Specific Policy on Organizational Controls

1. Objective

To establish the necessary organizational controls to protect the information and technological assets of the telecommunications company, ensuring their confidentiality, integrity, and availability, while complying with applicable legal, regulatory, and contractual requirements.

2. Scope

This policy applies to all employees, contractors, suppliers, and third parties who access, process, or manage the organization's information.

3. General Principles

- **Information Security Governance:** A clear governance structure will be established, with defined roles and responsibilities for managing information security.
- **Top Management Commitment:** Senior management will demonstrate leadership and commitment by allocating resources, approving policies, and overseeing compliance.
- **Risk Management:** A continuous process will be implemented for identifying, assessing, and treating information security risks.

4. Organizational Controls

4.1. Roles and Responsibilities

- An Information Security Officer (CISO) will be appointed with the authority to implement and oversee the ISMS.
- Each functional area must appoint a Local Security Officer to coordinate specific actions.

4.2. Awareness and Training

- All employees will receive mandatory information security training upon onboarding and periodically thereafter.
- Awareness campaigns will be conducted to reinforce best practices.

4.3. Supplier Management

- Suppliers' security will be assessed prior to contracting.
- Contracts will include specific clauses on information security and regulatory compliance.

4.4. Incident Management

- A formal process will be established for reporting, analyzing, and responding to security incidents.
- An up-to-date log of all incidents and corrective actions will be maintained.

4.5. Legal and Regulatory Compliance

- Compliance with regulations such as the Federal Law on Protection of Personal Data, IFT standards, and other applicable laws will be ensured.
- Periodic internal audits will be conducted to verify compliance.

4.6. Security in Projects and Changes

- All technology projects must include a security impact assessment.
- Changes to critical systems will require review and approval by the security team.

5. Review and Update

- This policy will be reviewed at least once a year or whenever significant changes occur in the technological, regulatory, or business environment.

6. Sanctions

- Non-compliance with this policy may result in disciplinary measures, including termination of employment or commercial contracts, depending on the severity of the case.

Specific Policy on Personnel Management Controls

1. Objective

To establish the necessary controls to securely manage personnel before, during, and after their employment relationship with the company, in order to protect information assets and reduce risks associated with the human factor.

2. Scope

This policy applies to all employees, contractors, consultants, suppliers, and third parties who have access to the organization's systems, networks, or information.

3. General Principles

- Information security is a shared responsibility among all personnel.
- Specific controls will be established at each stage of the employee lifecycle.
- A culture of security will be promoted through training, awareness, and continuous supervision.

4. Controls by Stage of the Personnel Lifecycle

4.1. Pre-Employment

- **Background Checks:** Employment, academic, and, where applicable, criminal background checks will be conducted in accordance with current legislation.
- **Contractual Clauses:** All contracts will include confidentiality clauses, acceptable use of information, and compliance with security policies.

4.2. During Employment

- **Security Training:** All personnel must complete initial and ongoing information security training programs.
- **Role-Based Access**: Access to systems and information will be granted based on the principle of least privilege and need-to-know.
- **Monitoring and Compliance:** Periodic audits and reviews will be conducted to ensure compliance with security policies.

4.3. Termination or Role Change

- **Access Revocation:** All physical and logical access will be immediately revoked upon termination or role change.
- **Return of Assets:** Personnel must return all company assets (devices, credentials, documents, etc.).
- **Reminder of Obligations:** Employees will be reminded of their post-employment obligations, especially regarding confidentiality.

5. Responsibilities

- **Human Resources:** Will coordinate onboarding, training, and offboarding processes.
- **Information Security:** Will define technical controls and conduct compliance audits.
- **Area Leaders:** Will oversee compliance with this policy within their respective teams.

6. Review and Update

This policy will be reviewed annually or when significant changes occur in legislation, organizational structure, or technology used.

7. Sanctions

Non-compliance with this policy may result in disciplinary actions, including termination of employment or commercial contracts, in accordance with internal and applicable legal regulations.

Specific Policy on Asset Management Controls

1. Objective

To establish the guidelines and necessary controls to properly identify, classify, protect, and manage the organization’s information assets throughout their entire lifecycle.

2. Scope

This policy applies to all information assets, including hardware, software, data, documentation, services, and human resources, that are owned by the company or under its custody.

3. General Principles

- All assets must be inventoried, classified, and managed according to their value, criticality, and sensitivity.
- The protection of assets is the responsibility of all users who utilize or manage them.
- Traceability and control of assets must be ensured during acquisition, use, maintenance, and final disposal.

