MODERN TOOLING SOLUTION

Information Security Risk Assessment

1. Purpose

This document provides an assessment of potential risks to information security within the organization and outlines control measures to mitigate them. It is prepared in alignment with ISO 27001, IATF 16949 requirements, and industry best practices.

---

2. Scope

This assessment covers:

- IT systems (servers, networks, applications)
- End-user devices (laptops, desktops, mobile phones)
- Data (confidential, customer, financial, and employee information)
- Third-party vendors and cloud services

---

3. Methodology

- **Identify** threats and vulnerabilities
- **Assess** likelihood and impact
- **Evaluate** risk level (High/Medium/Low)
- **Recommend** preventive and corrective controls

---

4. Risk Assessment Table

Threat / Risk	Vulnerability	Likelihood	Impact	Risk Level	Controls / Mitigation
Unauthorized access to systems	Weak passwords, lack of MFA	Medium	High	High	Enforce MFA, strong password policy, regular access reviews
Data loss due to hardware failure	No proper backups	Low	High	Medium	Automated daily backups, off-site/cloud backup storage
Phishing & social engineering attacks	Lack of employee awareness	High	High	High	Security awareness training, phishing simulations
Malware/Ransomware attacks	Outdated antivirus, unpatched software	Medium	High	High	Regular patching, endpoint protection, email filtering
Data leakage via removable media	Unrestricted USB access	Medium	Medium	Medium	Disable unauthorized USB use, data encryption
Insider threats	Excessive access rights	Low	High	Medium	Least privilege principle, monitoring, access logs
Vendor/third-party breaches	Lack of vendor security assessment	Medium	High	High	Vendor risk assessment, security clauses in contracts
Network intrusion	Weak firewalls, no intrusion detection	Low	High	Medium	Firewalls, IDS/IPS, 24/7 monitoring
Loss of confidentiality of customer data	Inadequate data encryption	Medium	High	High	Data encryption in transit & at rest, role-based access
Non-compliance with regulations	Lack of documented policies/procedures	Low	High	Medium	Regular compliance audits, policy updates

5. Residual Risk

After implementation of mitigation controls, residual risks should be re-assessed. Risks remaining above acceptable levels must be escalated to management for decision-making.

---

6. Monitoring & Review

- Risk assessments shall be reviewed **annually** or after major changes (new systems, threats, or incidents).
- Incident logs, audits, and monitoring tools will provide continuous feedback.

Prepared by: Chief Information Security Officer (CISO)

Reviewed by: Legal and Compliance Head

Approved by: Managing Director / CEO