BOHIOSYSTEM

HARDENING CHECKLIST · BOHIOSYSTEM

# Hardening Checklist

Hardening controls by layer, ordered by the ratio between effort and impact, ready to apply and verify.

DOCUMENT
BS-SVC-12B

VERSION
1.0

DATE
August 1, 2026

PREPARED BY
BohioSystem

VERIFIABLE CONTROLS

> This list is ordered by **what reduces risk the most for the least effort.** If you only do the first section, you will have already covered most common attacks.

The controls are based on the CIS benchmarks and the NIST framework, adapted to the size of organization we typically work with. This is not an exhaustive compliance checklist: it is the list of what actually gets exploited.

| 5 | Prioritized | Verifiable | CIS/NIST |
|---|---|---|---|
| CONTROL LAYERS | BY REAL IMPACT | EVERY ITEM IS CHECKED | REFERENCE FRAMEWORKS |

## 01 High priority · identity and access

Most incidents start with a credential. This section has the highest return.

### Authentication

- Mandatory second factor on email, cloud, and VPN.
- No accounts shared between people.
- Passwords managed through a corporate password manager.
- Lockout after repeated failed attempts.

### Authorization

- Least-privilege access by role.
- Administrative accounts separate from day-to-day accounts.
- Quarterly review of who has access to what.
- Administrative access only from a controlled network.

### Lifecycle

- Written onboarding and offboarding procedure.
- Immediate revocation upon offboarding.
- Service accounts inventoried and assigned an owner.
- Periodic rotation of secrets and API keys.

### Third parties

- Vendor access that is temporary and tied to a named individual.
- Logging of all third-party activity.
- Automatic revocation when the work is finished.
- No credentials shared over messaging apps.

## 02 High priority · backup and recovery

### Isolation

- At least one copy outside the production network.
- Immutable copies or copies with locked retention.
- Backup credentials different from domain credentials.
- A mass encryption event must not reach the copies.

### Verification

- Restore tested within the last six months.
- Actual restore time documented.
- Automatic alert if a backup fails.
- Integrity verification of the copies.

## 03 Medium priority · systems and network

### Systems

- Security patches with a defined window.
- No end-of-support systems in production.
- Unnecessary services disabled.
- Configuration following the platform's reference benchmark.

### Network

- Segmentation by function and criticality.
- Guest network isolated from the corporate one.
- Administration not exposed to the internet.
- Firewall rules documented and reviewed.

### Encryption

- Current TLS on every published service.
- Certificates with automatic renewal.
- Encryption at rest on laptops.
- Obsolete protocols and ciphers disabled.

### Devices

- Endpoint protection active and managed.
- Encrypted disk on laptops.
- Automatic session lock.
- Device inventory with an assigned owner.

## 04 Medium priority · applications and data

### Applications

- Dependencies scanned and kept up to date.
- No secrets hardcoded in source code.
- Input validation on every form.
- Security headers configured.

### Data

- Classification by sensitivity.
- Personal data identified and protected.
- Test environments without real data.
- Defined retention and deletion policy.

## 05 Ongoing priority · detection and response

### Logging

- Centralized logs stored outside the source system.
- Retention sufficient for investigation.
- Logging of administrative access.
- Time synchronization across systems.

### Detection

- Alerts on unusual administrative access.
- Detection of suspicious execution on endpoints.
- Monitoring of changes to critical configuration.
- Someone actually reviews the alerts.

### Response

- Written response plan accessible without network access.
- Updated contact tree.
- Device isolation procedure.
- Tabletop exercise run at least once a year.

### People

- Annual awareness training.
- Periodic phishing simulations.
- Reporting channel with no consequences for whoever flags it.
- Known procedure for reporting a suspicion.

HOW TO USE THIS CHECKLIST

Go through it checking off only what you can **prove**, not what you believe is in place. The difference between “we have backups” and “we successfully restored last month in forty minutes” is exactly the difference between believing you are protected and actually being protected.

## Let’s talk

NEXT STEP

Write to us and we’ll schedule a working session at no cost to review your specific case.

CONTACT
contacto@bohiosystem.dev

WEB
bohiosystem.dev

DOCUMENT
BS-SVC-12B · v1.0