4. Asset Management Controls

4.1. Asset Inventory

- An up-to-date inventory of all assets relevant to information security will be maintained.
- Each asset must have a clearly assigned owner responsible for its protection and proper use.

4.2. Asset Classification

- Assets will be classified according to their sensitivity level: Public, Internal, Confidential, and Restricted.
- The classification will determine access, storage, transmission, and disposal controls.

4.3. Acceptable Use of Assets

- Clear guidelines will be established regarding the acceptable use of devices, systems, and networks.
- Misuse of assets may be subject to sanctions in accordance with internal policies.

4.4. Asset Protection

- Physical and logical controls will be applied to protect assets against unauthorized access, loss, damage, or theft.
- Critical assets must have backup, redundancy, and monitoring measures in place.

4.5. Transfer and Mobility

- The transfer of assets (physical or digital) must be carried out through secure and authorized mechanisms.
- Mobile and portable devices must have encryption and strong authentication.

4.6. Disposal and Final Decommissioning

- Assets that are no longer needed must be securely disposed of, ensuring the destruction of sensitive information.
- The decommissioning and destruction process will be documented.

5. Responsibilities

- **IT Department:** Maintain the inventory of technological assets and apply technical controls.
- **End Users:** Use assets in accordance with policies and report any anomalies.
- **Information Security:** Oversee classification, protection, and compliance with this policy.

6. Review and Update

This policy will be reviewed annually or when new types of assets, technologies, or relevant threats are introduced.

7. Sanctions

Non-compliance with this policy may result in disciplinary actions, including termination of employment or commercial contracts, in accordance with internal and applicable legal regulations.

Specific Policy on Access Management Controls

1. Objective

Establish the necessary guidelines and controls to securely manage access to the organization's systems, networks, applications, and data, ensuring that only authorized individuals have access to the appropriate information, at the right time, and for the right reasons.

2. Scope

This policy applies to all employees, contractors, vendors, and third parties who require access to the company's information resources, whether locally or remotely.

3. General Principles

- Access to information assets must be based on the principle of least privilege and need-to-know.
- All access must be authenticated, authorized, logged, and monitored.
- Differentiated controls must be applied according to the sensitivity level of the information or system.

4. Access Management Controls

4.1. Identity Management

- Each user will have a unique identity to access the systems.
- Shared accounts will not be allowed, except in exceptional and controlled cases.

4.2. Authentication

- Multi-factor authentication (MFA) will be implemented for access to critical or remote systems.
- Passwords must meet minimum complexity requirements and be changed periodically.

4.3. Access Assignment and Review

- Access will be granted upon formal authorization from the area manager.
- Periodic access reviews will be conducted to detect unnecessary or inappropriate privileges.

4.4. Network and System Access Control

- Access control lists (ACLs), firewalls, and network segmentation will be applied to limit access to resources.
- Administrative access will be restricted and subject to enhanced monitoring.

4.5. Third-Party Access

- Third-party access must be justified, authorized, and limited in time and scope.
- Secure connections (VPN, encrypted tunnels) will be used, and all activities will be logged.

4.6. Access Deactivation

- Access will be immediately revoked upon termination of the employment or contractual relationship.
- A record of access creation, modification, and removal will be maintained.

5. Responsibilities

- **IT Department:** Manage access control platforms and execute authorized requests.
- **Area Managers:** Validate and approve access required by their staff.
- **Users:** Use their credentials securely and report any anomalies.

6. Review and Update

This policy will be reviewed annually or when new systems, technologies, or relevant threats are introduced.

7. Sanctions

Failure to comply with this policy may result in disciplinary actions, including termination of employment or commercial contracts, in accordance with applicable internal and legal regulations.

Specific Policy on Physical Controls

1. Objective

To establish the necessary physical controls to protect the organization's facilities, equipment, and information assets against unauthorized access, damage, theft, or interference.

2. Scope

This policy applies to all physical facilities of the company, including offices, data centers, technical rooms, warehouses, and any other location where information assets are located.

3. General Principles

- Physical access to facilities must be controlled, monitored, and restricted according to the criticality level of the area.
- Preventive and detection measures must be implemented to minimize physical risks.
- All personnel must be aware of and comply with established physical security rules.

4. Specific Physical Controls

4.1. Security Zoning

- Facilities will be divided into zones with different security levels: public, restricted, and critical.
- Access to critical zones (such as data centers) will be limited to authorized and registered personnel.

