CSNP
CYBERSECURITY NON-PROFIT

Complete Security Audit Checklist

A comprehensive quarterly and annual audit framework for small to medium businesses and nonprofit organizations. Ensure your organization meets essential security standards across all critical domains.

AUDIT OVERVIEW

Security Audit Domains

This comprehensive checklist covers nine essential security domains to protect your organization. Use this framework for quarterly reviews and annual audits to maintain robust security posture.

Access Control

User permissions, authentication, and authorization protocols

Network Security

Firewalls, monitoring, and network segmentation

Data Protection

Encryption, backups, and data lifecycle management

Endpoint Security

Device management and protection protocols

Communications

Email security and messaging safety

Physical Security

Facility access and hardware protection

DOMAIN 1

Access Control & Identity Management

1

Multi-Factor Authentication

- MFA enabled for all user accounts
- Administrative accounts require additional verification
- Password policies enforce complexity requirements

2

Access Reviews

- Quarterly review of user access permissions
- Removal of inactive accounts within 30 days
- Role-based access control properly implemented

3

Privileged Access

- Administrative access limited to authorized personnel
- Privileged sessions logged and monitored
- Regular rotation of administrative credentials

DOMAIN 2 & 3

Network Security & Data Protection

Network Security

- **Firewall Configuration**

  All firewalls properly configured and regularly updated with security patches

- **Network Monitoring**

  Intrusion detection systems active and alerts reviewed daily

- **WiFi Security**

  Guest and corporate networks segregated with WPA3 encryption

- **VPN Implementation**

  Remote access secured through encrypted VPN connections

Data Protection

- **Encryption Standards**

  Data encrypted at rest and in transit using industry standards

- **Backup Procedures**

  Automated backups run daily with monthly restoration tests

- **Data Classification**

  Sensitive data identified and labeled according to policy

- **Retention Policies**

  Data retention and disposal procedures documented and followed

DOMAIN 4 & 5

Endpoint & Communication Security

1

Endpoint Protection

All devices have updated antivirus and anti-malware software. Mobile device management policies enforce security configurations. Automatic patching enabled for operating systems and applications.

2

Email Security

Spam filters and anti-phishing tools actively blocking threats. Email authentication protocols (SPF, DKIM, DMARC) properly configured. Staff trained to identify and report suspicious emails.

3

Secure Messaging

Approved communication platforms use end-to-end encryption. File sharing tools meet organizational security requirements. Personal messaging apps restricted on company devices.

DOMAIN 6 & 7

Physical Security & Vendor Management

Physical Security

1 Facility Access

Badge systems control building entry. Visitor logs maintained and reviewed.

2 Hardware Security

Server rooms locked with limited access. Equipment disposal follows secure protocols.

3 Surveillance

Security cameras monitor critical areas. Footage retained per policy.

Vendor Management

1 Vendor Assessment

Security questionnaires completed before onboarding. Annual reviews conducted.

2 Contract Review

Security requirements included in all vendor contracts. Data handling agreements signed.

3 Access Control

Third-party access limited and monitored. Vendor accounts disabled when not needed.

DOMAIN 8

Incident Response & Recovery

Detection

Security incidents identified through monitoring systems. Clear reporting procedures established and communicated.

Response Plan

Documented incident response procedures available. Response team roles and responsibilities defined.

Communication

Stakeholder notification procedures in place. Legal and regulatory reporting requirements understood.

Recovery

Business continuity plans tested annually. Disaster recovery procedures documented and accessible.

DOMAIN 9

Compliance & Security Training

Regulatory Compliance

01

Requirements Tracking

Applicable regulations identified (GDPR, HIPAA, PCI-DSS, etc.)

02

Policy Documentation

Security policies updated and accessible to all staff

03

Regular Audits

Compliance audits scheduled and findings addressed

Security Awareness Training

01

Onboarding Training

New employees complete security training within first week

02

Annual Refreshers

All staff complete annual security awareness training

03

Phishing Simulations

Quarterly phishing tests conducted with follow-up training

AUDIT SCHEDULE

Quarterly & Annual Review Timeline

Use this timeline to maintain consistent security practices throughout the year. Regular audits help identify vulnerabilities before they become critical issues.

1

Q1 Review

Access control audit, policy updates, phishing simulation, backup restoration test

2

Q2 Review

Network security assessment, vendor reviews, security training, incident response drill

3

Q3 Review

Endpoint security check, physical security audit, phishing simulation, compliance review

4

Q4 Annual Audit

Comprehensive review of all domains, full compliance audit, disaster recovery test, strategic planning

About Cybersecurity Non-Profit (CSNP)

> Making cybersecurity knowledge accessible to everyone through education, community, and practical resources.

Our Free Programs

Business & Non-Profit Security

Comprehensive security frameworks and checklists for organizations

Family Cybersecurity

Protecting your home network and family digital life

Kids Safety

Age-appropriate online safety education for children

Senior Digital Safety

Practical security guidance for older adults

Women's Security

Privacy and safety resources tailored for women

Parents & Educators

Tools to teach cybersecurity to the next generation

Everything we offer is completely free. Visit **csnp.org** to explore our programs and **csnp.org/resources** to download checklists, guides, and templates.