Ethio-Djibouti Railway Share Company (EDRSC)

Cybersecurity Policy

Document Title: Cybersecurity Policy

Organization: Ethio-Djibouti Railway Share Company (EDRSC)

Policy Owner: Chief Digital Officer (CDO) / Information Security Manager
Approved By: Chief Executive Officer (CEO)

Version: 1.0
Effective Date: [DD/MM/YYYY]
Review Date: Annual

Table of Contents

1. **Introduction**
   1.1 Purpose
   1.2 Scope
   1.3 Objectives
   1.4 Policy Statement
   1.5 Definitions and Acronyms
2. **Governance and Responsibilities**
   2.1 Board of Directors Responsibilities
   2.2 Executive Management Responsibilities
   2.3 Information Security Team Responsibilities
   2.4 Employee Responsibilities
   2.5 Third-Party Responsibilities
3. **Information Security Framework**
   3.1 Security Principles
   3.2 Risk-Based Approach
   3.3 Security Standards and Guidelines
4. **Asset Management**
   4.1 Information Asset Inventory
   4.2 Asset Ownership
   4.3 Asset Classification and Labeling
   4.4 Asset Handling and Protection
5. **Risk Management**
   5.1 Risk Assessment Process
   5.2 Risk Treatment and Mitigation
   5.3 Risk Monitoring and Reporting
6. **Access Control Policy**
   6.1 User Access Management
   6.2 Privileged Access Management
   6.3 Password and Authentication Requirements
   6.4 Multi-Factor Authentication (MFA)
   6.5 Remote Access Security
7. **Identity and Access Management (IAM)**
   7.1 User Provisioning and De-provisioning
   7.2 Role-Based Access Control (RBAC)
   7.3 Periodic Access Reviews
8. **Data Protection and Privacy**

8.1 Data Classification
8.2 Data Storage and Retention
8.3 Data Encryption
8.4 Data Loss Prevention (DLP)
8.5 Privacy Protection Requirements
9. **Network Security**
9.1 Network Architecture Standards
9.2 Firewall Management
9.3 Intrusion Detection and Prevention
9.4 Wireless Network Security
9.5 Secure Remote Connectivity
10. **Endpoint Security**
10.1 Device Security Requirements
10.2 Anti-Malware Protection
10.3 Patch and Vulnerability Management
10.4 Mobile Device Security
11. **Cloud Security**
11.1 Cloud Governance
11.2 Cloud Service Provider Requirements
11.3 Cloud Access Security Controls
11.4 Data Protection in Cloud Environments
12. **Application Security**
12.1 Secure Software Development Lifecycle (SSDLC)
12.2 Secure Coding Practices
12.3 Application Testing and Reviews
12.4 Change Management
13. **Security Monitoring and Logging**
13.1 Audit Logging Requirements
13.2 Security Monitoring
13.3 Security Information and Event Management (SIEM)
13.4 Log Retention
14. **Vulnerability Management**
14.1 Vulnerability Assessments
14.2 Penetration Testing
14.3 Remediation Requirements
15. **Incident Response Management**

15.1 Incident Identification
15.2 Incident Reporting
15.3 Incident Response Procedures
15.4 Incident Recovery
15.5 Lessons Learned
16. **Business Continuity and Disaster Recovery**
16.1 Business Continuity Planning
16.2 Disaster Recovery Planning
16.3 Backup Management
16.4 Recovery Testing
17. **Third-Party and Vendor Security**
17.1 Vendor Risk Assessment
17.2 Third-Party Access Controls
17.3 Contractual Security Requirements
17.4 Supply Chain Security
18. **Security Awareness and Training**
18.1 Employee Security Awareness
18.2 Specialized Security Training
18.3 Phishing Awareness Programs
19. **Compliance and Legal Requirements**
19.1 Regulatory Compliance
19.2 Internal Audits
19.3 External Audits
19.4 Records Management
20. **Acceptable Use Policy**
20.1 Use of Organizational Systems
20.2 Internet and Email Usage
20.3 Social Media Usage
21. **Physical and Environmental Security**
21.1 Physical Access Controls
21.2 Data Center Security
21.3 Equipment Protection
22. **Policy Compliance and Enforcement**
22.1 Monitoring Compliance
22.2 Policy Violations
22.3 Disciplinary Actions
23. **Policy Exception Management**

23.1 Exception Request Process
23.2 Approval and Review of Exceptions
24. **Policy Review and Maintenance**
24.1 Policy Review Schedule
24.2 Version Control
24.3 Continuous Improvement
25. **Appendices** Appendix A: Roles and Responsibilities Matrix
Appendix B: Incident Reporting Form
Appendix C: Asset Classification Matrix
Appendix D: Glossary of Terms
Appendix E: Reference Standards (ISO 27001, NIST CSF, CIS Controls)

1. Introduction

1.1 Purpose

The Ethio-Djibouti Railway S.C (EDRSC) Cybersecurity policy means The purpose of this Cybersecurity Policy is to establish the principles, requirements, and responsibilities for protecting the information assets, operational technology (OT) systems, information technology (IT) infrastructure, communication networks, and business operations of Ethio-Djibouti Railway Share Company (EDRSC) from cybersecurity threats and risks.

This policy aims to ensure the confidentiality, integrity, availability, safety, and resilience of EDRSC's critical information and railway operational systems by implementing appropriate governance, security controls, risk management processes, and compliance measures.

1.2 Scope

This policy applies to:

- All EDRSC employees, management, consultants, contractors, and temporary staff.
- All third-party vendors, suppliers, service providers, and partners who have access to EDRSC information assets or systems.
- All information assets owned, leased, managed, or operated by EDRSC.
- Information Technology (IT) infrastructure, including:
    - Servers
    - Workstations
    - Laptops
    - Mobile devices
    - Databases
    - Applications
    - Cloud services
    - Data centers
- Operational Technology (OT) environments, including:
    - Railway signaling systems
    - Train control systems
    - SCADA systems
    - Communication systems
    - Power supply and traction systems
    - Railway operations control centers
- All forms of information, regardless of format, including:
    - Electronic records
    - Physical documents
    - Audio and video recordings
    - System logs

- Backup media

Compliance with this policy is mandatory for all personnel and entities within its scope.

1.3 Objectives

The objectives of this Cybersecurity Policy are to:

a) Protect Critical Assets

Protect EDRSC's information assets, operational technology systems, and critical railway infrastructure from unauthorized access, misuse, disclosure, alteration, destruction, or disruption.

b) Support Safe Railway Operations

Ensure cybersecurity measures contribute to the safe, secure, and reliable operation of railway services, signaling systems, communication systems, and control centers.

c) Manage Cybersecurity Risks

Identify, assess, monitor, and mitigate cybersecurity risks that may affect business operations, safety, reputation, finances, and regulatory compliance.

d) Ensure Regulatory Compliance

Comply with applicable cybersecurity, privacy, transportation, and regulatory requirements in Ethiopia, Djibouti, and other relevant jurisdictions.

e) Ensure Service Availability

Maintain the availability and resilience of critical systems and services necessary for passenger transport, freight operations, and business continuity.

f) Strengthen Cybersecurity Awareness

Promote a cybersecurity-conscious culture through training, awareness, and accountability across the organization.

g) Improve Incident Response Capability

Establish effective capabilities for detecting, responding to, recovering from, and learning from cybersecurity incidents.

h) Support Continuous Improvement

Continuously improve the cybersecurity program through risk assessments, audits, monitoring, testing, lessons learned, and evolving industry best practices.

1.4 Policy Statement

Ethio-Djibouti Railway Share Company is committed to maintaining an effective cybersecurity program that safeguards its information resources, critical railway systems, employees, customers, business partners, and stakeholders.

EDRSC shall:

- Implement cybersecurity controls based on risk management principles.
- Protect information assets throughout their lifecycle.
- Secure both Information Technology (IT) and Operational Technology (OT) environments.
- Apply the principles of least privilege, defense in depth, and secure-by-design.
- Conduct regular cybersecurity risk assessments.
- Monitor systems for cyber threats and suspicious activities.
- Maintain incident response, business continuity, and disaster recovery capabilities.
- Ensure personnel understand and fulfill their cybersecurity responsibilities.
- Comply with applicable legal, regulatory, and contractual requirements.
- Continuously improve cybersecurity capabilities to address emerging threats and technological changes.

All employees, contractors, consultants, vendors, and third parties are required to comply with this policy and associated cybersecurity standards, procedures, and guidelines.

Failure to comply may result in disciplinary action, termination of access privileges, contract termination, legal action, or other corrective measures as deemed appropriate by EDRSC.

1.5 Definitions and Acronyms

Definitions

Asset Any information, system, application, device, service, or resource that has value to EDRSC.

Availability Ensuring information and systems are accessible to authorized users when required.

Confidentiality Protection of information from unauthorized access, disclosure, or exposure.

Cybersecurity Incident Any event that compromises or attempts to compromise the confidentiality, integrity, or availability of information or systems.

Data Breach Unauthorized access, disclosure, alteration, loss, or destruction of sensitive information.

Integrity Preservation of the accuracy, completeness, and reliability of information.

Least Privilege A security principle that restricts users to the minimum level of access required to perform their job functions.

Operational Technology (OT) Hardware and software used to monitor and control industrial and railway operational processes.

Risk The potential for loss, damage, or disruption resulting from a threat exploiting a vulnerability.

Threat Any circumstance or event that may adversely affect information assets, systems, or operations.

Vulnerability A weakness that can be exploited by a threat actor to compromise systems or information.

Acronyms

Acronym	Meaning
CEO	Chief Executive Officer
CDO	Chief Digital Officer
CISO	Chief Information Security Officer
IT	Information Technology
OT	Operational Technology
SCADA	Supervisory Control and Data Acquisition
SOC	Security Operations Center
CSIRT	Computer Security Incident Response Team
MFA	Multi-Factor Authentication
VPN	Virtual Private Network
SIEM	Security Information and Event Management
DLP	Data Loss Prevention
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
RBAC	Role-Based Access Control
EDR	Endpoint Detection and Response
RTO	Recovery Time Objective
RPO	Recovery Point Objective
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
EDRSC	Ethio-Djibouti Railway Share Company

2. Governance and Responsibilities

2.1 Board of Directors Responsibilities

- **Policy Statement**

- The Board of Directors shall provide strategic oversight and governance for cybersecurity across Ethio-Djibouti Railway Share Company (EDRSC). The Board shall ensure that cybersecurity risks are managed effectively and integrated into the organization's overall risk management framework.

- **Responsibilities**

- The Board of Directors shall:
- Approve the Cybersecurity Policy and related strategic initiatives.
- Establish the organization's cybersecurity risk appetite and tolerance levels.
- Ensure adequate funding and resources are allocated to cybersecurity programs.
- Review significant cybersecurity risks, incidents, and mitigation plans.
- Ensure cybersecurity is incorporated into corporate governance and enterprise risk management processes.
- Monitor management's performance in implementing cybersecurity objectives.
- Promote a culture of cybersecurity awareness and accountability.
- Review cybersecurity performance reports at least annually.
- Ensure compliance with applicable legal, regulatory, and contractual cybersecurity requirements.
- Support continuous improvement of cybersecurity capabilities.

2.2 Executive Management Responsibilities

Policy Statement

- Executive Management is responsible for ensuring the effective implementation, operation, and continuous improvement of EDRSC's cybersecurity program.

- **Responsibilities**

- Executive Management shall:
- Demonstrate leadership and commitment to cybersecurity.
- Ensure cybersecurity objectives align with business and operational objectives.

- Assign cybersecurity roles and responsibilities throughout the organization.
- Provide adequate personnel, financial resources, and technologies for cybersecurity operations.
- Support the implementation of cybersecurity policies, standards, and procedures.
- Ensure cybersecurity risks are appropriately identified, assessed, and managed.
- Review cybersecurity reports and risk assessments regularly.
- Ensure business continuity and disaster recovery capabilities are maintained.
- Support incident response and crisis management activities during cybersecurity events.
- Ensure corrective actions are implemented following security incidents and audits.
- Promote organization-wide cybersecurity awareness and compliance.

- ### Chief Executive Officer (CEO)

- The CEO shall:
- Serve as the executive sponsor for cybersecurity initiatives.
- Ensure cybersecurity receives appropriate management attention.
- Approve major cybersecurity investments and strategic initiatives.
- Report significant cybersecurity risks and incidents to the Board.

- ### Chief Digital Officer (CDO)

- The CDO shall:
- Lead the cybersecurity program.
- Develop and maintain cybersecurity policies and standards.
- Oversee cybersecurity governance, risk management, and compliance.
- Report cybersecurity performance and risks to executive management.
- Coordinate cybersecurity activities across IT and Operational Technology (OT) environments.

2.3 Information Security Team Responsibilities

- ### Policy Statement

- The Information Security Team shall implement, monitor, and continuously improve EDRSC's cybersecurity controls and capabilities.

- ### Responsibilities

- The Information Security Team shall:
- Develop and maintain cybersecurity policies, standards, procedures, and guidelines.
- Conduct cybersecurity risk assessments.
- Monitor cybersecurity threats, vulnerabilities, and emerging risks.
- Operate cybersecurity monitoring and incident detection capabilities.
- Coordinate cybersecurity incident response activities.

- Conduct vulnerability assessments and penetration testing.
- Ensure compliance with cybersecurity requirements.
- Maintain asset inventories and security classifications.
- Perform security reviews of systems, applications, and projects.
- Support business units in implementing cybersecurity controls.
- Provide security awareness and training programs.
- Monitor third-party cybersecurity compliance.
- Prepare cybersecurity reports for management and the Board.