4.2. Physical Access Control

- Physical authentication mechanisms such as proximity cards, biometrics, or access codes will be used.
- Entry and exit logs will be maintained, especially in sensitive areas.

4.3. Equipment Protection

- Critical equipment must be located in secure areas, protected against fire, humidity, extreme temperatures, and sabotage.
- Direct physical access to servers, switches, routers, and other network devices will be restricted.

4.4. Supervision and Monitoring

- CCTV surveillance systems will be installed at strategic points, with secure storage of recordings.
- Security patrols and periodic physical audits will be conducted.

4.5. Visitors and Third Parties

- All visits must be registered, identified, and accompanied by authorized personnel.
- Visitors may not access critical zones without prior authorization and direct supervision.

4.6. Disaster Protection

- Facilities must have fire detection and suppression systems, as well as evacuation and business continuity plans.
- Emergency drills will be conducted periodically.

4.7. Secure Equipment Disposal

Equipment containing sensitive information must be securely disposed of or recycled, ensuring data destruction.

5. Responsibilities

- **Physical Security or Infrastructure Department:** Implement and maintain physical controls.
- **Information Security:** Coordinate with infrastructure to ensure the protection of critical assets.
- **All Personnel**: Comply with access rules and report any anomalies.

6. Review and Update

This policy will be reviewed annually or when significant changes occur in facilities or the threat environment.

7. Sanctions

Non-compliance with this policy may result in disciplinary actions, including termination of employment or commercial contracts, in accordance with internal and applicable legal regulations.

Specific Policy on Controls for Operational Security

1. Objective

Establish the necessary controls to ensure the safe, reliable, and efficient operation of information systems, minimizing the risk of interruptions, errors, unauthorized access, and data loss.

2. Scope

This policy applies to all operational processes related to the management of systems, networks, applications, databases, and technological services of the organization.

3. General Principles

- System operations must be documented, controlled, and monitored.
- Preventive, detective, and corrective controls must be applied to ensure the continuity and security of operations.
- Any change in the operational environment must be managed in a controlled manner.

4. Operational Security Controls

4.1. Change Management

- Any change in systems, applications, or infrastructure must be evaluated, approved, tested, and documented before implementation.
- A change log will be maintained, including justification, impact, and responsible parties.

4.2. Capacity Management

- The use of technological resources will be monitored to anticipate capacity needs and avoid interruptions.
- Trend analysis and growth planning will be conducted.

4.3. Malware Protection

- Malware protection solutions will be implemented on all devices and servers.
- Signatures will be regularly updated, and automatic scans will be performed.

4.4. Backups

- Periodic backups of critical information will be performed, with regular restoration tests.
- Backups will be protected against unauthorized access and stored in secure locations.

4.5. Monitoring and Logging

- Logging of relevant events (logs) will be enabled on critical systems.
- Monitoring tools will be implemented to detect anomalies, unauthorized access, or operational failures.

4.6. Environment Segregation

- Development, testing, and production environments will be kept separate to avoid interference and security risks.
- Access between environments will be controlled and justified.

4.7. Vulnerability Management

- Periodic vulnerability scans will be conducted, and security patches will be applied according to a defined schedule.
- Critical vulnerabilities must be addressed immediately.

5. Responsibilities

- **IT Operations Area:** Execute and maintain the defined operational controls.
- **Information Security:** Oversee the correct implementation of controls and conduct audits.
- **Technical Users:** Comply with established procedures and report any deviations.

6. Review and Update

This policy will be reviewed annually or when new technologies, processes, or relevant threats are introduced.

7. Sanctions

Non-compliance with this policy may result in disciplinary actions, including termination of employment or commercial contracts, in accordance with applicable internal and legal regulations.

Specific Policy on Telecommunications Controls

1. Objective

Establish the necessary controls to protect the organization's telecommunications infrastructure, ensuring the confidentiality, integrity, and availability of information transmitted through internal and external networks.

2. Scope

This policy applies to all telecommunications networks used by the company, including LAN, WAN, VPN, wireless links, mobile networks, satellite links, and any other data transmission medium.

3. General Principles

- Telecommunications must be protected against unauthorized access, interception, alteration, and service loss.
- Technical and administrative controls must be implemented to ensure the secure transmission of information.
- Any connection to external networks must be properly authorized, controlled, and monitored.

