Security Policy for Telecom Operator

1. Purpose

To establish a framework to protect the information assets, systems, and networks of Telecom Operator. It ensures secure operations, safeguards customer data, and maintains regulatory compliance with standards like GDPR and NIS2.

2. Scope

This policy applies to:

- All employees, contractors, vendors, and consultants.
- All IT systems, including servers, user workstations, network equipment, and telecom infrastructure.
- All data generated, processed, or stored by the company.

3. User Policies

3.1 Acceptable Use

- Users must not install unauthorized software or hardware.
- Internet and email usage must align with business purposes.

3.2 Password Management

- Users must create strong passwords (minimum 12 characters, mixed types).
- Passwords must be changed every 90 days.
- Passwords must never be shared or written on visible surfaces.

3.3 Email and Attachments

- Suspicious attachments must not be opened.
- Users should report any phishing attempts immediately.

4. System Administration Policies

4.1 Employee Lifecycle

- **Onboarding**: Grant access based on role (least privilege).
- **Termination**: Revoke access immediately and archive data securely.

4.2 Change Management

- All system changes must be documented via an RFC (Request for Change).
- A Change Advisory Board (CAB) must evaluate and approve high-impact changes.

4.3 Access Control

- Access is based on job roles and reviewed quarterly.
- Critical system logs must be audited regularly.

5. Firewall and Network Security

5.1 Firewall Requirements

- All traffic to/from the internet must pass through approved firewalls.
- Firewalls must be hardened and configured to:
    - Block unauthorized ports.
    - Enforce rules based on IP, port, protocol, user identity, and time.
    - Log all security-related events.

5.2 Network Topologies

- Use **DMZ zones** for publicly accessible services.
- Apply **host-based firewalls** on critical servers.
- **Stateful firewalls** must track connection states for better filtering.
- **Application-level gateways** should inspect application traffic where applicable.

5.3 Wireless Access

- Guest wireless access is segregated from the internal network.
- All Wi-Fi networks must be encrypted (WPA3 preferred) and monitored.

6. Incident Response Policy

- Maintain an Incident Response Plan (IRP) with the following steps:
    1. Identification
    2. Containment
    3. Eradication
    4. Recovery
    5. Post-incident review
- Report breaches within 72 hours (per GDPR requirements).
- Maintain a centralized SOC (Security Operations Center) or equivalent.

7. Data Classification and Handling

Classification	Examples	Protection Requirements
Public	Marketing materials	Basic integrity safeguards

Classification	Examples	Protection Requirements
Secure	Customer data, billing records	Encryption, strict access control
Sensitive	Employee records, IP, strategies	Encryption, monitoring, auditing

8. Disaster Recovery and Fault Tolerance

- Implement a **Disaster Recovery Plan (DRP)** and **Business Continuity Plan (BCP)**.
- Daily backups must be performed (full, incremental, or differential as needed).
- Use **RAID** for storage redundancy and performance.

9. Software Development and Security

- Developers must follow secure coding standards.
- All software must be tested for vulnerabilities before deployment.
- Access to source code is restricted based on need.

10. Compliance with Laws and Regulations

- Comply with **GDPR** and other applicable data protection laws.
- Personal data must only be processed with legal consent or contract basis.
- The **Data Protection Officer (DPO)** is responsible for GDPR compliance.
- Compliance with **HIPAA** applies if handling health-related data.

11. Logging and Auditing

- All critical systems must generate logs (access, changes, authentication).
- Logs must be retained securely for at least 12 months.
- Use automated tools to alert for suspicious behaviour.

12. Training and Awareness

- Security awareness training is mandatory and conducted annually.
- Special training is given for system admins, developers, and network engineers.
- Regular phishing simulation and policy updates will be enforced.

13. Policy Enforcement

- Non-compliance will result in disciplinary action, up to and including termination.
- The CISO is authorized to isolate systems during active threats.

14. Review and Updates

- This policy is reviewed **annually** or after major incidents.
- All revisions must be approved by senior management and distributed company wide.