Cyber Hygiene - Organization Questionnaire

Do you enforce multi-factor authentication (MFA) for all critical systems (e.g., email, financial systems, customer databases)? *

- (●) No
- ( ) Only for administrators (1)
- ( ) For some employees (2)
- ( ) For most employees (3)
- ( ) Mandatory for all employees (4)

How often are user access privileges reviewed? *

- ( ) Never (0)
- (●) Annually (1)
- ( ) Semi-annually (2)
- ( ) Quarterly (3)
- ( ) Monthly or continuously monitored (4)

Are strong password policies enforced (length, complexity, expiration, reuse restrictions)? *

- (●) No (0)
- ( ) Basic enforcement, but not monitored (1)
- ( ) Enforced for administrators only (2)
- ( ) Enforced for most employees (3)
- ( ) Strictly enforced for all employees (4)

Are inactive or terminated employee accounts deactivated immediately? *

- ( ) No formal process (0)
- (●) Deactivated within a month (1)
- ( ) Deactivated within a week (2)
- ( ) Deactivated within 48 hours (3)
- ( ) Deactivated immediately upon termination (4)

Do employees have access only to the data and systems required for their job roles (least privilege principle)? *

- ○ No restrictions (0)
- ◉ Limited restrictions (1)
- ○ Some departments follow least privilege (2)
- ○ Most departments follow least privilege (3)
- ○ Strict least privilege policy enforced across the organization (4)

Does your organization provide and require the use of password managers? *

- ◉ No (0)
- ○ Available but not required (1)
- ○ Required for administrators (2)
- ○ Required for most employees (3)
- ○ Required for all employees (4)

Does your organization have a centralized system for managing software updates? *

- (●) No (0)
- ( ) Updates are done manually by users (1)
- ( ) IT manages updates but not automatically (2)
- ( ) Centralized automatic updates for some systems (3)
- ( ) Fully automated patch management (4)

Do you perform regular vulnerability scans? *

- (●) No (0)
- ( ) Annually (1)
- ( ) Semi-annually (2)
- ( ) Quarterly (3)
- ( ) Monthly or continuously monitored (4)

Are antivirus and endpoint protection solutions installed and updated? *

- ( ) No protection in place (0)
- ( ) Installed but not updated regularly (1)
- (●) Installed and updated semi-regularly (2)
- ( ) Installed and updated regularly (3)
- ( ) Installed, updated, and centrally monitored (4)

How often are operating systems, software, and applications updated? *

- ○ Never or rarely (0)
- ○ Only critical updates applied manually (1)
- ○ Updates applied within 3 months of release (2)
- ○ Updates applied within 1 month of release (3)
- ◉ Automated patching system in place (4)

Does your organization have a formal data classification policy (e.g., "Do you inventory and restrict access to sensitive data?")? *

- ◉ No classification policy (0)
- ○ Basic classification exists (1)
- ○ Classified data has access restrictions (2)
- ○ Classified data is encrypted (3)
- ○ Data is encrypted and regularly audited (4)

Are sensitive files and communications encrypted at rest and in transit? *

- (●) No encryption (0)
- ( ) Basic encryption but not enforced (1)
- ( ) Encryption applied to some systems (2)
- ( ) Encryption applied to most systems (3)
- ( ) Full encryption for all sensitive data (4)

Do you have a data backup and recovery process? *

- ( ) No backup system in place (0)
- ( ) Backups exist but are not performed regularly (1)
- (●) Backups are performed regularly but not tested for recovery (2)
- ( ) Backups are performed regularly and tested occasionally (3)
- ( ) Backups are performed regularly, encrypted, stored securely, and tested frequently (4)

How frequently are data backups performed? *

- ( ) No backup system in place (0)
- ( ) Monthly (1)
- ( ) Weekly (2)
- (●) Daily (3)
- ( ) Continuous real-time backups (4)

Are backups stored securely in an offsite or cloud location? *

- ○ No backups (0)
- ○ Backups stored on-premises only (1)
- ◉ Offsite backups stored but not encrypted (2)
- ○ Offsite backups stored with encryption (3)
- ○ Encrypted offsite backups with multi-location redundancy (4)

Are backups regularly tested for successful restoration? *

- ◉ Never (0)
- ○ Annually (1)
- ○ Semi-annually (2)
- ○ Quarterly (3)
- ○ Monthly or more frequently (4)

How often do employees receive cybersecurity awareness training? *

- ◉ Never (0)
- ○ Once during onboarding (1)
- ○ Annually (2)
- ○ Semi-annually (3)
- ○ Regular ongoing training with simulations (4)

Are simulated phishing attacks conducted to test employee awareness? *

- (●) No (0)
- ( ) Once per year (1)
- ( ) Semi-annually (2)
- ( ) Quarterly (3)
- ( ) Monthly with detailed reporting (4)

