# 8 Technological Controls


**34 Controls**

- Technological controls are security measures for IT systems.
- These controls are used to prevent unauthorized access.
- Examples include access controls and encryption.
- Monitoring and logging are also important controls.
- These controls help detect and prevent security incidents.
- Backup and recovery procedures are part of technological controls.
- Physical security measures also fall under technological controls.
- These controls are implemented to protect data confidentiality.
- They are also used to ensure data integrity and availability.
- Technological controls should be regularly reviewed and updated.

# Technological Controls (8.1-8.5)

**8.1 User Endpoint Devices**: Protect information from user endpoint device threats

**8.2 Privileged access rights**: Ensure authorized privileged access rights only granted

**8.3 Information Access Restriction**: To restrict access to authorized users only

**8.4 Access To Source Code**: Prevent unauthorized changes & maintain intellectual property confidentiality

**8.5 Secure Authentication:** Ensure secure access via authentication for systems, apps, services

# Technological Controls (8.6-8.10)


**8.6 Capacity Management**: Ensure sufficient resources for information processing and facilities

**8.7 Protection Against Malware**: Protect information and assets against malware

**8.8 Management of Technical Vulnerabilities**: To prevent exploitation of technical vulnerabilities

**8.9 Configuration Management**: To avoid sensitive data exposure and meet legal, regulatory, and contractual obligations

**8.10 Information deletion**: To ensure compliant information deletion and avoid exposure of sensitive data.

# Technological Controls (8.11-8.15)


**8.11 Data Masking**: Ensure compliance with regulations and protect sensitive data

**8.12 Data Leakage Prevention**:  Prevent unauthorized information disclosure/extraction by individuals or systems

**8.13 Information Backup**: To enable recovery from loss of data or systems.

**8.14 Redundancy of Information Processing Facilitie**s: Ensure the continuous operation of information processing facilities

**8.15 Logging**: To capture events, maintain log integrity, detect security events, prevent unauthorized access, support investigations.

# Technological Controls (8.16-8.20)


**8.16 Monitoring Activities**: To detect anomalous behaviour and information security incidents

**8.17 Clock Synchronization**: Support analysis of security events and investigations

**8.18 Use of Privileged Utility Programs**: Ensure safe use of utility programs for security

**8.19 Installation of Software on Operational Systems**: Ensure system integrity, prevent vulnerabilities

**8.20 Networks Security**: Protect network information from compromise

# Technological Controls (8.21-8.25)

**8.21 Security of Network Services**: To ensure security in the use of network services

**8.22 Segregation of Networks**: Segment network for controlled traffic based on business needs.

**8.23 Web Filtering**: Protect systems from malware and unauthorized web access.

**8.24 Use of Cryptography**: Protect information using cryptography that meets legal requirements.

**8.25 Secure Development Life Cycle**: Ensure secure development life cycle of software and systems.

# Technological Controls (8.26-8.30)

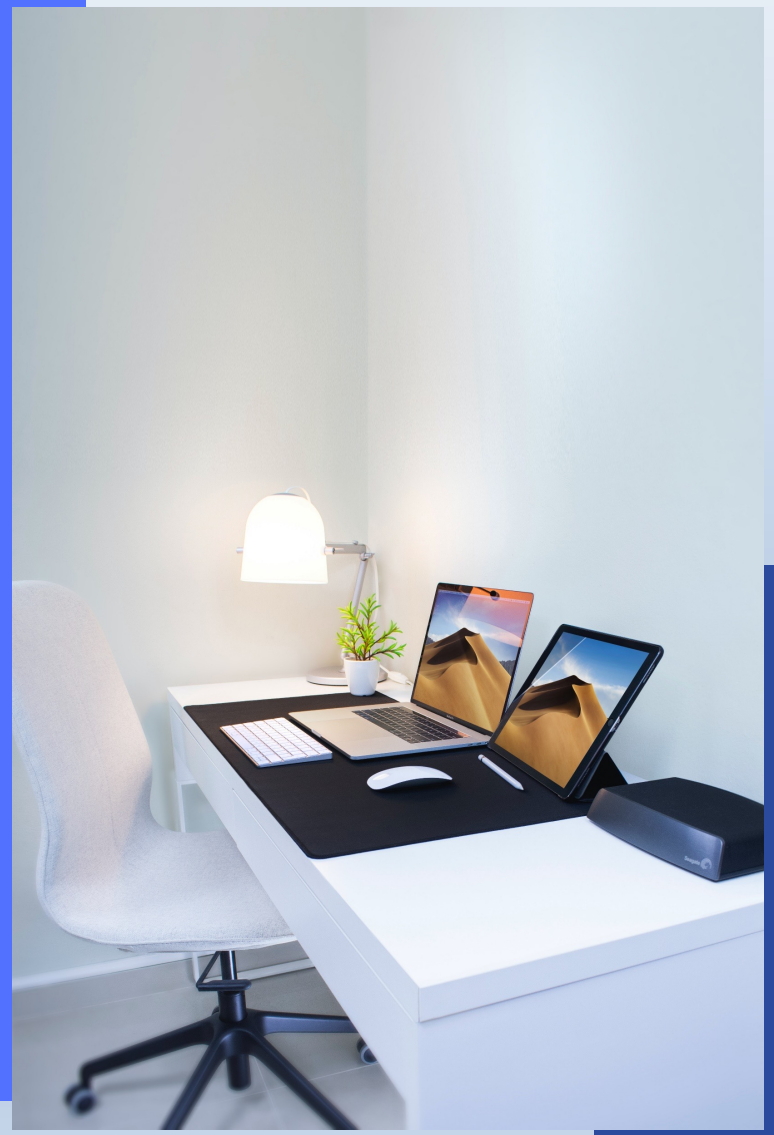
**8.26 Application Security Requirement**s:  Address all security requirements when developing or acquiring applications.

**8.27 Secure System Architecture and Engineering Principles**: Securely design, implement, and operate information systems in development life cycle

**8.28 Secure Coding**: Ensure secure software to reduce vulnerabilities.

**8.29 Security Testing in Development and Acceptance**: Validate security requirements during code deployment

**8.30 Outsourced Development**: Ensure infosec measures in outsourced development



# Technological Controls (8.31-8.34)

**8.31 Separation of Development, Test and Production Environments**: Protect production and data from dev/test compromise

**8.32 Change Management:** To preserve information security when executing changes

**8.33 Test Information**: Ensure relevant testing & protect operational information used for testing

**8.34 Protection of Information Systems During Audit Testing**: Prevent unauthorized access and damage to assets.