4. Telecommunications Controls

4.1. Network Infrastructure Security

- Firewalls, intrusion detection and prevention systems (IDS/IPS), and network segmentation will be used to protect perimeters.
- Critical networks will be logically separated using VLANs or physically when necessary.

4.2. Communication Encryption

- All transmission of sensitive information must be carried out using secure protocols (e.g., TLS, IPsec, SSH, VPN).
- Valid and up-to-date digital certificates will be used to ensure the authenticity of connections.

4.3. Remote Connection Management

- Remote access to the corporate network must be conducted exclusively through secure VPNs and multi-factor authentication.
- All remote sessions will be logged and monitored.

4.4. Network Supervision and Monitoring

- Traffic monitoring and behavior analysis tools will be implemented to detect anomalous activities.
- Network event logs will be maintained for auditing and incident response.

4.5. Protection Against Interference and Sabotage

- Telecommunications facilities must be physically protected against unauthorized access and adverse environmental conditions.
- Redundancy and fault tolerance controls will be applied to critical links.

4.6. Telecommunications Provider Management

- Network service providers must comply with the security requirements established by the organization.
- The performance and compliance with service level agreements (SLAs) will be periodically evaluated.

5. Responsibilities

- **Networks and Telecommunications Area:** Implement and maintain the defined technical controls.
- **Information Security**: Oversee compliance with this policy and coordinate audits.
- **Users:** Use network services in accordance with policies and report any anomalies.

6. Review and Update

This policy will be reviewed annually or when new technologies, threats, or changes in network infrastructure are introduced.

7. Sanctions

Non-compliance with this policy may result in disciplinary actions, including termination of employment or commercial contracts, in accordance with applicable internal and legal regulations.

Specific Policy on Controls for the Acquisition, Development, and Maintenance of Information Systems

1. Objective

Establish the necessary controls to ensure that information systems acquired, developed, or modified by the organization meet security requirements from conception to retirement, minimizing risks and ensuring operational continuity.

2. Scope

This policy applies to all acquisition, internal development, maintenance, or enhancement projects of information systems, including software, applications, databases, and technological components used by the company.

3. General Principles

- Security must be integrated from the early stages of the system life cycle.
- Every system must comply with security, privacy, regulatory compliance, and business continuity requirements.
- Secure development practices and rigorous testing must be applied before production deployment.

4. Controls for Acquisition, Development, and Maintenance

4.1. Security Requirements

- Security requirements must be defined and documented from the system analysis phase.
- Aspects such as authentication, authorization, encryption, traceability, and personal data protection must be considered.

4.2. Supplier and Solution Evaluation

- Any externally acquired solution must be evaluated in terms of security, compliance, and compatibility.
- Contracts with suppliers must include clauses on security, auditing, and support.

4.3. Secure Development

- Secure development methodologies (such as DevSecOps) will be adopted, and technical staff will be trained in secure coding practices.
- Static and dynamic code analysis tools will be used to detect vulnerabilities.

4.4. Security Testing

- Before implementation, systems must undergo penetration testing, vulnerability analysis, and control validation.
- Results will be documented, and identified weaknesses will be corrected.

4.5. Change Management

- Any modification to existing systems must follow a formal change management process, including a security impact assessment.
- A version and change history will be maintained.

4.6. Data Protection in Development and Testing

- Real customer data must not be used in development or testing environments unless properly anonymized or encrypted.
- Access to these environments will be restricted and monitored.

4.7. Secure Maintenance

- Updates, patches, and improvements must be evaluated and applied in a controlled manner.
- Maintenance windows and backup procedures will be established before any intervention.

5. Responsibilities

- **Development and Technology Area:** Apply the defined controls at each phase of the system life cycle.
- **Information Security:** Validate security requirements, conduct audits, and perform compliance testing.
- **Functional Users:** Participate in requirements definition and acceptance testing.

6. Review and Update

This policy will be reviewed annually or when new technologies, methodologies, or relevant threats are introduced.

7. Sanctions

Non-compliance with this policy may result in disciplinary actions, including termination of employment or commercial contracts, in accordance with applicable internal and legal regulations.

Specific Policy on Controls for Supplier Management

1. Objective

Establish the necessary controls to securely and effectively manage the relationship with suppliers and third parties who have access to the organization's information assets, systems, or critical services, ensuring compliance with security, legal, and contractual requirements.

2. Scope

This policy applies to all suppliers, contractors, technology partners, and third parties who provide services, develop solutions, or have access to the company's information or infrastructure.