Security Operations Responsibilities

- The Information Security Team shall:
- Monitor security events continuously.
- Investigate suspicious activities and alerts.
- Escalate significant incidents according to incident response procedures.
- Maintain logs and evidence for investigations.
- Perform threat intelligence and threat-hunting activities where applicable.

Operational Technology (OT) Security Responsibilities

- The Information Security Team shall work with railway operations personnel to:
- Protect signaling and train control systems.
- Monitor OT networks for cyber threats.
- Assess OT-specific cybersecurity risks.
- Support secure configuration and maintenance of OT systems.
- Ensure IT and OT security integration.

2.4 Employee Responsibilities

Policy Statement

- All employees are responsible for protecting EDRSC information assets and complying with cybersecurity requirements.

Responsibilities

- Employees shall:
- Comply with this Cybersecurity Policy and all associated procedures.
- Protect company information from unauthorized access, disclosure, alteration, or destruction.
- Use company systems only for authorized business purposes.
- Maintain the confidentiality of passwords and authentication credentials.
- Immediately report cybersecurity incidents, suspected breaches, and suspicious activities.

- Complete mandatory cybersecurity awareness training.
- Follow data classification and handling requirements.
- Secure company devices and equipment under their control.
- Protect sensitive information while working remotely or traveling.
- Cooperate with cybersecurity investigations and audits.
- Ensure physical security of company assets and information.

Employees Shall Not:

- Share passwords or user accounts.
- Install unauthorized software.
- Bypass security controls.
- Access systems without authorization.
- Connect unauthorized devices to company networks.
- Disclose confidential information without approval.
- Engage in activities that may compromise company security.
- Failure to comply with cybersecurity requirements may result in disciplinary action.

2.5 Third-Party Responsibilities

Policy Statement

- Third parties that access EDRSC systems, networks, facilities, or information assets shall comply with applicable cybersecurity requirements and contractual obligations.

Responsibilities

- Third-party vendors, contractors, consultants, service providers, and business partners shall:
- Comply with EDRSC cybersecurity policies and security requirements.
- Protect EDRSC information and systems from unauthorized access or disclosure.
- Implement appropriate security controls to safeguard information entrusted to them.
- Ensure personnel with access to EDRSC systems receive appropriate security awareness training.
- Promptly report cybersecurity incidents that may affect EDRSC.
- Participate in security assessments and audits when requested.
- Maintain confidentiality of EDRSC information.
- Restrict access to authorized personnel on a need-to-know basis.
- Ensure subcontractors comply with equivalent cybersecurity requirements.
- Support investigations related to cybersecurity incidents involving EDRSC information or systems.

Vendor Access Requirements

- Third-party access shall:

- Be formally approved before access is granted.
- Be limited to approved business purposes.
- Be regularly reviewed.
- Be monitored and logged.
- Be revoked immediately upon contract termination or when access is no longer required.

- **Contractual Security Requirements**

- Contracts with third parties shall include:
- Confidentiality obligations.
- Information security requirements.
- Incident notification requirements.
- Data protection obligations.
- Right-to-audit clauses.
- Compliance requirements.
- Service level and security performance expectations.

3. Information Security Framework

3.1 Security Principles

- **Policy Statement**

- Ethio-Djibouti Railway Share Company (EDRSC) shall establish, implement, and maintain an information security framework based on internationally recognized security principles to safeguard its information assets, operational technology (OT) systems, railway operations, and critical infrastructure.
- The following security principles shall guide all cybersecurity activities, decisions, and controls within EDRSC.

3.1.1 Confidentiality

- EDRSC shall protect information from unauthorized access, disclosure, or misuse.
- **Requirements:**
- Access to information shall be granted only to authorized individuals.
- Sensitive information shall be classified and protected according to its sensitivity level.
- Confidential and Restricted information shall be encrypted during storage and transmission.
- Information sharing shall follow the principle of need-to-know.

3.1.2 Integrity

- EDRSC shall maintain the accuracy, completeness, and reliability of information and systems.
- **Requirements:**
- Information shall be protected against unauthorized modification or destruction.
- Critical systems shall maintain audit trails and logging capabilities.
- Changes to systems and applications shall follow approved change management procedures.
- Data validation and integrity checks shall be implemented where appropriate.

3.1.3 Availability

- EDRSC shall ensure that information, systems, and services are available to authorized users when required.
- **Requirements:**
- Critical systems shall have backup and recovery mechanisms.
- Business Continuity and Disaster Recovery Plans shall be maintained.
- System performance and availability shall be monitored.
- Redundancy shall be implemented for critical railway and business systems where feasible.

3.1.4 Least Privilege

- Users shall be granted the minimum level of access necessary to perform their assigned duties.
- **Requirements:**
- Access rights shall be role-based.
- Privileged access shall be restricted and monitored.
- User access shall be reviewed periodically.
- Elevated privileges shall be approved and documented.

3.1.5 Defense in Depth

- EDRSC shall implement multiple layers of security controls to protect systems and information.
- **Examples include:**
- Physical security controls
- Firewalls
- Endpoint protection
- Network segmentation
- Access controls
- Monitoring systems
- Security awareness programs
- No single security control shall be relied upon as the sole means of protection.

3.1.6 Secure by Design

- Security shall be incorporated into systems, applications, and processes from the earliest stages of development and acquisition.
- **Requirements:**
- Security requirements shall be included in project planning.
- Systems shall undergo security reviews before deployment.
- Secure development practices shall be implemented.
- Risk assessments shall be conducted before introducing new technologies.

3.1.7 Accountability

- All users shall be accountable for activities performed using their assigned credentials and access privileges.
- **Requirements:**
- Unique accounts shall be assigned to all users.
- Security logs shall be maintained.
- User activities may be monitored in accordance with applicable laws and regulations.
- Violations shall be investigated and addressed appropriately.

3.1.8 Railway Safety First

- Cybersecurity measures shall support and enhance railway operational safety.
- **Requirements:**
- Safety-critical systems shall receive enhanced protection.
- Cybersecurity controls shall not compromise operational safety.
- OT cybersecurity risks shall be evaluated with safety impacts considered.
- Security incidents affecting railway operations shall receive immediate priority response.

3.2 Risk-Based Approach

Policy Statement

- EDRSC shall adopt a risk-based approach to cybersecurity management to ensure resources are focused on protecting the organization's most critical assets, systems, services, and railway operations.

Risk Management Principles

- Cybersecurity decisions shall be based on:
- Business impact
- Safety impact
- Operational impact

- Regulatory obligations
- Threat likelihood
- Vulnerability exposure

Risk Management Process

Risk Identification

- EDRSC shall identify cybersecurity risks related to:
- Information assets
- IT systems
- Operational technology systems
- Railway signaling infrastructure
- Third-party services
- Cloud services
- Physical infrastructure

Risk Assessment

- Cybersecurity risks shall be evaluated based on:

- **Likelihood**

Level	Description
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

- **Impact**

Level	Description
1	Insignificant
2	Minor
3	Moderate
4	Major
5	Severe

Risk Rating

- Risk Score = Likelihood × Impact

Score	Risk Level
1–4	Low
5–9	Medium
10–16	High
17–25	Critical

Risk Treatment

- EDRSC shall address identified risks through one or more of the following actions:

Mitigate

- Implement controls to reduce the likelihood or impact of the risk.

Transfer

- Transfer risk through insurance, outsourcing, or contractual agreements.

Avoid

- Eliminate activities that create unacceptable risk.

Accept

- Formally accept residual risk where justified and approved.

Risk Review

- Cybersecurity risk assessments shall be conducted:
- At least annually.
- Prior to major projects or system implementations.
- Following significant changes to systems or operations.
- Following major cybersecurity incidents.
- When significant new threats emerge.
- Critical and High risks shall be reported to Executive Management promptly.

3.3 Security Standards and Guidelines

Policy Statement

- EDRSC shall establish and maintain security standards, procedures, and guidelines that support the implementation of this Cybersecurity Policy and ensure consistent protection of information assets and railway operational systems.

Security Standards

- The cybersecurity program shall align with recognized standards and best practices, including:
- ISO/IEC 27001 Information Security Management Systems
- ISO/IEC 27002 Information Security Controls
- NIST Cybersecurity Framework (CSF)
- CIS Critical Security Controls
- ISO/IEC 22301 Business Continuity Management
- Relevant railway cybersecurity and operational safety standards
- Applicable laws and regulations of Ethiopia and Djibouti

Supporting Security Standards

- EDRSC shall maintain documented standards for:

Access Control Standard

- Defines requirements for:
- User access management
- Password management
- Multi-factor authentication
- Privileged access control

Network Security Standard

- Defines requirements for:
- Firewalls
- Network segmentation
- Wireless security
- Remote access

Endpoint Security Standard

- Defines requirements for:

- Anti-malware protection
- Patch management
- Device hardening
- Mobile device security

Data Protection Standard

- Defines requirements for:
- Data classification
- Data handling
- Encryption
- Retention and disposal

Operational Technology Security Standard

- Defines requirements for:
- Signaling systems security
- SCADA protection
- OT network security
- Control center protection

Incident Response Standard

- Defines requirements for:
- Incident reporting
- Investigation
- Escalation procedures
- Recovery activities

Business Continuity and Disaster Recovery Standard

- Defines requirements for:
- Backup management
- Continuity planning
- Recovery testing
- Crisis management

Security Procedures

- Detailed procedures shall be developed and maintained to support the implementation of security standards.
- Examples include:

- User account provisioning procedure
- Incident reporting procedure
- Vulnerability management procedure
- Backup and recovery procedure
- Change management procedure
- Vendor security assessment procedure
- OT maintenance security procedure

Security Guidelines

- Guidelines may be issued to provide practical recommendations and best practices for users and administrators.
- Examples include:
- Password creation guidelines
- Email security guidelines
- Remote working guidelines
- Secure use of mobile devices
- Phishing awareness guidance
- Secure handling of sensitive information

Compliance and Review

- All security standards, procedures, and guidelines shall:
- Be reviewed at least annually.
- Be updated following significant business or technology changes.
- Be communicated to relevant stakeholders.
- Support compliance with this Cybersecurity Policy.

4. Asset Management

4.1 Information Asset Inventory

Policy Statement

- Ethio-Djibouti Railway Share Company (EDRSC) shall establish, maintain, and regularly update an accurate inventory of all information assets to ensure appropriate protection, accountability, and risk management.

Requirements

- EDRSC shall identify and inventory all assets that support business operations, railway services, safety-critical functions, and information processing activities.
- The asset inventory shall include, but not be limited to:

Information Assets

- Business records
- Passenger and freight information
- Financial data
- Human resource records
- Operational reports
- Contracts and legal documents
- Technical drawings and engineering documents

Information Technology (IT) Assets

- Servers
- Desktop computers
- Laptops
- Mobile devices
- Network devices
- Databases
- Software applications
- Cloud services

Operational Technology (OT) Assets

- Signaling systems
- Train control systems
- SCADA systems
- Power management systems
- Traffic control systems

- Railway communication systems
- Control center equipment

Physical Assets

- Data centers
- Communication facilities
- Backup media
- Network cabinets
- Security devices

Asset Register Requirements

- The asset inventory shall include:
- Asset identification number
- Asset description
- Asset type
- Asset owner
- Asset custodian
- Physical or logical location
- Classification level
- Business criticality
- System dependencies
- Maintenance status
- Date of acquisition
- Disposal date (when applicable)

Inventory Review

- Asset inventories shall be:
- Reviewed at least annually
- Updated following acquisitions, transfers, modifications, or disposals
- Verified during audits and risk assessments

4.2 Asset Ownership

Policy Statement

- All information assets shall have an assigned owner responsible for ensuring the asset is appropriately classified, protected, maintained, and managed throughout its lifecycle.

Asset Owner Responsibilities

- Asset Owners shall:
- Identify and document assigned assets.
- Determine the asset classification level.
- Define access requirements.
- Approve user access requests.
- Review access privileges periodically.
- Ensure appropriate security controls are implemented.
- Participate in risk assessments affecting their assets.
- Ensure compliance with applicable policies and standards.
- Approve asset disposal and data destruction activities.

Asset Custodian Responsibilities

- Asset custodians are responsible for the day-to-day administration and protection of assets.
- Custodians shall:
- Maintain security controls.
- Perform backups and maintenance activities.
- Monitor asset performance and security.
- Report incidents affecting assigned assets.
- Support audits and compliance reviews.

User Responsibilities

- Users shall:
- Use assets only for authorized purposes.
- Protect assets against unauthorized access or damage.
- Immediately report lost, stolen, or compromised assets.
- Follow all applicable security requirements.

4.3 Asset Classification and Labeling

Policy Statement

- Information assets shall be classified according to their sensitivity, value, criticality, and legal or regulatory requirements to ensure appropriate protection measures are applied.

Classification Levels

Public

- Information approved for public disclosure.
- **Examples:**
- Published train schedules
- Press releases
- Marketing materials
- Public announcements
- **Label:** PUBLIC

Internal

- Information intended for internal organizational use only.
- **Examples:**
- Internal procedures
- Staff directories
- Operational reports
- Internal communications
- **Label:** INTERNAL

Confidential

- Information that could cause financial, operational, legal, or reputational damage if disclosed without authorization.
- **Examples:**
- Financial records
- Procurement information
- Employee records
- Vendor contracts
- Customer information
- **Label:** CONFIDENTIAL

Restricted

- Highly sensitive information whose disclosure, alteration, or loss could significantly impact railway operations, safety, security, or national interests.
- **Examples:**
- Signaling configurations
- SCADA system data
- Train control system configurations

- Network architecture diagrams
- Security credentials
- Vulnerability reports
- Security incident records
- **Label:** RESTRICTED

Labeling Requirements

- Information assets shall be labeled according to their classification.
- Labels may be applied through:
- Document headers and footers
- Electronic file naming conventions
- System classifications
- Physical labels on storage media
- Asset management systems

Reclassification

- Information shall be reclassified whenever:
- Business requirements change.
- Regulatory requirements change.
- Asset sensitivity changes.
- Ownership changes.

