Bring Your Own Device (BYOD) Policy

1. Purpose / Objective

The purpose of this policy is to define security requirements for employees and contractors who use personal devices (laptops, tablets, smartphones) to access company systems, data, or networks. The goal is to protect the confidentiality, integrity, and availability of company information while enabling flexibility in work practices.

---

2. Scope

This policy applies to:

- All employees, contractors, interns, and third parties who use personal devices for company work.
- All types of personal devices including laptops, tablets, and smartphones.
- All systems and services accessed via personal devices (email, internal applications, cloud storage, etc.).

---

3. Policy Statement

- Only devices that meet company security standards (e.g., updated OS, antivirus, disk encryption) may connect to company resources.
- Multi-Factor Authentication (MFA) must be enabled for all BYOD access.
- Company-approved security software (such as VPN and endpoint protection) must be installed before access is granted.
- Personal devices must not store sensitive company data locally unless explicitly approved.
- Lost or stolen devices must be reported immediately to the IT Security Department.
- The company reserves the right to remotely wipe company data from any BYOD device if it is compromised.
- Employees are prohibited from jailbreaking, rooting, or otherwise disabling security features on BYOD devices used for work.

---

4. Roles & Responsibilities

- **Employees / Users**: Ensure their devices comply with BYOD requirements before accessing company resources.
- **IT Security Department**: Provide configuration guidelines, monitor access logs, and enforce compliance.
- **Line Managers**: Ensure team members are aware of and follow this policy.

---

5. Compliance & Enforcement

- Non-compliance with this policy may result in:
    - Removal of BYOD access rights.
    - Disciplinary action, up to and including termination of employment (for employees).
    - Termination of contract (for contractors/third parties).
- Legal action may be taken in case of deliberate policy violations resulting in security breaches.

---

6. References

- ISO/IEC 27001: Annex A.5.10 (Acceptable use of information and assets)
- ISO/IEC 27001: Annex A.5.23 (Information security for use of cloud services)
