Security Readiness Checklist

Asset Management

- ❑ Maintain a complete and updated asset inventory (hardware, software, cloud, users)
- ❑ Identify business-critical systems and data repositories
- ❑ Remove or isolate unsupported or end-of-life systems
- ❑ Ensure all devices are enrolled in management (MDM/EDR/patching systems)

Identity & Access Management

- ❑ Enforce MFA for all privileged and remote accounts
- ❑ Implement least-privilege access across all systems
- ❑ Review admin accounts quarterly
- ❑ Disable stale, unused, or orphaned accounts
- ❑ Enforce strong password policies or passwordless authentication
- ❑ Implement SSO and centralized identity management (Azure AD, Okta, etc.)

Endpoint & Device Security

- ❑ Deploy EDR/AV on all endpoints (workstations, servers, cloud workloads)
- ❑ Enforce disk encryption (BitLocker/FileVault)
- ❑ Enforce OS and application patching within compliance timeframes
- ❑ Lock down USB and removable media usage
- ❑ Enforce secure configuration baselines (CIS, NIST)

Network Security

- ❑ Configure firewalls with least privilege rules
- ❑ Segment networks (user, server, guest, IoT)
- ❑ Disable unused ports, services, and VLANs
- ❑ Monitor internal east-west traffic for anomalies
- ❑ Use secure VPN or Zero Trust Access for remote work

Data Protection

- ❑ Maintain encrypted backups stored offline or immutably
- ❑ Classify data by sensitivity (public / internal / confidential)

- ❑ Enforce encryption in transit and at rest
- ❑ Limit access to sensitive data repositories
- ❑ Monitor data exfiltration and abnormal access patterns

Security Operations

- ❑ Security logs collected and centralized (SIEM)
- ❑ Alerts triaged within defined SLAs
- ❑ Regular asset vulnerability scans
- ❑ Monthly security patch reviews
- ❑ Threat intelligence monitoring enabled
- ❑ Regular phishing simulations and user awareness programs

Policies & Governance

- ❑ Updated Information Security Policy
- ❑ Acceptable Use Policy for all employees
- ❑ Access Control & Password Policies
- ❑ Change Management Process
- ❑ Vendor Management & Third-Party Risk Policies
- ❑ Annual business continuity & disaster recovery testing

Signature: _____

Name: _____

Date: _____