4.4 Asset Handling and Protection

Policy Statement

- Information assets shall be protected throughout their lifecycle, including creation, storage, processing, transmission, archival, and disposal.

General Protection Requirements

- All information assets shall be:
- Protected from unauthorized access.
- Protected from accidental or intentional alteration.
- Available to authorized users when required.
- Handled according to their classification.

Storage Requirements

Public Information

- May be stored on approved company systems without special restrictions.

Internal Information

- Shall be stored within authorized company systems.

Confidential Information

- Shall be:
- Stored on approved systems only.
- Protected through access controls.
- Backed up regularly.
- Encrypted where appropriate.

Restricted Information

- Shall be:
- Encrypted at rest.
- Stored only in approved secure environments.
- Accessible only to authorized personnel.
- Subject to enhanced monitoring and logging.

Transmission Requirements

- Information transmitted electronically shall use secure communication methods.

Confidential and Restricted Information

- Must be protected through:
- Encryption
- Secure file transfer mechanisms
- Approved communication channels
- Transmission through personal email accounts or unauthorized systems is prohibited.

Physical Protection Requirements

- Physical assets and storage media shall be protected through:

- Locked cabinets
- Controlled access facilities
- CCTV monitoring
- Visitor management controls
- Environmental protections
- Special protection shall be applied to railway control centers, data centers, and signaling facilities.

Media Handling

- Storage media including USB drives, external hard drives, CDs, and backup tapes shall:
- Be authorized before use.
- Be encrypted when containing Confidential or Restricted information.
- Be securely stored when not in use.
- Be tracked and inventoried where appropriate.
- Unauthorized removable media shall not be connected to EDRSC systems.

Asset Disposal

- Information assets shall be securely disposed of when no longer required.

Electronic Media

- Must be:
- Securely wiped
- De-gaussed where applicable
- Physically destroyed when necessary

Paper Records

- Must be:
- Shredded
- Pulped
- Destroyed using approved methods

Disposal Authorization

- Asset disposal shall require:
- Asset Owner approval
- Verification of data removal
- Documentation of disposal activities

Lost, Stolen, or Damaged Assets

- Employees shall immediately report:
- Lost laptops
- Stolen mobile devices
- Missing storage media
- Damaged equipment
- Suspected asset compromise
- Incidents involving Restricted information or operational technology assets shall be escalated immediately to the Information Security Team and relevant management.

5. Risk Management

5.1 Risk Assessment Process

- **Policy Statement**

- Ethio-Djibouti Railway Share Company (EDRSC) shall establish and maintain a structured cybersecurity risk assessment process to identify, analyze, evaluate, and prioritize risks that may affect the confidentiality, integrity, availability, safety, and resilience of the organization's information assets, operational technology (OT), and railway operations.

Risk Assessment Objectives

- The risk assessment process shall:
- Identify cybersecurity threats and vulnerabilities.
- Evaluate risks to business operations and railway services.
- Assess the potential impact on safety-critical systems.
- Support informed decision-making and resource allocation.
- Ensure compliance with legal, regulatory, and contractual obligations.
- Facilitate continuous improvement of cybersecurity controls.

Risk Assessment Scope

- Risk assessments shall cover:
- Information assets
- IT infrastructure
- Operational Technology (OT) systems
- Signaling and train control systems
- SCADA systems

- Communication networks
- Cloud services
- Third-party services
- Physical infrastructure
- Business processes

Risk Assessment Methodology

Step 1: Asset Identification

- Identify and document:
- Critical business assets
- Railway operational assets
- Information systems
- Applications
- Data repositories
- Network infrastructure

Step 2: Threat Identification

- Potential threats include:
- Malware and ransomware
- Phishing attacks
- Insider threats
- Unauthorized access
- Denial-of-Service (DoS) attacks
- Supply chain attacks
- Service disruptions
- Natural disasters
- Human error
- Nation-state cyber threats

Step 3: Vulnerability Identification

- Identify weaknesses that may expose assets to threats, including:
- Unpatched systems
- Weak passwords
- Misconfigured systems
- Inadequate monitoring
- Outdated software
- Insecure remote access
- Poor physical security controls

Step 4: Likelihood Assessment

- Evaluate the probability of a threat exploiting a vulnerability.

Score	Likelihood
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

Step 5: Impact Assessment

- Evaluate the consequences if the risk materializes.

Score	Impact
1	Insignificant
2	Minor
3	Moderate
4	Major
5	Severe

Impact Considerations

- Assessment shall include:
- Safety impact
- Operational disruption
- Financial loss
- Regulatory penalties
- Reputation damage
- Customer impact
- Service interruption

Step 6: Risk Rating

- Risk Score = Likelihood × Impact

Risk Score	Risk Level
1-4	Low
5-9	Medium

10-16	High
17-25	Critical

Assessment Frequency

- Cybersecurity risk assessments shall be conducted:
- Annually
- Before implementation of major projects
- Before introducing new technologies
- Following significant system changes
- After major cybersecurity incidents
- Upon identification of significant new threats

Risk Assessment Documentation

- The Information Security Team shall maintain:
- Risk registers
- Assessment reports
- Risk treatment plans
- Management approvals
- Residual risk records

5.2 Risk Treatment and Mitigation

Policy Statement

- EDRSC shall implement appropriate measures to eliminate, reduce, transfer, or formally accept identified cybersecurity risks based on business needs, operational requirements, and risk appetite.

Risk Treatment Options

- **Risk Mitigation**

- Risks may be reduced through implementation of security controls such as:
- Multi-Factor Authentication (MFA)
- Firewalls
- Network segmentation
- Endpoint protection
- Security monitoring
- Encryption
- Employee awareness training

- Access controls
- OT security controls

Risk Avoidance

- Risk may be eliminated by:
- Discontinuing high-risk activities
- Removing vulnerable systems
- Avoiding unnecessary exposure to threats
- Preventing unauthorized technology deployments

Risk Transfer

- Risk may be transferred through:
- Cybersecurity insurance
- Service contracts
- Outsourcing agreements
- Vendor liability clauses

Risk Acceptance

- Risk may be accepted when:
- Treatment costs exceed potential impact.
- The risk falls within approved risk tolerance levels.
- Appropriate management approval has been obtained.

Risk Treatment Plan Requirements

- For all High and Critical risks, a documented treatment plan shall include:
- Risk description
- Risk owner
- Recommended mitigation measures
- Required resources
- Implementation timeline
- Target completion date
- Residual risk assessment

Safety-Critical Risks

- Risks affecting:
- Train control systems
- Signaling systems

- SCADA environments
- Railway communication systems
- Power and traction systems
- shall receive priority treatment and executive oversight.

Implementation Responsibilities

- Risk Owners shall:
- Ensure treatment actions are implemented.
- Monitor remediation progress.
- Report status updates.
- Verify that controls are functioning effectively.

Residual Risk

- After mitigation measures are implemented, remaining risks shall be evaluated and formally accepted by the appropriate authority where required.

Risk Acceptance Authority

Risk Level	Approval Authority
Low	Department Manager
Medium	Department Head
High	Chief Digital Officer (CDO)
Critical	CEO and Executive Management

5.3 Risk Monitoring and Reporting

- **Policy Statement**

- EDRSC shall continuously monitor cybersecurity risks and provide timely reporting to ensure management maintains appropriate visibility into the organization's cybersecurity posture.

Risk Monitoring Activities

- The Information Security Team shall monitor:
- Threat intelligence
- Security incidents
- Vulnerability assessments
- Penetration testing results

- Compliance findings
- Third-party risks
- Emerging cybersecurity threats
- OT security events
- Control effectiveness

Key Risk Indicators (KRIs)

- The organization shall establish and monitor KRIs, including:
- Number of critical vulnerabilities
- Number of unresolved security incidents
- Failed login attempts
- Phishing attack rates
- Patch compliance levels
- Third-party security findings
- Security awareness training completion rates
- OT security alerts

Risk Register Maintenance

- A centralized cybersecurity risk register shall be maintained and shall include:
- Risk identification number
- Risk description
- Asset affected
- Business owner
- Likelihood rating
- Impact rating
- Risk level
- Treatment status
- Review date
- Residual risk rating

Reporting Requirements

Operational Reporting

- The Information Security Team shall provide:
- Monthly cybersecurity risk reports
- Vulnerability management reports
- Incident trend reports
- Compliance status reports

Management Reporting

- Executive Management shall receive:
- Quarterly cybersecurity risk summaries
- Significant risk notifications
- Major incident reports
- Risk treatment progress reports

Board Reporting

- The Board of Directors shall receive:
- Annual cybersecurity risk assessment reports
- Strategic cybersecurity risk updates
- Major incident summaries
- Cybersecurity maturity assessments

Escalation Requirements

- The following shall be escalated immediately to Executive Management:
- Critical cybersecurity risks
- Significant data breaches
- Incidents affecting railway operations
- OT security incidents
- Regulatory compliance violations
- Third-party incidents impacting EDRSC

Continuous Improvement

- Risk monitoring results shall be used to:
- Improve security controls
- Update risk treatment plans
- Enhance incident response capabilities
- Strengthen security awareness programs
- Improve resilience of railway operations

6. Access Control Policy

6.1 User Access Management

- **Policy Statement**

- Ethio-Djibouti Railway Share Company (EDRSC) shall implement formal user access management processes to ensure that access to information assets, information systems, operational technology (OT) systems, and network resources is authorized, controlled, monitored, and periodically reviewed.

Access Control Principles

- Access to EDRSC systems and information shall be based on:
- Business need-to-know
- Least privilege
- Role-Based Access Control (RBAC)
- Segregation of duties
- Accountability and traceability

User Registration and Provisioning

- All user accounts shall:
- Be uniquely assigned to an individual user.
- Require documented management approval.
- Be created through established access provisioning procedures.
- Be assigned appropriate access rights based on job responsibilities.

Access Modification

- Access rights shall be reviewed and modified whenever:
- Employees change roles.
- Employees are transferred.
- Responsibilities change.
- Temporary access periods expire.

Access Termination

- User access shall be revoked:
- Immediately upon termination of employment.
- Immediately upon contract termination.
- Within 24 hours of role changes requiring access removal.
- Upon identification of unauthorized or inappropriate access.

Periodic Access Reviews

- Department managers and system owners shall review user access rights:
- Quarterly for critical systems.
- Semi-annually for standard business systems.
- Immediately following significant organizational changes.

Service Accounts

- Service and system accounts shall:
- Have documented ownership.
- Be approved by system owners.
- Be monitored regularly.
- Use strong authentication controls.
- Not be used for interactive user activities unless specifically authorized.

6.2 Privileged Access Management

Policy Statement

- Privileged access shall be strictly controlled, monitored, and limited to authorized personnel whose job responsibilities require elevated system privileges.

Privileged Accounts

- Privileged accounts include, but are not limited to:
- System administrators
- Database administrators
- Network administrators
- Cloud administrators
- Security administrators
- OT system administrators
- Emergency access accounts

Requirements

- Privileged access shall:
- Be formally approved by management and the asset owner.
- Be granted only when necessary for business functions.
- Be assigned to named individuals whenever possible.
- Be regularly reviewed.
- Be removed when no longer required.

Privileged Access Controls

- The organization shall:
- Maintain a register of privileged accounts.
- Limit the number of privileged users.
- Separate administrative and standard user accounts.
- Monitor privileged account activities.
- Log all administrative activities.
- Periodically review all privileged permissions.

Emergency Access Accounts

- Emergency or "break-glass" accounts shall:
- Be restricted to authorized personnel.
- Be used only during emergency situations.
- Be monitored and logged.
- Be reviewed after every use.

Operational Technology (OT) Privileged Access

- Administrative access to:
- Signaling systems
- Train control systems
- SCADA systems
- Railway communication systems
- shall require enhanced controls and approval from both the responsible operational manager and Information Security Team.

6.3 Password and Authentication Requirements

- **Policy Statement**

- EDRSC shall enforce strong authentication mechanisms to reduce the risk of unauthorized access to systems, applications, and data.

Password Requirements

Standard User Accounts

- Passwords shall:
- Contain a minimum of 12 characters.
- Include uppercase and lowercase letters.

- Include numbers and special characters.
- Not contain easily guessed information.
- Not contain usernames or employee names.

Privileged Accounts

- Passwords for privileged accounts shall:
- Contain a minimum of 15 characters.
- Be unique for each system.
- Be protected using MFA.
- Not be shared under any circumstances.

Password Protection

- Users shall not:
- Share passwords.
- Store passwords in plain text.
- Send passwords through email or messaging systems.
- Reuse organizational passwords for personal accounts.

Password Managers

- EDRSC may provide approved password management solutions to securely store and manage credentials.

Account Lockout Controls

- Systems shall implement account lockout mechanisms after repeated failed authentication attempts.
- Recommended standard:
- Lock account after five unsuccessful attempts.
- Automatic unlock after 30 minutes or administrator intervention.

Authentication Requirements

- Authentication mechanisms shall support:
- Unique user identification
- Secure password storage
- Session management
- Logging and monitoring
- Where supported, modern authentication technologies shall be used instead of legacy authentication methods.

