Cyber Security Best Practices PDF Checklist

Cyber Security Best Practices PDF Checklist
(Preview of Key Sections)

1. Employee Training & Awareness

✅ Conduct quarterly AI-phishing simulations using tools like KnowBe4 or Cofense.

✅ Host GDPR 2.0 compliance workshops for EU data handling.

✅ Distribute this PDF guide to all employees and contractors.

2. Zero-Trust Architecture Implementation

✅ Enable multi-factor authentication (MFA) for all systems (Microsoft Authenticator, Duo).

✅ Segment networks to isolate sensitive data (e.g., finance, R&D).

✅ Deploy Zscaler Zero Trust Exchange or Cloudflare Access for secure remote access.

3. Data Encryption & Backup

🔐 Migrate to quantum-safe encryption (CRYSTALS-Kyber/NTRU) for sensitive files.

🔐 Automate daily backups to immutable storage (AWS S3 Glacier, Backblaze).

🔐 Use VeraCrypt 2025 for encrypting local drives and containers.

4. Threat Detection & Response

🛡 Install AI-powered tools like Darktrace PREVENT or CrowdStrike Falcon.

🛡 Create an incident response plan with roles, escalation paths, and 24/7 monitoring.

🛡 Test recovery protocols semi-annually using ransomware attack simulations.

5. Compliance & Reporting

📜 Document all access requests and permissions (GDPR 2.0 Article 17).

📜 Use NIST 2025 templates for risk assessments and audit trails.

📜 Submit breach reports within 72 hours with forensic evidence.

6. Physical & IoT Security

🔒 Block unauthorized USB devices via endpoint management (Microsoft Intune).

🔒 Update firmware on IoT devices (cameras, smart sensors) monthly.

🔒 Restrict server room access with biometric scanners (Kisi, HID Global).