3. General Principles

- Information security must be considered from the selection of the supplier through to the end of the contract.
- Suppliers must comply with the security standards defined by the organization.
- Mechanisms for evaluation, monitoring, and continuous control of third-party risks must be established.

4. Controls for Supplier Management

4.1. Supplier Evaluation and Selection

- Before contracting, suppliers will be evaluated based on their technical capacity, regulatory compliance, and maturity in information security.
- Preference will be given to suppliers with recognized certifications (ISO 27001, SOC 2, etc.).

4.2. Contracts with Security Clauses

All contracts must include specific clauses regarding:

- Confidentiality and data protection
- Compliance with security policies
- Audit rights
- Security incident notification
- Legal and contractual responsibilities

4.3. Supplier Classification

- Suppliers will be classified according to the level of risk they represent to the organization (high, medium, low).
- This classification will determine the frequency and depth of security evaluations.

4.4. Continuous Monitoring and Review

- Periodic reviews of the performance and compliance of critical suppliers will be conducted.
- Audits, security reviews, and contractual compliance analyses may be applied.

4.5. Third-Party Access Management

- Supplier access to systems or information must be authorized, time- and scope-limited, and monitored.
- Upon termination of the contractual relationship, all access will be revoked and delivered assets recovered.

4.6. Incident Management with Suppliers

- Suppliers must immediately report any security incident that may affect the organization.
- Joint response and mitigation procedures will be established.

5. Responsibilities

- **Procurement or Contracting Area:** Coordinate the evaluation and formalization of contracts with suppliers.
- **Information Security:** Define security requirements, assess risks, and conduct audits.
- **User Areas:** Oversee compliance with agreements and report deviations.

6. Review and Update

This policy will be reviewed annually or when new types of services, suppliers, or relevant regulatory changes are introduced.

7. Sanctions

Non-compliance with this policy may result in contractual sanctions, service suspension, or termination of the business relationship, as established in the signed agreements.

Specific Policy on Controls for Information Security Incident Management

1. Objective

Establish the guidelines and necessary controls for the detection, reporting, analysis, response, documentation, and learning from information security incidents, in order to minimize their impact and prevent recurrence.

2. Scope

This policy applies to all employees, contractors, suppliers, and third parties who use, manage, or have access to the organization's information systems, networks, data, or technological services.

3. General Principles

- Every security incident must be reported immediately and managed according to established procedures.
- The organization must have a specialized team for incident management (CSIRT or equivalent).
- A culture of proactive and retaliation-free reporting must be promoted.

4. Controls for Incident Management

4.1. Incident Classification

- Incidents will be classified according to their nature, impact, and urgency (e.g., unauthorized access, malware, data leakage, denial of service, etc.).
- Severity levels will be established to prioritize response.

4.2. Detection and Reporting

- Automatic and manual mechanisms will be implemented for incident detection (SIEM, IDS/IPS, log monitoring).
- All personnel must report incidents through the designated channel (email, ticketing system, hotline).

4.3. Response and Containment

- The incident response team must act immediately to contain, mitigate, and eradicate the incident.
- All actions taken will be documented, and digital evidence will be preserved when necessary.

4.4. Analysis and Recovery

- A technical and forensic analysis of the incident will be conducted to determine its root cause.
- Affected services will be restored in a secure and controlled manner.

4.5. Communication and Escalation

- Internal and external communication protocols will be established, including notification to regulatory authorities if applicable.
- Critical incidents must be escalated to senior management and the Security Committee.

4.6. Lessons Learned and Continuous Improvement

- After each incident, a post-mortem review meeting will be held.
- Controls, procedures, and policies will be updated based on lessons learned.

5. Responsibilities

- **End Users:** Report any incident or suspicious behavior.
- **Information Security Team:** Coordinate incident management, analysis, response, and documentation.
- **Technical Areas:** Support containment, recovery, and control improvements.
- **Senior Management:** Make strategic decisions in high-impact incidents.

6. Review and Update

This policy will be reviewed annually or when significant incidents occur that require adjustments to the established controls.

7. Sanctions

Non-compliance with this policy, including failure to report incidents, may result in disciplinary actions in accordance with applicable internal and legal regulations.

Specific Policy on Controls for Business Continuity Management

1. Objective

Establish the necessary controls to ensure the continuity of the organization's critical operations in the face of disruptive events, minimizing the impact on services, reputation, and regulatory compliance.

2. Scope

This policy applies to all critical areas, processes, systems, and resources of the organization, including personnel, infrastructure, technology, suppliers, and essential services.