6.4 Multi-Factor Authentication (MFA)

- **Policy Statement**

- Multi-Factor Authentication (MFA) shall be used to strengthen identity verification and reduce the risk of credential compromise.

MFA Requirements

- MFA is mandatory for:
- Remote access connections
- VPN access
- Cloud services
- Administrative accounts
- Email systems
- Financial systems
- Human Resource systems
- Security management systems
- OT administrative functions

Acceptable MFA Methods

- Approved authentication factors may include:
- Hardware security tokens
- Mobile authenticator applications
- Biometric authentication
- Smart cards
- One-time password (OTP) solutions

Prohibited Methods

- The following shall not be used as the sole authentication factor:
- Shared credentials
- Generic user accounts
- Weak authentication mechanisms

MFA Exceptions

- Exceptions shall:
- Be documented.
- Be risk assessed.
- Be approved by the Chief Digital Officer (CDO).

- Include compensating security controls.
-

6.5 Remote Access Security

- **Policy Statement**

- Remote access to EDRSC systems shall be authorized, secured, monitored, and managed to protect organizational information and railway operational environments.

Authorized Remote Access

- Remote access shall only be provided when:
- Business justification exists.
- Management approval is obtained.
- Security requirements have been met.

Remote Access Controls

- Remote access connections shall:
- Use approved VPN technologies.
- Utilize MFA.
- Employ encrypted communication channels.
- Be logged and monitored.
- Comply with organizational security standards.

Endpoint Requirements

- Devices used for remote access shall:
- Have current antivirus or endpoint protection installed.
- Be regularly patched and updated.
- Use approved operating systems.
- Have disk encryption enabled where feasible.
- Be protected with passwords or biometric authentication.

Remote Access to OT Systems

- Access to operational technology environments shall:
- Be restricted to authorized personnel.
- Require explicit approval.
- Use secure remote access gateways.
- Be monitored in real time.

- Be logged for audit purposes.

Public Network Usage

- When using public networks, employees shall:
- Connect only through approved VPN services.
- Avoid accessing sensitive information without encryption.
- Protect devices from unauthorized viewing and access.

Remote Working Responsibilities

- Employees working remotely shall:
- Protect company information.
- Prevent unauthorized access by family members or third parties.
- Secure devices when unattended.
- Immediately report lost or stolen devices.
- Report suspected cybersecurity incidents without delay.

Monitoring and Auditing

- EDRSC reserves the right to monitor and audit remote access activities to ensure compliance with cybersecurity policies, legal requirements, and operational security obligations.

7. Identity and Access Management (IAM)

7.1 User Provisioning and De-provisioning

- **Policy Statement**

- Ethio-Djibouti Railway Share Company (EDRSC) shall implement formal Identity and Access Management (IAM) processes to ensure that user accounts are created, modified, managed, and removed in a secure and timely manner throughout the user lifecycle.
- The IAM program shall ensure that access to EDRSC information assets, information systems, operational technology (OT) environments, applications, and facilities is granted only to authorized individuals based on approved business requirements.

User Provisioning

- User accounts shall be created only after:
- Verification of employment or contractual relationship.
- Approval by the employee's supervisor or department head.
- Approval by the relevant system or asset owner.

- Confirmation of required access levels based on job responsibilities.
- Completion of mandatory onboarding requirements, where applicable.

Provisioning Requirements

- Each user account shall:
- Be uniquely assigned to an individual.
- Be linked to an approved identity source.
- Follow EDRSC naming conventions.
- Be assigned appropriate access privileges.
- Be traceable to the responsible manager.
- The Information Technology Department shall maintain records of:
- Access requests
- Approvals
- Provisioning activities
- Modification history
- User account inventories

Temporary Access Provisioning

- Temporary access may be granted for:
- Contractors
- Consultants
- Project personnel
- External support personnel
- Emergency operational requirements
- Temporary accounts shall:
- Have a documented business justification.
- Include an expiration date.
- Be approved by the asset owner.
- Be automatically disabled upon expiration.

Access Modification

- Access rights shall be reviewed and updated whenever:
- Employees change positions.
- Employees transfer departments.
- Additional responsibilities are assigned.
- Projects are completed.
- Temporary assignments end.
- Managers shall notify the IT Department and Information Security Team whenever access changes are required.

User De-provisioning

- Access privileges shall be revoked promptly when:
- Employment is terminated.
- Contracts expire.
- Users resign.
- Business relationships end.
- Access is no longer required.

De-provisioning Requirements

- The Human Resources Department shall notify IT and Information Security immediately upon employee separation.
- The IT Department shall:
- Disable user accounts immediately upon termination.
- Remove access to applications and databases.
- Disable VPN and remote access privileges.
- Remove access to cloud services.
- Recover company-owned devices.
- Revoke physical access credentials.
- Document de-provisioning activities.

High-Risk Terminations

- In cases involving:
- Security concerns
- Disciplinary actions
- Insider threat investigations
- account access may be disabled immediately before employee notification, in coordination with Human Resources and management.

7.2 Role-Based Access Control (RBAC)

Policy Statement

- EDRSC shall implement Role-Based Access Control (RBAC) to ensure that access permissions are assigned according to job functions and business responsibilities.
- RBAC shall reduce the risk of unauthorized access while improving consistency, accountability, and operational efficiency.

RBAC Principles

- Access shall be granted based on:
- Job role
- Business need
- Least privilege
- Segregation of duties
- Users shall receive only the access required to perform their assigned duties.

Role Definitions

EDRSC shall maintain documented access roles for:

Executive Management

- Access to:
- Executive reporting systems
- Strategic planning systems
- Financial dashboards

Human Resources Personnel

- Access to:
- Employee records
- Payroll systems
- Recruitment systems

Finance Personnel

- Access to:
- Financial systems
- Accounting systems
- Procurement systems

IT Administrators

- Access to:
- Infrastructure management systems
- Server administration tools
- Network management systems

Operational Technology Personnel

- Access to:
- Signaling systems
- Train control systems
- SCADA systems
- Railway communications systems

Information Security Personnel

- Access to:
- Security monitoring systems
- SIEM platforms
- Incident response tools
- Security reporting systems

Segregation of Duties (SoD)

- EDRSC shall implement segregation of duties controls to prevent conflicts of interest and reduce fraud and operational risks.
- Examples include:
- System administrators shall not approve their own access requests.
- Payment initiators shall not approve payments.
- Developers shall not deploy production changes without independent approval.
- Security auditors shall remain independent of operational administration activities.

Role Approval and Management

- Role creation and modification shall require:
- Business owner approval
- Security review
- Documentation of assigned permissions
- Role definitions shall be reviewed periodically to ensure alignment with business requirements.

Privileged Roles

- Roles granting elevated privileges shall be:
- Minimized
- Documented
- Approved by management
- Monitored continuously
- Reviewed more frequently than standard accounts

- Enhanced controls shall apply to OT and safety-critical environments.

7.3 Periodic Access Reviews

Policy Statement

- EDRSC shall perform periodic reviews of user access rights to ensure access remains appropriate, authorized, and aligned with business needs.

Objectives

- Access reviews shall:
- Detect excessive access privileges.
- Identify inactive accounts.
- Remove unauthorized access.
- Verify compliance with the principle of least privilege.
- Support regulatory and audit requirements.

- **Review Frequency**

Access Type	Review Frequency
Privileged Accounts	Quarterly
OT/SCADA Administrative Accounts	Quarterly
Critical Business Systems	Quarterly
Standard User Accounts	Semi-Annually
Vendor Accounts	Quarterly
Temporary Accounts	Monthly
Emergency (Break-Glass) Accounts	After Each Use and Quarterly

Access Review Process

Step 1: Generate Access Reports

- The IT Department shall generate user access listings for each system.

Step 2: Management Review

- Managers and asset owners shall review:
- Active users
- Assigned roles

- Privileged accounts
- Access appropriateness

Step 3: Validation

- Reviewers shall verify that:
- Access is still required.
- Access levels remain appropriate.
- Segregation of duties requirements are maintained.
- Inactive users are identified.

Step 4: Remediation

- Unnecessary or excessive access shall be:
- Modified
- Reduced
- Revoked
- Documented

Step 5: Approval and Record Retention

- Completed reviews shall be:
- Approved by the responsible manager.
- Retained for audit purposes.
- Available for compliance verification.

Inactive Accounts

- Accounts that remain inactive for more than **90 days** shall be reviewed and may be disabled pending management approval.
- Accounts inactive for more than **180 days** shall normally be disabled unless a documented business justification exists.

Third-Party Access Reviews

- Vendor and contractor access shall be reviewed regularly to ensure:
- Access remains necessary.
- Contractual relationships remain valid.
- Access permissions are appropriate.
- Expired accounts are removed.

Audit and Compliance

- The Information Security Team shall:
- Monitor completion of access reviews.
- Report non-compliance to management.
- Maintain evidence of review activities.
- Support internal and external audit requirements.

Exceptions

- Any exception to IAM requirements shall:
- Be documented.
- Include a business justification.
- Undergo risk assessment.
- Be approved by the Chief Digital Officer (CDO).
- Be reviewed at least annually.

8. Data Protection and Privacy

8.1 Data Classification

Policy Statement

- Ethio-Djibouti Railway Share Company (EDRSC) shall classify information based on its sensitivity, business value, legal obligations, operational importance, and potential impact resulting from unauthorized disclosure, modification, destruction, or loss.
- Information classification shall enable the implementation of appropriate protection measures throughout the information lifecycle.

Classification Objectives

- EDRSC shall classify information to:
- Ensure appropriate protection of information assets.
- Support safe and secure railway operations.
- Facilitate regulatory compliance.
- Protect customer, employee, and business information.
- Guide information handling and access requirements.

Information Classification Levels

Public

- Information approved for public release.
- **Examples:**
- Public train schedules
- Press releases
- Published annual reports
- Marketing materials
- **Protection Requirements:**
- No special restrictions.
- Maintain integrity and accuracy.

Internal

- Information intended for internal EDRSC use only.
- **Examples:**
- Internal policies
- Operational reports
- Staff directories
- Internal correspondence
- **Protection Requirements:**
- Access limited to authorized personnel.
- Stored on approved EDRSC systems.

Confidential

- Information whose unauthorized disclosure may adversely affect EDRSC operations, finances, customers, or reputation.
- **Examples:**
- Employee records
- Procurement information
- Financial reports
- Contractual agreements
- Customer data
- **Protection Requirements:**
- Access restricted to authorized personnel.
- Encryption during transmission.
- Enhanced monitoring and protection.

Restricted

- Highly sensitive information whose compromise could significantly impact railway operations, public safety, security, regulatory compliance, or national interests.
- **Examples:**
- Train control configurations
- Signaling system data
- SCADA configurations
- Network security architecture
- Encryption keys
- Security investigation reports

Protection Requirements:

- Strong encryption at rest and in transit.
- Strict access controls.
- Enhanced monitoring and logging.
- Executive oversight where applicable.

Classification Responsibilities

- Asset Owners shall:
- Classify information assets.
- Periodically review classifications.
- Ensure appropriate handling controls are applied.
- Reclassify information when business requirements change.

8.2 Data Storage and Retention

Policy Statement

- EDRSC shall securely store, retain, archive, and dispose of information in accordance with legal, regulatory, contractual, operational, and business requirements.

Data Storage Requirements

- Information shall be stored only on authorized:
- Servers
- Databases
- Cloud platforms
- Workstations
- Backup systems

- Approved storage media

Storage Controls

- Data storage solutions shall provide:
- Access control mechanisms
- Backup capabilities
- Logging and monitoring
- Malware protection
- Physical security controls
- Data recovery capabilities

Retention Requirements

- Records shall be retained based on legal, operational, and business requirements.

- **Recommended Minimum Retention Periods**

Information Type	Retention Period
Employee Records	7 Years
Financial Records	10 Years
Contracts	10 Years after expiration
Procurement Records	7 Years
Security Logs	12 Months Minimum
Incident Reports	5 Years
Backup Data	According to backup policy
OT System Logs	24 Months Minimum
Railway Operational Records	As required by regulations

Archiving

- Archived information shall:
- Remain accessible when required.
- Be protected according to its classification.
- Be regularly reviewed for retention compliance.

Secure Disposal

- When retention periods expire, information shall be securely disposed of using approved destruction methods.
- Examples include:

- Secure wiping
- Cryptographic erasure
- Physical destruction
- Shredding
- Documentation of disposal activities shall be maintained.

8.3 Data Encryption

Policy Statement

- EDRSC shall use encryption to protect the confidentiality and integrity of sensitive information during storage, processing, and transmission.

Encryption Requirements

- Encryption shall be applied to:
- Confidential information
- Restricted information
- Personal information
- Financial information
- Railway operational information
- Backup media

Data at Rest

- Confidential and Restricted information stored on:
- Servers
- Databases
- Laptops
- Mobile devices
- Cloud services
- Backup media
- shall be protected using approved encryption mechanisms.

Data in Transit

- Sensitive information transmitted through:
- Email
- VPN connections
- Web applications
- File transfer systems
- Cloud services

- shall use secure encrypted protocols.
- Examples include:
- TLS
- HTTPS
- SFTP
- IPSec VPN

Encryption Key Management

- EDRSC shall establish controls for:
- Generation of encryption keys
- Storage of encryption keys
- Key backup and recovery
- Key rotation
- Key destruction
- Access to cryptographic keys shall be restricted to authorized personnel.

Prohibited Activities

- The following are prohibited:
- Use of obsolete encryption standards.
- Unauthorized encryption tools.
- Sharing encryption keys with unauthorized individuals.

8.4 Data Loss Prevention (DLP)

Policy Statement

- EDRSC shall implement technical, administrative, and operational controls to prevent the unauthorized disclosure, leakage, destruction, alteration, or loss of sensitive information.