Do employees receive role-specific cybersecurity training? *

- (●) No (0)
- ( ) Basic training for all (1)
- ( ) Role-specific training for some (2)
- ( ) Role-specific training for most (3)
- ( ) Continuous training tailored to roles (4)

Do employees know how to report security incidents and suspicious activity? *

- (●) No awareness (0)
- ( ) Some employees know (1)
- ( ) A formal reporting system exists but is not well known (2)
- ( ) A formal system exists and most employees are aware (3)
- ( ) A well-established system exists with clear reporting procedures (4)

Do employees understand and actively participate in cybersecurity practices (e.g., reporting suspicious activity, following policies)? *

- (●) No expectations or policies in place (0)
- ( ) Basic policies exist, but no training provided (1)
- ( ) Employees receive occasional awareness training (2)
- ( ) Employees actively report threats and follow security procedures (3)
- ( ) A strong cybersecurity culture is embedded across the organization (4)

Does your organization enforce secure Wi-Fi policies (e.g., WPA3, no default credentials, guest network separation)? *

- (●) No (0)
- ( ) Basic security, default passwords exist (1)
- ( ) Secure settings, but not reviewed (2)
- ( ) Regular security reviews (3)
- ( ) Enforced policies with monitoring (4)

Are all devices protected with endpoint security solutions (e.g., EDR, antivirus, firewalls)? *

- ○ No protection (0)
- ◉ Basic antivirus only (1)
- ○ Antivirus & basic firewall (2)
- ○ Advanced endpoint detection and response (EDR) (3)
- ○ Fully managed EDR with advanced threat detection tools (4)

How is remote access to company systems secured? *

- ◉ No security measures (0)
- ○ Basic VPN access (1)
- ○ VPN with MFA (2)
- ○ Strict access controls partially implemented (3)
- ○ Full Zero Trust Model with strict controls (4)

Does your organization have a documented incident response plan? *

- ◉ No (0)
- ○ Exists but never tested (1)
- ○ Tested once a year (2)
- ○ Tested semi-annually (3)
- ○ Regularly tested with live drills (4)

Do you have a cybersecurity expert or service provider to help during emergencies (e.g., ransomware, data breaches)? *

- (●) No (0)
- ( ) Evaluating options (1)
- ( ) External partner but no SLA (2)
- ( ) Partner on retainer (3)
- ( ) 24/7 emergency support (4)

Are security incidents logged and analyzed for patterns? *

- (●) No logging system (0)
- ( ) Some manual logging (1)
- ( ) Automated logging but no analysis (2)
- ( ) Automated logging with periodic analysis (3)
- ( ) Advanced logging with continuous monitoring and AI-driven analysis (4)

Is there a cyber insurance policy to mitigate financial losses from cyber incidents? *

- (●) No (0)
- ( ) Evaluating options (1)
- ( ) Basic coverage (2)
- ( ) Moderate coverage with defined incident response support (3)
- ( ) Comprehensive cyber insurance with crisis management (4)

How quickly are cybersecurity incidents required to be reported internally?

- (●) No formal reporting process (0)
- ( ) Within a week (1)
- ( ) Within 72 hours (2)
- ( ) Within 24 hours (3)
- ( ) Immediately (4)

Does your organization follow industry-specific cybersecurity regulations or standards (e.g., ISO 27001, E-ITS, NIS2)?

- (●) No compliance efforts (0)
- ( ) Aware of requirements but not implemented (1)
- ( ) Partially compliant (2)
- ( ) Mostly compliant (3)
- ( ) Fully compliant with audits (4)

Are third-party vendors required to meet cybersecurity standards?

- (●) No security requirements for vendors (0)
- ( ) Basic security requirements but not enforced (1)
- ( ) Some vendors required to meet security standards (2)
- ( ) Most vendors required to meet security standards (3)
- ( ) All vendors required to meet strict security standards with audits (4)

Are devices (laptops, servers, etc.) physically secured against unauthorized access? *

- ○ No physical security measures (0)
- ◉ Basic measures (e.g., office locks) (1)
- ○ Sensitive devices secured (2)
- ○ Most devices secured (3)
- ○ All devices secured and monitored (4)

Do you assess vendors/partners for cybersecurity practices before sharing data or system access? *

- ◉ No vendor assessments (0)
- ○ Informal verbal assurances (1)
- ○ Basic checklist for critical vendors (2)
- ○ Formal assessments for all vendors (3)
- ○ Continuous monitoring of vendor security (4)

Are employees required to use VPNs or secure networks when accessing company data remotely? *

- (●) No requirements (0)
- ( ) Recommended but not enforced (1)
- ( ) Enforced for administrators (2)
- ( ) Enforced for most employees (3)
- ( ) Mandatory for all remote access (4)