3. General Principles

- Business continuity is the responsibility of the entire organization, with leadership from senior management.
- Critical processes must be identified, and continuity and recovery plans must be established.
- Preparedness, response, and recovery must be tested and continuously improved.

4. Controls for Business Continuity Management

4.1. Business Impact Analysis (BIA)

- An impact analysis will be conducted to identify critical processes, dependencies, maximum tolerable downtime (RTO), and minimum acceptable levels of operation (RPO).
- The BIA will be reviewed periodically or upon significant changes.

4.2. Risk Assessment

- Threats that may affect business continuity (natural disasters, technological failures, cyberattacks, etc.) will be identified.
- Mitigation and contingency measures will be established.

4.3. Business Continuity Plans (BCP)

- Documented plans will be developed and maintained, including procedures for response, recovery, and restoration of operations.
- Plans must be available, up to date, and accessible to those responsible.

4.4. Disaster Recovery Plans (DRP)

- Specific plans will be established for IT system recovery, including backups, alternate sites, and technical procedures.
- Roles, responsibilities, and recovery times will be defined.

4.5. Testing and Exercises

- Periodic tests of continuity and recovery plans will be conducted, including drills and tabletop exercises.
- Results will be documented, and improvements will be applied based on lessons learned.

4.6. Training and Awareness

- Key personnel will be trained in their roles within the BCP and DRP.
- An organizational culture focused on operational resilience will be promoted.

4.7. Critical Supplier Management

- The ability of strategic suppliers to maintain continuity of their services will be evaluated.
- Contracts must include continuity and recovery clauses.

5. Responsibilities

- **Senior Management:** Approve and support the business continuity program.
- **Business Continuity Officer:** Coordinate the development, maintenance, and testing of plans.
- **Area Managers:** Identify critical processes and participate in plan implementation.
- **All Personnel:** Be familiar with basic procedures for responding to incidents and emergencies.

6. Review and Update

This policy will be reviewed annually or when significant changes occur in processes, organizational structure, or threat environment.

7. Sanctions

Non-compliance with this policy may result in disciplinary actions in accordance with applicable internal and legal regulations.

Specific Policy on Controls for Compliance Management

1. Objective

Establish the necessary controls to ensure that the organization complies with all legal, regulatory, contractual, and normative obligations related to information security, data protection, and business operations.

2. Scope

This policy applies to all areas, processes, employees, contractors, and third parties involved in activities that may be subject to compliance requirements within the context of the organization.

3. General Principles

- Compliance is a shared responsibility that must be integrated at all levels of the organization.
- All applicable obligations must be identified, documented, and monitored.
- Non-compliance can lead to significant legal, financial, and reputational risks.

4. Controls for Compliance Management

4.1. Identification of Requirements

- An up-to-date inventory of laws, regulations, standards, and contracts applicable to the organization will be maintained (e.g., Federal Law on the Protection of Personal Data, IFT regulations, ISO/IEC 27001).
- Responsible parties will be assigned for each type of obligation.

4.2. Compliance Assessment

- Periodic assessments will be conducted to verify compliance with identified requirements.
- Findings will be documented, and corrective action plans will be established.

4.3. Internal and External Audits

- Internal audits on information security and regulatory compliance will be conducted at least once a year.
- External audits by authorities or certifying bodies will be facilitated when applicable.

4.4. Non-Compliance Management

- Any detected non-compliance will be recorded, analyzed, and addressed through corrective and preventive actions.
- Competent authorities will be notified when required by applicable regulations.

4.5. Awareness and Training

- Personnel will receive regular training on compliance topics, including data protection, ethics, information security, and industry regulations.
- A culture of compliance will be promoted through internal campaigns.

4.6. Monitoring and Reporting

- Continuous monitoring mechanisms and periodic reports to senior management on the compliance status will be established.
- Key compliance indicators (KPIs) will be used to evaluate performance.

5. Responsibilities

- **Compliance or Legal Officer:** Coordinate the identification and tracking of legal and regulatory obligations.
- **Information Security:** Ensure compliance with technical standards and internal policies.
- **Area Managers:** Implement specific controls and collaborate in audits.
- **All Personnel:** Comply with policies and report any potential non-compliance.

6. Review and Update

This policy will be reviewed annually or when changes occur in the legal, regulatory, or contractual framework affecting the organization.

7. Sanctions

Non-compliance with this policy may result in disciplinary, contractual, or legal sanctions, in accordance with applicable internal and external regulations.