DLP Objectives

- The Data Loss Prevention Program shall:
- Protect sensitive information.
- Detect unauthorized data transfers.
- Prevent accidental disclosure.
- Monitor information movement.
- Reduce insider and external risks.

DLP Controls

- EDRSC may implement:
- Email filtering
- Content inspection
- File transfer monitoring
- Endpoint DLP solutions
- USB device controls
- Cloud DLP controls
- Network monitoring

Monitoring Requirements

- The organization shall monitor activities involving:
- Customer information
- Employee information
- Financial data
- Restricted railway operational data
- Security-sensitive information

Removable Media Controls

- Use of removable media shall:
- Require business justification.
- Be approved where necessary.
- Use encryption for sensitive information.
- Be monitored and controlled.

Incident Response

- Detected data loss events shall:
- Be investigated immediately.
- Be reported according to incident response procedures.
- Be documented and tracked to closure.

Data Transfer Requirements

- Sensitive information shall only be transferred through approved and secure channels.
- Unauthorized use of:
- Personal email accounts
- Public file-sharing services
- Unapproved cloud storage platforms

- is prohibited.

8.5 Privacy Protection Requirements

Policy Statement

- EDRSC is committed to protecting the privacy and confidentiality of personal information relating to employees, passengers, customers, suppliers, contractors, and other stakeholders.
- Personal information shall be collected, processed, stored, shared, and disposed of in accordance with applicable legal, regulatory, and contractual requirements.

Privacy Principles

- EDRSC shall process personal information according to the following principles:

Lawfulness and Fairness

- Personal information shall be collected and processed only for legitimate business purposes.

Purpose Limitation

- Information shall only be used for authorized and documented purposes.

Data Minimization

- Only the minimum amount of personal information necessary shall be collected and processed.

Accuracy

- Personal information shall be accurate and kept up to date where required.

Storage Limitation

- Personal information shall not be retained longer than necessary.

Confidentiality and Security

- Appropriate safeguards shall protect personal information from unauthorized access, disclosure, alteration, or destruction.

Personal Information Covered

- Examples include:

- Employee records
- Passenger information
- Customer information
- Contact details
- Identification documents
- Payroll information
- Recruitment records
- Health and safety records

Access to Personal Information

- Access shall be restricted to personnel with a legitimate business need.
- Access requests shall:
- Be approved by authorized management.
- Be logged where appropriate.
- Be periodically reviewed.

Third-Party Privacy Requirements

- Third parties processing EDRSC information shall:
- Sign confidentiality agreements.
- Implement adequate security controls.
- Use information only for authorized purposes.
- Report privacy incidents immediately.

Privacy Incident Reporting

- Any actual or suspected:
- Data breach
- Unauthorized disclosure
- Loss of personal information
- Unauthorized access
- shall be reported immediately to:
- The Information Security Team
- The Data Protection Officer (if appointed)
- Relevant management
- The organization shall investigate and respond to privacy incidents in accordance with established incident response procedures.

Cross-Border Data Transfer

- Transfer of personal information outside Ethiopia or Djibouti shall:

- Be authorized by management.
- Meet applicable legal requirements.
- Be secured through approved protection mechanisms.
- Be documented and risk assessed.

Compliance

- Failure to comply with this Data Protection and Privacy Policy may result in:
- Disciplinary action
- Access revocation
- Contract termination
- Legal and regulatory consequences

9. Network Security

9.1 Network Architecture Standards

Policy Statement

- Ethio-Djibouti Railway Share Company (EDRSC) shall design, implement, and maintain secure network architectures that protect information assets, operational technology (OT) systems, railway operations, and critical infrastructure from unauthorized access, cyber threats, and service disruptions.

Objectives

- The network architecture shall:
- Protect the confidentiality, integrity, and availability of information.
- Support safe and reliable railway operations.
- Minimize cybersecurity risks.
- Enable secure communications across EDRSC facilities.
- Support regulatory and compliance requirements.

Network Design Principles

- EDRSC shall implement the following principles:

Defense in Depth

- Multiple layers of security controls shall be deployed to provide protection at the:
- Perimeter
- Network

- Application
- Endpoint
- User levels

Network Segmentation

- Networks shall be segmented based on business functions and security requirements.
- At a minimum, the following environments shall be logically or physically separated:
- Corporate IT Network
- Operational Technology (OT) Network
- SCADA Network
- Signaling Systems Network
- Train Control Systems
- Data Center Network
- Guest Wireless Network
- Internet-facing Services

Operational Technology (OT) Segregation

- Safety-critical railway systems shall be isolated from business networks through:
- Industrial firewalls
- Demilitarized Zones (DMZs)
- Secure gateways
- Access control mechanisms
- Direct Internet connectivity for critical OT systems is prohibited unless explicitly approved and protected.

Secure Network Design Requirements

- All networks shall:
- Use approved network equipment.
- Follow secure configuration standards.
- Maintain current architecture documentation.
- Minimize unnecessary services and protocols.
- Support monitoring and logging capabilities.

Network Documentation

- The IT Department shall maintain:
- Network diagrams
- IP address inventories
- VLAN allocation records

- Network device inventories
- Interconnection documentation

9.2 Firewall Management

Policy Statement

- Firewalls shall be deployed and managed to protect EDRSC networks and systems from unauthorized access and malicious activity.

Firewall Deployment

- Firewalls shall be implemented at:
- Internet gateways
- Data centers
- Remote access gateways
- Network segmentation boundaries
- OT network perimeters
- Cloud environments

Firewall Configuration Requirements

- Firewall rules shall:
- Follow the principle of least privilege.
- Deny traffic by default unless explicitly authorized.
- Be documented and approved.
- Be reviewed periodically.

Firewall Rule Management

- The Information Technology Department shall:
- Maintain firewall rule inventories.
- Review firewall configurations quarterly.
- Remove unused or obsolete rules.
- Monitor firewall performance and alerts.

Change Management

- Changes to firewall configurations shall:
- Follow change management procedures.
- Include risk assessments where applicable.
- Be approved before implementation.

- Be tested and documented.

Logging Requirements

- Firewalls shall generate logs for:
- Access attempts
- Denied connections
- Administrative activities
- Security events
- Configuration changes
- Logs shall be retained according to the organization's logging and monitoring requirements.

OT Firewall Requirements

- Traffic between IT and OT environments shall:
- Pass through approved firewalls.
- Be restricted to authorized protocols.
- Be monitored continuously.
- Be reviewed regularly.

9.3 Intrusion Detection and Prevention

Policy Statement

- EDRSC shall implement intrusion detection and prevention capabilities to identify, alert, and respond to unauthorized or malicious activity affecting its networks, systems, and railway operational environments.

Intrusion Detection Systems (IDS)

- IDS technologies shall be used to:
- Monitor network traffic.
- Detect suspicious activity.
- Identify policy violations.
- Support incident investigations.

Intrusion Prevention Systems (IPS)

- IPS technologies shall:
- Detect malicious traffic.
- Block known attacks where appropriate.
- Protect critical systems and services.

- Support proactive threat mitigation.

Monitoring Requirements

- Intrusion monitoring shall cover:
- Internet gateways
- Data centers
- Critical servers
- OT environments
- Cloud services
- Remote access environments

Detection Capabilities

- Monitoring systems should detect:
- Malware activity
- Unauthorized access attempts
- Port scanning
- Network reconnaissance
- Denial-of-Service attacks
- Command and control communications
- Insider threats

Alert Management

- The Information Security Team shall:
- Investigate security alerts promptly.
- Escalate significant threats.
- Document incidents and actions taken.
- Maintain incident response records.

OT Monitoring

- Additional monitoring controls shall be implemented for:
- Signaling systems
- Train control systems
- SCADA environments
- Railway communications infrastructure
- Any suspected attack impacting railway operations shall be treated as a high-priority incident.

9.4 Wireless Network Security

Policy Statement

- Wireless networks shall be secured to prevent unauthorized access, interception of communications, and compromise of EDRSC systems and information assets.

Authorized Wireless Networks

- Only approved wireless networks may be deployed within EDRSC facilities.
- Unauthorized wireless access points are prohibited.

Wireless Security Requirements

- Wireless networks shall:
- Use WPA3 encryption where supported.
- Use strong authentication methods.
- Be configured according to approved standards.
- Be monitored regularly.

Network Segmentation

- Wireless networks shall be separated according to usage:

Corporate Wireless Network

- Access limited to authorized employees and approved devices.

Guest Wireless Network

- Isolated from corporate systems.
- Limited Internet access only.
- Subject to monitoring and usage controls.

Operational Wireless Networks

- Wireless networks supporting railway operations shall:
- Use enhanced security controls.
- Restrict access to authorized operational personnel.
- Be monitored continuously.

Wireless Device Controls

- Only approved devices may connect to EDRSC wireless networks.
- The organization may implement:
- Network Access Control (NAC)
- Device authentication
- Endpoint compliance verification

Wireless Monitoring

- Periodic wireless security assessments shall be conducted to identify:
- Rogue access points
- Unauthorized devices
- Weak configurations
- Security vulnerabilities

9.5 Secure Remote Connectivity

Policy Statement

- Remote connectivity services shall be secured to protect EDRSC information systems, cloud services, and railway operational environments from unauthorized access and cyber threats.

Approved Remote Access Methods

- Authorized users shall connect through:
- Secure VPN services
- Approved remote access gateways
- Secure cloud access platforms
- Direct access to internal systems from the Internet is prohibited unless specifically approved.

VPN Requirements

- VPN services shall:
- Use strong encryption.
- Require Multi-Factor Authentication (MFA).
- Support centralized monitoring.
- Comply with approved security standards.

Access Restrictions

- Remote access permissions shall:

- Be approved by management.
- Be granted based on business need.
- Be reviewed periodically.
- Be revoked when no longer required.

Remote Access Logging

- Remote connectivity systems shall record:
- Login attempts
- Connection times
- Source locations
- Authentication failures
- Administrative activities

Operational Technology Remote Access

- Remote access to:
- Signaling systems
- Train control systems
- SCADA systems
- Communications infrastructure
- shall:
- Be limited to authorized personnel.
- Require management approval.
- Use MFA and encrypted connections.
- Be monitored continuously.
- Be logged for audit purposes.

Third-Party Remote Access

- Vendors and contractors shall:
- Obtain formal approval before remote access is granted.
- Use approved remote access mechanisms.
- Comply with EDRSC cybersecurity requirements.
- Have their activities monitored and logged.

Prohibited Activities

- The following are prohibited:
- Use of unauthorized remote access software.
- Sharing remote access credentials.
- Use of personal VPN services to access company systems.

- Circumvention of security controls.
- Unapproved direct connections to OT environments.

Compliance Monitoring

- The Information Security Team shall monitor remote connectivity activities and investigate suspicious access attempts or policy violations.

10. Endpoint Security

10.1 Device Security Requirements

Policy Statement

- Ethio-Djibouti Railway Share Company (EDRSC) shall implement and maintain security controls on all endpoint devices to protect information assets, operational technology (OT) environments, railway operations, and business systems from cyber threats and unauthorized access.

Scope

- This policy applies to:
- Desktop computers
- Laptops
- Servers
- Virtual machines
- Mobile devices
- Tablets
- Industrial workstations
- Engineering workstations
- OT-connected devices
- Company-owned and approved third-party devices

Device Security Requirements

- All endpoint devices shall:
- Be registered in the EDRSC Asset Inventory.
- Be configured according to approved security standards.
- Use organization-approved operating systems.
- Be protected by authentication controls.
- Be maintained through regular updates and patching.
- Be monitored by centralized security management tools.
- Be protected from unauthorized access and modification.

Secure Configuration

- The IT Department shall implement secure baseline configurations that include:
- Removal of unnecessary software and services.
- Secure account configurations.
- Strong password policies.
- Logging and auditing controls.
- Access restrictions.
- Secure network settings.

Endpoint Hardening

- All devices shall be hardened through:
- Disabling unnecessary ports and protocols.
- Restricting administrator access.
- Disabling default accounts where possible.
- Limiting execution of unauthorized applications.
- Applying secure configuration standards.

Endpoint Monitoring

- Critical endpoint devices shall be monitored for:
- Security events
- Unauthorized software installation
- Malware activity
- Configuration changes
- Suspicious user activity

Device Ownership and Accountability

- Users are responsible for:
- Protecting assigned devices.
- Preventing unauthorized use.
- Reporting lost, stolen, or compromised devices immediately.
- Complying with EDRSC security requirements.

OT Endpoint Security

- Devices connected to:
- Signaling systems
- Train control systems
- SCADA environments

- Railway communication systems
- shall be subject to enhanced security controls and continuous monitoring.

10.2 Anti-Malware Protection

Policy Statement

- EDRSC shall deploy anti-malware and endpoint protection solutions to prevent, detect, contain, and respond to malicious software threats.

- **Protection Requirements**

- Approved anti-malware software shall be installed on:
- Workstations
- Laptops
- Servers
- Mobile devices where applicable
- Virtual environments

Anti-Malware Controls

- Solutions shall provide:
- Real-time protection
- Malware detection
- Behavioral monitoring
- Threat intelligence updates
- Quarantine capabilities
- Automated alerting

Signature Updates

- Anti-malware signatures shall:
- Update automatically.
- Be monitored centrally.
- Be verified regularly.

Scheduled Scanning

- The IT Department shall implement:
- Daily signature updates
- Weekly full-system scans
- Continuous real-time monitoring

Detection and Response

- When malware is detected:
- The affected device shall be isolated.
- The Information Security Team shall be notified.
- Incident response procedures shall be initiated.
- Malware shall be removed or contained.
- Recovery actions shall be documented.

