Based Access Control (RBAC) — High

Principle of least privilege, regular access reviews, automated deprovisioning

Single Sign-On (SSO) with SAML 2.0 — Medium

Centralized authentication, session management, federated identity

Account lockout policies — High

5 failed attempts, 30-minute lockout, CAPTCHA after 3 attempts

Privileged Access Management (PAM) — High

Vault for admin credentials, just-in-time access, session recording

API key management and rotation — High

Encrypted storage, 90-day rotation, usage monitoring

💾 Data Protection

⚠️ Encryption at rest (AES-256) Critical

Database encryption, file system encryption, encrypted backups

🔒 Encryption in transit (TLS 1.2+) Critical

All data transfers, API communications, internal services

🔒 Database security hardening High

Remove default accounts, parameterized queries, connection encryption

🔒 Input validation and sanitization Critical

Prevent SQL injection, XSS, command injection, XXE attacks

🔒 Secure file upload handling High

File type validation, size limits, virus scanning, sandboxing

🔒 Data Loss Prevention (DLP) Medium

Content inspection, data classification, egress monitoring

🔒 Secure data disposal Medium

DOD 5220.22-M standard, certificate of destruction

Logging & Monitoring

Centralized log management (SIEM) High

Aggregate all logs, correlation rules, automated alerting

Security event monitoring 24/7 Critical

Real-time threat detection, incident response team

File Integrity Monitoring (FIM) High

Critical file changes, unauthorized modifications, compliance reporting

User activity auditing High

Login attempts, privilege escalation, data access patterns

Network traffic analysis Medium

NetFlow/sFlow, anomaly detection, behavioral analysis

Log retention policy (1+ years) Medium

Compliance requirements, encrypted storage, tamper-proof

Vulnerability Management

Regular security patching schedule — Critical

Critical patches within 24 hours, regular patches monthly

Vulnerability scanning (weekly) — High

Authenticated scans, web application scanning, API testing

Penetration testing (quarterly) — High

External/internal tests, social engineering, physical security

Dependency scanning for libraries — High

OWASP dependency check, npm audit, automated updates

Security code review — Medium

Static/dynamic analysis, peer review, secure coding standards

Bug bounty program — Low

Responsible disclosure, vulnerability rewards, hall of fame

Incident Response

⚠ Incident Response Plan (IRP) documented — Critical

Roles, procedures, escalation, communication templates

Incident Response Team identified — Critical

24/7 contact list, defined responsibilities, backup personnel

Forensic toolkit prepared — High

Evidence collection tools, chain of custody procedures

Communication plan for breaches — High

Customer notification, regulatory reporting, PR response

Regular incident response drills — Medium

Tabletop exercises, simulated breaches, lessons learned

Cyber insurance coverage — Medium

Data breach, business interruption, cyber extortion

🎓 Security Awareness

Security awareness training (quarterly) High

Phishing, social engineering, password security, data handling

Phishing simulation campaigns Medium

Monthly tests, targeted training for failures, metrics tracking

Security policies and procedures High

Acceptable use, BYOD, remote work, incident reporting

Vendor security assessments Medium

Third-party risk management, security questionnaires, audits

📊 Compliance Requirements

Regulation	Applies To	Key Requirements
GDPR	EU Data	Privacy by design, consent, data portability, breach notification (72hrs)
CCPA	California Residents	Privacy rights, opt-out, data disclosure, non-discrimination
PCI DSS	Payment Cards	Network security, encryption, access control, testing
HIPAA	Healthcare Data	PHI protection, minimum necessary, audit controls, BAAs
SOC 2	Service Providers	Security, availability, confidentiality, privacy controls
ISO 27001	International	ISMS, risk assessment, continuous improvement

✅ Security Best Practices

- Implement Zero Trust architecture - never trust, always verify
- Adopt DevSecOps - integrate security into development lifecycle
- Regular security assessments - quarterly reviews minimum
- Maintain security documentation - policies, procedures, runbooks
- Stay informed - subscribe to security advisories and threat feeds
- Test your backups - regular restoration drills

Version 3.0 | Security Framework Compliant | Last Updated: August 2025