**Cybersecurity Templates**

**Cybersecurity Readiness Checklist**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Cybersecurity Readiness Checklist** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version:** |  | **Approved By:** |  |
| **Last Review Date:** |  | **Next Review Date:** |  |

Contents

[1. Cybersecurity Readiness Checklist 3](#_Toc206632078)

[1.1.Governance & Management 3](#_Toc206632079)

[1.2.Workforce Security 4](#_Toc206632080)

[1.3.Technical Controls 5](#_Toc206632081)

[1.4.Incident Response Readiness 6](#_Toc206632082)

[1.5.IT Projects & Change Management 7](#_Toc206632083)

[1.6.Recovery & Continuous Improvement 8](#_Toc206632084)

# Cybersecurity Readiness Checklist

## 1.1.Governance & Management

|  |  |  |  |
| --- | --- | --- | --- |
| **Check point** | **Description** | **Status (✔/✖)** | **Responsible** |
| |  | | --- | | Cybersecurity Policy |  |  | | --- | |  | | |  | | --- | | The organization has a documented cybersecurity policy covering prevention, detection, response, and recovery. |  |  | | --- | |  | |  |  |
| |  | | --- | | Roles & Responsibilities |  |  | | --- | |  | | |  | | --- | | A Cybersecurity Lead, CSIRT, and Executive oversight roles are defined. |  |  | | --- | |  | |  |  |
| |  | | --- | | Risk Assessments |  |  | | --- | |  | | |  | | --- | | Regular (annual/quarterly) security risk assessments are performed and documented. |  |  | | --- | |  | |  |  |
| |  | | --- | | Legal & Regulatory Compliance |  |  | | --- | |  | | Organization complies with applicable laws (GDPR, HIPAA, etc.). |  |  |
| |  | | --- | | Vendor & Third-Party Security |  |  | | --- | |  | | |  | | --- | | Contracts include cybersecurity clauses, risk assessments, and monitoring. |  |  | | --- | |  | |  |  |

## 1.2.Workforce Security

|  |  |  |  |
| --- | --- | --- | --- |
| **Check point** | **Description** | **Status (✔/✖)** | **Responsible** |
| |  | | --- | | Security Awareness Training |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Annual training on phishing, password hygiene, and incident reporting. |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  |  |  | | --- | --- | --- | | |  | | --- | | Access Control |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Role-based access management, least privilege applied. |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  |  |  | | --- | --- | --- | | |  | | --- | | Onboarding/Offboarding |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | User access is reviewed at hiring, role change, and termination. |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Background Screening |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | | |  | | --- | | Personnel with access to sensitive data undergo vetting. |  |  | | --- | |  | |  |  |

## 1.3.Technical Controls

|  |  |  |  |
| --- | --- | --- | --- |
| **Check point** | **Description** | **Status (✔/✖)** | **Responsible** |
| |  |  |  | | --- | --- | --- | | |  | | --- | | Data Backup & Recovery |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  |  |  | | --- | --- | --- | --- | | |  |  | | --- | --- | | Daily backups, offsite storage, immutable copies, and restore are tested annually. |  |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Multi-Factor Authentication |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Enforced on all critical systems, SaaS apps, and admin accounts. |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Patch Management |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Systems are updated monthly (critical patches within 72 hours). |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Endpoint Security |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | All devices run updated EDR/AV, firewall enabled. |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| Encryption | |  | | --- | | Full-disk encryption on laptops/servers, as well as encrypted communication (TLS). |  |  | | --- | |  | |  |  |
| Network Security | |  | | --- | | Firewalls, IDS/IPS, DNS protections, and email filtering are in place. |  |  | | --- | |  | |  |  |

## 1.4.Incident Response Readiness

|  |  |  |  |
| --- | --- | --- | --- |
| **Check point** | **Description** | **Status (✔/✖)** | **Responsible** |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Incident Response Plan (IRP) |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Documented, tested annually, and aligned with the business continuity plan. |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Incident Detection & Logging |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Enforced on all critical systems, SaaS apps, and admin accounts. |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | CSIRT Activation |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Roles and contact list defined for incident response. |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Evidence Handling |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Evidence collection procedures and chain-of-custody templates exist. |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  | | --- | | Communications Plan |  |  | | --- | |  | | |  |  | | --- | --- | | |  | | --- | |  | |  |  | | --- | |  | | Internal & external communication protocols defined (media, regulators, clients). | |  |  | | --- | |  | |  |  |

## 1.5.IT Projects & Change Management

|  |  |  |  |
| --- | --- | --- | --- |
| **Check point** | **Description** | **Status (✔/✖)** | **Responsible** |
| |  | | --- | | Security Awareness Training |  |  | | --- | |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | All changes are classified planned/emergency/project. |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Threat Modeling |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Security risks are identified and assessed before implementation. |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Testing & Simulation |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Changes are tested in the staging environment before being deployed to production. |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Sign-Off Process |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Stakeholder and security approval are required before going live. |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  | | --- | | Post-Implementation Review |  |  | | --- | |  | | |  | | --- | | Monitoring and documentation of implemented changes. |  |  | | --- | |  | |  |  |

## 1.6.Recovery & Continuous Improvement

|  |  |  |  |
| --- | --- | --- | --- |
| **Check point** | **Description** | **Status (✔/✖)** | **Responsible** |
| |  |  |  | | --- | --- | --- | | |  | | --- | | Disaster Recovery Plan |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | DRP is tested annually and includes critical systems, as well as a communication plan. |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Cyber Insurance |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Policy reviewed annually, includes ransomware coverage. |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Post-Incident Review |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Lessons learned are documented after each incident. |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Security Metrics |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | Regular reporting on security KPIs (patching %, phishing test results, Secure Score). |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  |
| |  |  |  | | --- | --- | --- | | |  | | --- | | Continuous Improvement |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | The security roadmap has been updated based on threats, incidents, and audits. |  |  | | --- | |  | |  |  | | --- | |  | |  |  |