User Responsibilities

- Users shall:
- Not disable endpoint protection software.
- Report suspicious system behavior immediately.
- Avoid downloading software from unapproved sources.
- Follow safe browsing and email practices.

OT Environment Considerations

- For OT systems where traditional anti-malware solutions cannot be installed:
- Compensating controls shall be implemented.
- Network monitoring shall be enhanced.
- System integrity monitoring shall be conducted.
- Security assessments shall be performed regularly.

10.3 Patch and Vulnerability Management

Policy Statement

- EDRSC shall maintain a structured Patch and Vulnerability Management Program to ensure timely identification, assessment, remediation, and monitoring of vulnerabilities affecting information systems and operational technology environments.

Objectives

- The program shall:
- Reduce exposure to cyber threats.
- Improve system security.
- Support business continuity.
- Protect railway operational systems.
- Maintain compliance requirements.

Vulnerability Identification

- Vulnerability management activities shall include:
- Automated vulnerability scanning.
- Configuration reviews.
- Security assessments.
- Threat intelligence monitoring.
- Penetration testing.
- Vendor security notifications.

Patch Management Requirements

- All supported operating systems, applications, firmware, and network devices shall receive security updates according to risk classifications.

Patching Timeframes

Vulnerability Severity	Remediation Target
Critical	Within 15 Days
High	Within 30 Days
Medium	Within 60 Days
Low	Within 90 Days

Testing Requirements

- Security patches shall be:
- Evaluated for operational impact.
- Tested before deployment where practical.
- Approved according to change management procedures.

Operational Technology Patch Management

- Patches affecting:
- Signaling systems
- SCADA systems
- Train control systems
- Operational communication systems
- shall undergo:
- Operational risk assessment.
- Safety review.
- Controlled testing.

- Change approval procedures.

Vulnerability Tracking

- The Information Security Team shall maintain records of:
- Vulnerabilities identified.
- Severity ratings.
- Remediation activities.
- Exception approvals.
- Validation results.

Exception Management

- Where immediate patching is not feasible:
- Risk assessments shall be conducted.
- Compensating controls shall be implemented.
- Management approval shall be obtained.
- Review dates shall be established.

10.4 Mobile Device Security

Policy Statement

- EDRSC shall protect mobile devices used to access organizational information, systems, and services from unauthorized access, loss, theft, and cyber threats.

Scope

- This policy applies to:
- Smartphones
- Tablets
- Company-owned mobile devices
- Approved Bring Your Own Device (BYOD) devices
- Mobile devices used by contractors and third parties

Mobile Device Requirements

- Devices accessing EDRSC resources shall:
- Be approved by the IT Department.
- Use supported operating systems.
- Be protected with PINs, passwords, or biometrics.
- Have encryption enabled.

- Be capable of remote wipe functionality.
- Be configured according to security standards.

Mobile Device Management (MDM)

- EDRSC may implement Mobile Device Management (MDM) solutions to:
- Enforce security settings.
- Manage application usage.
- Monitor compliance.
- Remotely lock or wipe devices.
- Control access to corporate resources.

Application Security

- Users shall:
- Install applications only from approved sources.
- Avoid untrusted applications.
- Remove unauthorized applications when instructed.

Lost or Stolen Devices

- Users must immediately report:
- Lost devices.
- Stolen devices.
- Suspected compromises.
- The IT Department shall:
- Disable access credentials.
- Initiate remote lock or wipe procedures where appropriate.
- Assess potential information exposure.

Mobile Access Controls

- Access to corporate resources from mobile devices shall require:
- Authentication controls.
- MFA where applicable.
- Encrypted communication.
- Compliance with security policies.

Data Storage on Mobile Devices

- Confidential and Restricted information stored on mobile devices shall:
- Be minimized where possible.

- Be encrypted.
- Be protected against unauthorized access.
- Be removed when no longer required.

International Travel

- Personnel traveling with company devices shall:
- Follow approved travel security procedures.
- Protect devices against theft and unauthorized inspection.
- Report any security incidents immediately.

11. Cloud Security

11.1 Cloud Governance

Policy Statement

- Ethio-Djibouti Railway Share Company (EDRSC) shall establish and maintain a Cloud Security Governance Framework to ensure the secure adoption, management, operation, and monitoring of cloud services supporting business operations, information systems, and railway services.
- Cloud services shall be managed in accordance with EDRSC cybersecurity policies, risk management requirements, regulatory obligations, and contractual commitments.

Objectives

- Cloud governance shall ensure:
- Secure use of cloud technologies.
- Protection of organizational information assets.
- Compliance with legal and regulatory requirements.
- Effective risk management.
- Business continuity and operational resilience.
- Accountability for cloud resources and data.

Governance Requirements

- The Chief Digital Officer (CDO) shall oversee cloud governance and ensure:
- Cloud usage is approved and documented.
- Cloud risks are assessed before implementation.
- Security responsibilities are clearly defined.
- Cloud controls are monitored and reviewed regularly.
- Security incidents are managed appropriately.

Cloud Service Approval

- Prior to adopting any cloud service, EDRSC shall perform:
- Business justification review.
- Cybersecurity risk assessment.
- Privacy impact assessment, where applicable.
- Compliance review.
- Vendor security assessment.
- Management approval.

Shared Responsibility Model

- EDRSC shall clearly define and document responsibilities between:
- Cloud Service Providers (CSPs)
- EDRSC Management
- System Owners
- Information Security Team
- Users
- Cloud security responsibilities shall be communicated to all stakeholders.

Cloud Asset Inventory

- The IT Department shall maintain an inventory of:
- Cloud platforms
- Cloud applications
- Cloud-hosted databases
- Storage services
- Virtual machines
- SaaS subscriptions
- Cloud administrators

Prohibited Activities

- The following are prohibited:
- Use of unauthorized cloud services ("Shadow IT").
- Storage of Restricted information in unapproved cloud environments.
- Deployment of cloud solutions without security review.
- Sharing cloud credentials with unauthorized users.

11.2 Cloud Service Provider Requirements

Policy Statement

- All Cloud Service Providers (CSPs) engaged by EDRSC shall demonstrate appropriate cybersecurity, privacy, operational resilience, and compliance capabilities before being approved for use.

Provider Assessment Requirements

- Cloud Service Providers shall undergo:
- Security due diligence review.
- Risk assessment.
- Compliance assessment.
- Contractual review.
- Technical evaluation.

Minimum Security Requirements

- Cloud Service Providers shall demonstrate:
- Information security governance programs.
- Secure access controls.
- Multi-Factor Authentication (MFA) capabilities.
- Encryption capabilities.
- Vulnerability management processes.
- Security monitoring capabilities.
- Incident response procedures.
- Backup and recovery capabilities.

Preferred Security Certifications

- Providers should maintain certifications such as:
- ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 27018
- SOC 1
- SOC 2
- PCI-DSS (where applicable)

Contractual Requirements

- Cloud provider contracts shall include:
- Security obligations.

- Data ownership provisions.
- Data privacy requirements.
- Service level agreements (SLAs).
- Incident notification requirements.
- Business continuity commitments.
- Audit rights.
- Secure termination requirements.

Security Incident Notification

- Cloud providers shall notify EDRSC of security incidents affecting EDRSC data or services:
- Immediately upon discovery of critical incidents.
- Within contractual notification timeframes.
- With sufficient details to support response activities.

Provider Performance Reviews

- Cloud providers shall be reviewed periodically to assess:
- Security performance.
- Compliance status.
- Service reliability.
- Incident history.
- Contractual obligations.

11.3 Cloud Access Security Controls

Policy Statement

- Access to cloud services shall be authorized, monitored, and controlled to prevent unauthorized access and misuse of cloud resources.

Identity and Access Management

- Cloud environments shall integrate with EDRSC Identity and Access Management (IAM) controls where feasible.

Access Control Requirements

- Cloud access shall be based on:
- Business need.
- Role-Based Access Control (RBAC).
- Least privilege principles.

- Segregation of duties.

Authentication Controls

- All cloud services shall require:
- Unique user accounts.
- Strong password policies.
- Multi-Factor Authentication (MFA) for privileged users.
- MFA for remote access users.

Administrative Access Controls

- Administrative access to cloud environments shall:
- Be limited to authorized personnel.
- Be approved by management.
- Be monitored continuously.
- Be logged for audit purposes.

Privileged Account Management

- Privileged cloud accounts shall:
- Use dedicated administrator accounts.
- Prohibit shared credentials.
- Require MFA.
- Be reviewed quarterly.

Session Management

- Cloud systems shall implement:
- Automatic session timeout.
- Account lockout controls.
- Re-authentication for sensitive activities.

Logging and Monitoring

- Cloud access activities shall be logged, including:
- Authentication events.
- Administrative actions.
- Access failures.
- Privilege changes.
- Configuration modifications.
- Logs shall be retained according to EDRSC logging requirements.

Third-Party Access

- Third-party cloud access shall:
- Be formally approved.
- Be restricted to authorized activities.
- Be monitored and reviewed regularly.
- Be revoked when no longer needed.

11.4 Data Protection in Cloud Environments

Policy Statement

- EDRSC shall protect information stored, processed, transmitted, or backed up within cloud environments according to its classification and sensitivity.

Data Classification Requirements

- Data hosted in cloud environments shall maintain the same classification and protection requirements that apply to on-premises environments.
- The following classifications apply:
- Public
- Internal
- Confidential
- Restricted

Data Storage Controls

- Cloud-hosted data shall:
- Be stored only in approved cloud environments.
- Be protected by appropriate security controls.
- Be included in backup and recovery processes.
- Be monitored for unauthorized access.

Data Encryption

Encryption at Rest

- Confidential and Restricted information stored in cloud environments shall be encrypted using approved encryption standards.
- Examples include:
- Cloud storage services
- Databases

- Backup repositories
- Virtual machine storage

Encryption in Transit

- Sensitive information transmitted between:
- Users and cloud services
- Cloud services and on-premises environments
- Cloud platforms and third parties
- shall use secure encrypted protocols such as:
- HTTPS
- TLS
- IPSec VPN

Key Management

- Encryption key management shall:
- Be controlled and documented.
- Restrict access to authorized personnel.
- Support backup and recovery.
- Include key rotation procedures.
- Protect cryptographic keys from unauthorized disclosure.

Backup and Recovery

- Cloud-hosted data shall:
- Be backed up based on business requirements.
- Support disaster recovery objectives.
- Be periodically tested for recoverability.
- Be protected from unauthorized modification or deletion.

Data Retention and Disposal

- Cloud-stored information shall:
- Follow EDRSC retention schedules.
- Be disposed of securely when no longer required.
- Be removed from cloud environments upon service termination where appropriate.

Cross-Border Data Transfers

- Cloud providers that store or process data outside Ethiopia or Djibouti shall:
- Obtain appropriate approvals.

- Meet legal and regulatory requirements.
- Implement appropriate security safeguards.
- Conduct risk assessments prior to transfer.

Data Loss Prevention (DLP)

- Cloud environments shall support controls to:
- Prevent unauthorized data sharing.
- Detect data leakage.
- Monitor sensitive information movement.
- Restrict unauthorized downloads and transfers.

Cloud Security Monitoring

- The Information Security Team shall monitor cloud environments for:
- Unauthorized access attempts.
- Configuration weaknesses.
- Security incidents.
- Compliance violations.
- Unusual user behavior.

Incident Response

- Cloud security incidents shall:
- Be reported immediately.
- Follow EDRSC Incident Response procedures.
- Be investigated and documented.
- Include coordination with the Cloud Service Provider where necessary.

Compliance

- Failure to comply with this Cloud Security Policy may result in:
- Suspension of cloud access privileges.
- Disciplinary action.
- Contract termination.
- Legal or regulatory penalties where applicable.

12. Application Security

12.1 Secure Software Development Lifecycle (SSDLC)

Policy Statement

- Ethio-Djibouti Railway Share Company (EDRSC) shall implement a Secure Software Development Lifecycle (SSDLC) to ensure security is integrated into the planning, design, development, testing, deployment, operation, and maintenance of all applications and systems.
- The SSDLC shall apply to:
- Internally developed applications
- Customized applications
- Mobile applications
- Web applications
- Cloud-based applications
- OT and railway operational applications
- Third-party software implementations

SSDLC Objectives

- The SSDLC shall:
- Reduce application security risks.
- Identify vulnerabilities early in development.
- Protect business and railway operational systems.
- Ensure regulatory compliance.
- Improve software quality and resilience.

SSDLC Phases

Requirements and Planning

- Security requirements shall be identified and documented during project initiation.
- Activities include:
- Business requirements review
- Security requirements definition
- Compliance assessment
- Privacy impact assessment
- Risk assessment
- Threat modeling

Design

- Application designs shall incorporate security controls including:
- Authentication mechanisms

- Authorization controls
- Encryption requirements
- Logging requirements
- Data protection controls
- Secure integration controls

Development

- Developers shall follow approved secure coding standards and development procedures.

Testing

- Applications shall undergo security testing before deployment.

Deployment

- Applications shall be deployed using approved release management and change control procedures.

Maintenance

- Applications shall be continuously monitored, updated, and maintained throughout their lifecycle.

Security by Design

- All applications shall incorporate:
- Least privilege principles
- Secure defaults
- Defense-in-depth controls
- Secure authentication methods
- Data protection mechanisms

Third-Party Software

- Before procurement or deployment, third-party software shall undergo:
- Security assessment
- Vendor review
- Risk evaluation
- Licensing validation
- Security testing where appropriate

Operational Technology (OT) Applications

- Applications supporting:

- Signaling systems
- Train control systems
- SCADA environments
- Railway operations
- shall undergo enhanced security reviews due to their operational and safety impact.

12.2 Secure Coding Practices

Policy Statement

- EDRSC shall ensure that software development activities follow secure coding principles to minimize vulnerabilities and reduce cybersecurity risks.

Secure Coding Requirements

- Developers shall:
- Follow approved coding standards.
- Use secure development frameworks.
- Validate inputs and outputs.
- Implement proper error handling.
- Protect sensitive information.
- Avoid insecure coding practices.

Input Validation

- Applications shall validate all user-supplied input to prevent:
- SQL Injection
- Command Injection
- Cross-Site Scripting (XSS)
- Buffer Overflow attacks
- Code Injection attacks

Authentication and Authorization

- Applications shall:
- Use approved authentication mechanisms.
- Enforce strong password requirements.
- Support MFA where applicable.
- Apply role-based authorization controls.
- Restrict access based on business requirements.

Session Management

- Applications shall:
- Generate secure session identifiers.
- Automatically terminate inactive sessions.
- Protect session information from unauthorized access.

Data Protection

- Sensitive information shall:
- Be encrypted during transmission.
- Be encrypted while stored when required.
- Not be hardcoded into applications.
- Be protected from unauthorized disclosure.

Error Handling

- Applications shall:
- Avoid exposing sensitive information in error messages.
- Log security-related events securely.
- Prevent disclosure of system configurations or source code details.

Secure Use of APIs

- All APIs shall:
- Require authentication.
- Validate requests.
- Encrypt communications.
- Restrict unauthorized access.
- Maintain audit logs.

Source Code Protection

- Source code repositories shall:
- Be access-controlled.
- Be backed up regularly.
- Use version control mechanisms.
- Maintain audit trails of changes.

Prohibited Practices

- Developers shall not:
- Hardcode passwords or encryption keys.

- Use unsupported libraries or software components.
- Disable security controls without approval.
- Store sensitive information in plaintext.

12.3 Application Testing and Reviews

Policy Statement

- All applications shall undergo security testing and reviews to identify and remediate vulnerabilities before deployment and throughout their operational lifecycle.

Security Testing Requirements

- Applications shall be tested before:
- Initial deployment
- Major upgrades
- Significant code changes
- Integration with critical systems

Security Review Types

Code Reviews

- Source code shall undergo peer review to identify:
- Security weaknesses
- Coding errors
- Compliance violations
- Quality issues

Static Application Security Testing (SAST)

- Applications shall be scanned for vulnerabilities within source code during development.

Dynamic Application Security Testing (DAST)

- Applications shall be tested while running to identify exploitable weaknesses.

Vulnerability Assessments

- Applications shall be assessed for known vulnerabilities and configuration weaknesses.

Penetration Testing

- Critical applications shall undergo penetration testing before production deployment and at least annually thereafter.

Security Testing Coverage

- Testing shall assess:
- Authentication controls
- Authorization controls
- Input validation
- Data protection mechanisms
- Session management
- API security
- Logging capabilities
- Configuration management

Risk-Based Testing

- Applications supporting:
- Railway operations
- Freight management
- Passenger services
- Financial systems
- Human resource systems
- shall receive enhanced security testing.

Vulnerability Remediation

- Identified vulnerabilities shall be remediated according to the following targets:

Severity	Remediation Timeline
Critical	15 Days
High	30 Days
Medium	60 Days
Low	90 Days

Exception Handling

- Unresolved vulnerabilities shall:
- Be documented.
- Undergo risk assessment.

- Have compensating controls applied.
- Receive management approval.

12.4 Change Management

Policy Statement

- EDRSC shall implement a formal change management process to ensure that changes to applications, systems, infrastructure, and operational technology environments are controlled, authorized, tested, documented, and implemented securely.

Objectives

- The change management process shall:
- Reduce operational risk.
- Prevent unauthorized modifications.
- Maintain system integrity.
- Protect railway operations.
- Ensure accountability and traceability.

Scope

- This process applies to:
- Application changes
- Software updates
- Configuration changes
- Infrastructure modifications
- Security control changes
- Database changes
- Cloud service changes
- OT system changes

Change Categories

Standard Changes

- Pre-approved, low-risk changes performed routinely.
- Examples:
- Scheduled patching
- Routine maintenance
- Approved configuration updates

Normal Changes

- Changes requiring review, testing, and approval before implementation.
- Examples:
- Application enhancements
- Infrastructure upgrades
- New functionality deployment

Emergency Changes

- Changes required to address:
- Critical vulnerabilities
- System outages
- Security incidents
- Safety risks
- Emergency changes shall be reviewed after implementation.

Change Request Requirements

- Change requests shall include:
- Description of the change
- Business justification
- Risk assessment
- Impact assessment
- Rollback plan
- Testing results
- Implementation schedule

Approval Requirements

- Changes shall be approved by:
- System Owner
- Business Owner
- IT Manager
- Information Security Team (for security-impacting changes)

Testing Requirements

- Changes shall be tested before implementation to verify:
- Functionality
- Security
- Compatibility

- Performance
- Recovery capability

Production Deployment

- Deployment activities shall:
- Follow approved procedures.
- Be documented.
- Be monitored.
- Include rollback capability.

Segregation of Duties

- Where practical:
- Developers shall not approve their own changes.
- Testers shall be independent from developers.
- Production deployments shall be independently authorized.

Operational Technology (OT) Change Management

- Changes affecting:
- Signaling systems
- Train control systems
- SCADA systems
- Railway communication infrastructure
- shall require:
- Operational risk assessment
- Safety impact assessment
- Management approval
- Security review
- Controlled implementation windows

Documentation and Audit Trail

- All changes shall be documented and retained for audit purposes, including:
- Requests
- Approvals
- Testing evidence
- Deployment records
- Rollback activities
- Post-implementation reviews

Post-Implementation Review

- Significant changes shall undergo review to confirm:
- Objectives were achieved.
- No unexpected impacts occurred.
- Security requirements were met.
- Lessons learned are documented.

13. Security Monitoring and Logging

13.1 Audit Logging Requirements

Policy Statement

- Ethio-Djibouti Railway Share Company (EDRSC) shall generate, collect, protect, monitor, and retain audit logs to support cybersecurity operations, incident investigations, regulatory compliance, operational monitoring, and forensic analysis.
- Audit logs shall provide sufficient information to detect unauthorized activities, reconstruct events, support investigations, and demonstrate accountability.

Objectives

- Audit logging shall:
- Detect security incidents and suspicious activities.
- Support incident response investigations.
- Provide accountability for user actions.
- Facilitate compliance and audit activities.
- Support monitoring of business and railway operational systems.

Systems Subject to Logging

- Logging shall be enabled on:
- Servers
- Workstations
- Network devices
- Firewalls
- Cloud services
- Databases
- Applications
- Operating systems
- VPN systems

- Active Directory services
- Email systems
- Operational Technology (OT) systems
- Signaling systems
- SCADA systems
- Railway communication systems

Audit Events to be Logged

- The following events shall be logged, where technically feasible:

User Authentication Events

- Successful logins
- Failed login attempts
- Account lockouts
- Password changes
- Privilege escalations
- MFA events

Access Control Events

- User account creation
- User account modification
- User account deletion
- Permission changes
- Role assignments

Administrative Activities

- System configuration changes
- Firewall rule modifications
- Security policy changes
- Software installation and removal
- Administrative access activities

Security Events

- Malware detections
- Intrusion attempts
- Security alerts
- Antivirus events

- Endpoint Detection and Response (EDR) events

Network Events

- VPN connections
- Firewall denials
- Network anomalies
- Remote access activity
- Wireless access events

Application Events

- Application access
- Transaction failures
- Privileged actions
- Data modification activities

OT and Railway Operational Events

- Signaling system access
- SCADA system activity
- Control system modifications
- Communication system events
- Unauthorized access attempts to railway operational environments

Log Content Requirements

- Audit logs shall include, where available:
- Date and time
- User identifier
- System identifier
- Source IP address
- Event type
- Event description
- Result of the action
- Device or system affected

Time Synchronization

- All systems generating audit logs shall synchronize with approved time sources to ensure accurate event correlation and investigation.

Protection of Audit Logs

- Audit logs shall be protected against:
- Unauthorized access
- Modification
- Deletion
- Disclosure
- Only authorized personnel shall have access to log management functions.

13.2 Security Monitoring

Policy Statement

- EDRSC shall continuously monitor information systems, networks, cloud environments, and operational technology systems to detect, analyze, and respond to cybersecurity threats and security incidents.

Monitoring Objectives

- Security monitoring shall:
- Detect malicious activity.
- Identify security incidents.
- Protect critical railway operations.
- Support incident response.
- Improve organizational cybersecurity posture.

Monitoring Coverage

- Security monitoring shall include:

Information Technology (IT) Systems

- Servers
- Endpoints
- Databases
- Business applications
- Identity management systems

Network Infrastructure

- Routers
- Switches

- Firewalls
- VPN systems
- Wireless networks

Cloud Services

- SaaS environments
- Cloud platforms
- Cloud storage solutions
- Virtual servers

Operational Technology (OT) Systems

- Signaling systems
- Train control systems
- SCADA systems
- Railway communications networks
- Power management systems

Security Events Subject to Monitoring

- The Information Security Team shall monitor:
- Unauthorized access attempts
- Malware activity
- Privileged account usage
- Unusual user behavior
- Data exfiltration attempts
- Network anomalies
- System integrity violations
- Policy violations
- Cybersecurity threat intelligence indicators

Alert Management

- Security alerts shall be:
- Classified according to severity.
- Investigated promptly.
- Escalated according to incident response procedures.
- Documented and tracked.

Monitoring Responsibilities

- The Information Security Team shall:
- Review security events regularly.
- Investigate suspicious activities.
- Escalate incidents as required.
- Maintain monitoring tools and configurations.
- Produce security monitoring reports.

Critical Incident Escalation

- The following events shall be immediately escalated:
- Data breaches
- Ransomware infections
- OT security incidents
- Compromise of privileged accounts
- Threats impacting railway operations
- Attacks affecting safety-critical systems

13.3 Security Information and Event Management (SIEM)

Policy Statement

- EDRSC shall implement and maintain a Security Information and Event Management (SIEM) capability to centrally collect, correlate, analyze, and retain security events from critical systems and infrastructure.

SIEM Objectives

- The SIEM platform shall:
- Centralize log management.
- Detect cybersecurity threats.
- Support incident investigation.
- Correlate security events.
- Improve threat visibility.
- Support compliance reporting.

Log Sources

- The SIEM shall collect logs from:

Infrastructure Systems

- Firewalls
- Routers
- Switches
- Wireless controllers

Endpoint Systems

- Workstations
- Servers
- Endpoint protection systems
- EDR solutions

Security Solutions

- IDS/IPS systems
- DLP solutions
- Vulnerability scanners
- Security gateways

Identity Systems

- Active Directory
- Identity providers
- Authentication services
- MFA systems

Cloud Environments

- Microsoft 365
- Azure services
- Cloud security platforms
- Cloud applications

OT Systems

- SCADA systems
- Signaling systems
- Train control systems
- Industrial firewalls
- Railway communication systems

Event Correlation

- The SIEM shall be configured to detect:
- Multiple failed login attempts
- Privilege escalation activity
- Malware infections
- Lateral movement attempts
- Unauthorized configuration changes
- Data exfiltration activities
- Insider threats
- OT system anomalies

Security Use Cases

- The Information Security Team shall maintain SIEM use cases for:
- Account compromise detection
- Phishing attacks
- Ransomware activity
- Unauthorized remote access
- Critical system modifications
- OT cybersecurity incidents

SIEM Administration

- SIEM access shall:
- Be restricted to authorized personnel.
- Require MFA.
- Be logged and monitored.
- Be reviewed quarterly.

Reporting

- The SIEM platform shall generate:
- Security dashboards
- Incident reports
- Executive cybersecurity summaries
- Compliance reports
- Threat intelligence reports

13.4 Log Retention

Policy Statement

- EDRSC shall retain logs for a sufficient period to support operational requirements, security investigations, forensic analysis, legal obligations, regulatory compliance, and audit requirements.

Log Retention Requirements

- All logs shall be retained according to their classification, importance, and legal requirements.

Log Type	Minimum Retention Period
Security Logs	12 Months
Firewall Logs	12 Months
VPN Logs	12 Months
Authentication Logs	12 Months
Active Directory Logs	12 Months
Endpoint Protection Logs	12 Months
Cloud Security Logs	12 Months
Incident Investigation Logs	5 Years
Audit Logs	5 Years
OT System Logs	24 Months
Signaling System Logs	24 Months
SCADA Logs	24 Months
Railway Operational Security Logs	24 Months

Long-Term Archiving

- Where required for legal, regulatory, operational, or investigative purposes, logs may be archived beyond minimum retention periods.
- Archived logs shall:
- Remain protected from alteration.
- Be recoverable upon request.
- Maintain integrity and authenticity.
- Be accessible only to authorized personnel.

Log Storage Security

- Log repositories shall:
- Use secure storage mechanisms.

- Implement access controls.
- Encrypt sensitive log data.
- Support backup and recovery.

Log Disposal

- At the end of retention periods, logs shall be securely disposed of according to EDRSC records management and data disposal requirements.

Log Review Requirements

- Critical logs shall be reviewed:
- Daily for high-risk systems.
- Weekly for standard systems.
- Immediately following significant security events.

Compliance Verification

- The Information Security Team and Internal Audit function shall periodically verify:
- Log retention compliance.
- Log integrity.
- Monitoring effectiveness.
- SIEM configuration effectiveness.

14. Vulnerability Management

14.1 Vulnerability Assessments

Policy Statement

- Ethio-Djibouti Railway Share Company (EDRSC) shall establish and maintain a Vulnerability Management Program to identify, assess, prioritize, and manage vulnerabilities affecting information assets, information technology (IT) systems, operational technology (OT) systems, applications, networks, cloud environments, and railway operational infrastructure.
- The objective is to reduce the organization's exposure to cyber threats and improve the security and resilience of business and railway operations.

Objectives

- Vulnerability assessments shall be conducted to:
- Identify security weaknesses before they are exploited.
- Assess risks to critical systems and assets.
- Support compliance with cybersecurity standards.
- Improve the effectiveness of security controls.
- Reduce business and operational risks.

Scope

- Vulnerability assessments shall include:

Information Technology Systems

- Servers
- Workstations
- Laptops
- Databases
- Applications
- Network devices
- Active Directory
- Email systems

Cloud Services

- Cloud-hosted infrastructure
- SaaS applications
- Cloud storage services
- Virtual environments

Operational Technology Systems

- Signaling systems
- Train control systems
- SCADA systems
- Power management systems
- Railway communication systems
- Operations Control Center infrastructure

Vulnerability Identification Methods

- EDRSC shall utilize:
- Automated vulnerability scanning tools
- Configuration reviews
- Security assessments
- Threat intelligence feeds
- Vendor security advisories
- Penetration testing
- Internal audits
- External audits

Assessment Frequency

Asset Type	Minimum Frequency
Internet-Facing Systems	Monthly
Critical Business Systems	Quarterly
Network Infrastructure	Quarterly
Cloud Environments	Quarterly
OT Systems	Semi-Annually
Signaling and Train Control Systems	Annually or Following Major Changes
High-Risk Assets	As Required

Vulnerability Classification

- Vulnerabilities shall be classified based on severity and business impact.

Severity Level	Description
Critical	Immediate risk of compromise or service disruption
High	Significant risk requiring urgent remediation
Medium	Moderate risk requiring planned remediation
Low	Limited risk requiring routine remediation

Vulnerability Assessment Reporting

- Assessment reports shall include:
- Date of assessment
- Systems reviewed
- Vulnerabilities identified
- Severity ratings
- Risk analysis
- Recommended corrective actions
- Responsible owners
- Target remediation dates
- Assessment results shall be maintained in the organization's Vulnerability Register.

14.2 Penetration Testing

Policy Statement

- EDRSC shall conduct penetration testing to evaluate the effectiveness of security controls and identify vulnerabilities that may be exploited by malicious actors.
- Penetration testing shall simulate real-world attack scenarios against EDRSC systems and infrastructure.

Objectives

- Penetration testing shall:
- Identify exploitable vulnerabilities.
- Assess the effectiveness of security controls.
- Validate vulnerability remediation efforts.
- Support regulatory and compliance requirements.
- Strengthen overall cybersecurity posture.

Scope

- Penetration testing may cover:

External Testing

- Internet-facing systems
- Network perimeter security
- Public-facing applications
- Cloud services

Internal Testing

- Internal networks
- Servers
- Applications
- Databases
- Identity management systems

Application Security Testing

- Web applications
- Mobile applications
- APIs
- Cloud applications

Wireless Security Testing

- Corporate wireless networks
- Guest wireless networks
- Operational wireless systems

Operational Technology Testing

- Where operationally safe and approved, testing may include:
- Signaling systems
- Railway communication systems
- SCADA environments
- Control center networks
- Testing involving safety-critical systems shall follow strict operational safeguards and require executive approval.

Penetration Testing Frequency

System Type	Minimum Frequency
Internet-Facing Infrastructure	Annually
Critical Applications	Annually
Cloud Services	Annually
Network Infrastructure	Annually
OT Environments	Every Two Years or After Major Changes
Following Major System Changes	As Required

Testing Requirements

- Penetration testing shall:
- Be performed by qualified personnel.
- Follow approved methodologies.
- Be authorized before execution.
- Be documented and approved.
- Include validation of identified vulnerabilities.

Test Reporting

- Penetration test reports shall include:
- Executive summary
- Scope of testing
- Methodology used
- Findings and evidence
- Risk ratings
- Exploitation results
- Recommendations
- Management response
- Reports shall be classified as **Restricted** information.

Retesting

- Critical and High-risk findings shall be retested after remediation to verify effectiveness.

14.3 Remediation Requirements

Policy Statement

- EDRSC shall ensure identified vulnerabilities are remediated or appropriately managed within defined timeframes based on risk, severity, business impact, and operational requirements.

Remediation Responsibilities

Information Security Team

- Responsible for:
- Tracking vulnerabilities.
- Monitoring remediation efforts.
- Reporting remediation status.
- Validating corrective actions.

System Owners

- Responsible for:
- Reviewing identified vulnerabilities.
- Implementing corrective actions.
- Coordinating remediation activities.
- Reporting remediation progress.

IT and OT Administrators

- Responsible for:
- Applying security patches.
- Correcting configuration weaknesses.
- Implementing compensating controls.
- Supporting remediation verification.

Remediation Timeframes

Severity	Remediation Target
Critical	Within 15 Days
High	Within 30 Days
Medium	Within 60 Days
Low	Within 90 Days

- For vulnerabilities affecting safety-critical railway operations, remediation shall be prioritized and completed as soon as operationally feasible.

Remediation Methods

- Corrective actions may include:
- Security patch deployment
- Software upgrades
- Configuration changes
- Access control improvements
- Network segmentation
- Security monitoring enhancements
- System replacement
- Compensating security controls

Verification and Validation

- Following remediation:

- Vulnerabilities shall be re-scanned.
- Security controls shall be tested.
- Evidence of remediation shall be documented.
- Results shall be reviewed by the Information Security Team.

Exception Management

- Where remediation cannot be completed within required timeframes:
- A formal exception request must include:
- Business justification
- Risk assessment
- Compensating controls
- Risk owner approval
- Target remediation date
- Approval authority shall be:

Risk Level	Approval Authority
Low	Department Manager
Medium	Department Head
High	Chief Digital Officer (CDO)
Critical	CEO and Executive Management

-

Vulnerability Metrics and Reporting

- The Information Security Team shall maintain and report:
- Total vulnerabilities identified
- Open vulnerabilities by severity
- Remediation compliance rates
- Average remediation time
- Repeated vulnerabilities
- Critical vulnerabilities outstanding
- Penetration testing findings status
- Monthly reports shall be provided to management, and quarterly summaries shall be presented to Executive Management.

Compliance

- Failure to remediate identified vulnerabilities within approved timelines may result in:
- Escalation to management
- Risk acceptance review

- Audit findings
- Disciplinary action where negligence is identified

15. Incident Response Management

15.1 Incident Identification

- **Policy Statement**

- Ethio-Djibouti Railway Share Company (EDRSC) shall establish and maintain processes to identify cybersecurity incidents promptly to minimize disruption to business operations, railway services, information assets, and operational technology (OT) environments.
- Timely identification of security incidents is essential to reduce operational, financial, safety, legal, and reputational impacts.

Objectives

- Incident identification processes shall:
- Detect cybersecurity threats and attacks.
- Identify unauthorized access attempts.
- Detect malicious software activity.
- Protect railway operational systems.
- Support timely incident response and recovery.

Sources of Incident Identification

- Cybersecurity incidents may be identified through:

Security Monitoring Systems

- SIEM platforms
- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- Endpoint Detection and Response (EDR)
- Cloud Security Monitoring Tools

User Reporting

- Employees
- Contractors
- Vendors
- Customers

- External stakeholders

Security Assessments

- Vulnerability assessments
- Penetration tests
- Compliance audits
- Security reviews

Third-Party Notifications

- Service providers
- Government agencies
- Security partners
- Cyber threat intelligence providers

Examples of Security Incidents

Unauthorized Access

- Unauthorized login attempts
- Account compromise
- Privilege escalation
- Unauthorized remote access

Malware Incidents

- Viruses
- Worms
- Trojans
- Spyware
- Ransomware

Data Security Incidents

- Data breaches
- Data leakage
- Unauthorized disclosure
- Information theft

Network Security Incidents

- Denial-of-Service (DoS) attacks
- Network intrusions
- Suspicious network activity

Operational Technology Incidents

- Signaling system compromise
- SCADA system compromise
- Train control system attacks
- Communication system disruptions

Physical Security Incidents

- Theft of devices
- Lost laptops
- Unauthorized facility access

Incident Classification

- Incidents shall be classified according to severity.

Severity	Description
Critical	Major impact on railway safety, operations, or sensitive information
High	Significant operational or business impact
Medium	Limited impact with manageable disruption
Low	Minor event with minimal impact

15.2 Incident Reporting

Policy Statement

- All employees, contractors, consultants, vendors, and third parties shall immediately report actual or suspected cybersecurity incidents affecting EDRSC information assets, systems, or operations.
- Failure to report incidents may increase organizational risk and may result in disciplinary action.

Reporting Requirements

- The following events shall be reported immediately:
- Suspected malware infections

- Phishing emails
- Unauthorized access attempts
- Data breaches
- Lost or stolen devices
- Suspicious user activity
- Network attacks
- Website defacement
- OT security events
- Safety-related cyber incidents

Reporting Channels

- Incidents may be reported through:

- **Security Operations Center (SOC)**

- Email: security@edrsc.et

- **Information Security Team**

- Direct reporting through approved channels.

Help Desk

- For initial escalation and triage.

Emergency Reporting

- Critical incidents affecting railway operations shall be reported immediately by telephone and escalated to the Incident Response Team.

Incident Report Information

- Reports should include:
- Name of reporter
- Date and time detected
- System affected
- Description of incident
- Screenshots or evidence where available
- Actions already taken
- Potential business or operational impact

Reporting Timeframes

Incident Type	Reporting Time
Critical	Immediately
High	Within 1 Hour
Medium	Within 4 Hours
Low	Within 24 Hours

Non-Retaliation

- Employees who report cybersecurity concerns in good faith shall not be subject to retaliation.

15.3 Incident Response Procedures

Policy Statement

- EDRSC shall establish a formal Incident Response Process to contain, investigate, eradicate, and manage cybersecurity incidents using a structured and coordinated approach.

Incident Response Team (IRT)

- The Incident Response Team shall include:
- Chief Digital Officer (CDO)
- Information Security Manager
- IT Manager
- Network Administrator
- System Administrators
- OT Operations Representatives
- Legal Representative
- Human Resources Representative
- Communications Officer
- Depending on the incident, additional personnel may be assigned.

Incident Response Lifecycle

Phase 1: Preparation

- EDRSC shall maintain:
- Incident response plans
- Response procedures
- Contact lists

- Communication plans
- Investigation tools
- Incident reporting mechanism

Phase 2: Identification

- Activities include:
- Reviewing alerts
- Validating incidents
- Assessing affected systems
- Determining incident severity

Phase 3: Containment

- Short-term containment may include:
- Disconnecting affected systems
- Blocking malicious IP addresses
- Disabling compromised accounts
- Isolating infected endpoints
- Long-term containment shall aim to prevent reinfection or recurrence.

Phase 4: Investigation and Analysis

- The Incident Response Team shall:
- Collect evidence
- Determine root cause
- Assess impact
- Identify attack vectors
- Preserve forensic evidence

Phase 5: Eradication

- Activities may include:
- Malware removal
- Patch deployment
- Password resets
- Removal of unauthorized accounts
- Closure of exploited vulnerabilities

- **Phase 6: Recovery**

- Systems shall be restored through controlled and verified processes.

- Recovery activities shall include:
- System restoration
- Service validation
- Monitoring for recurrence
- User notification where required

Incident Escalation Matrix

Severity	Escalation Authority
Critical	CEO, Executive Management, Board
High	CDO and Executive Management
Medium	Information Security Manager
Low	IT Operations Team

OT and Railway Operational Incidents

- Incidents affecting:
- Signaling systems
- Train control systems
- SCADA systems
- Operational communications
- shall receive immediate escalation and priority response due to potential safety implications.

15.4 Incident Recovery

Policy Statement

- EDRSC shall restore affected systems, services, and operations safely and efficiently following a cybersecurity incident while minimizing operational disruption and preventing recurrence.

Recovery Objectives

- Recovery activities shall:
- Restore normal operations.
- Verify system integrity.
- Protect critical information.
- Ensure railway operational safety.
- Reduce downtime and financial losses.

Recovery Activities

System Restoration

- Restore systems from:
- Approved backups
- Disaster recovery sites
- Recovery images

Validation and Testing

- Recovered systems shall be tested to confirm:
- Functionality
- Security controls
- Data integrity
- User access functionality
- Performance requirements

Operational Verification

- For railway operational systems:
- Signaling functions shall be validated.
- Control systems shall be confirmed operational.
- Communications systems shall be tested.
- Safety checks shall be completed before returning systems to production.

Recovery Prioritization

Priority	System Category
Priority 1	Train Control Systems
Priority 1	Signaling Systems
Priority 1	Communications Systems
Priority 2	Freight Operations Systems
Priority 2	Passenger Systems
Priority 3	Corporate Services

Business Continuity Integration

- Recovery activities shall align with:
- Business Continuity Plans (BCP)

- Disaster Recovery Plans (DRP)
- Emergency Response Procedures

15.5 Lessons Learned

Policy Statement

- EDRSC shall conduct post-incident reviews following cybersecurity incidents to identify lessons learned, improve security controls, and strengthen future response capabilities.

Objectives

- Lessons learned activities shall:
- Identify root causes.
- Improve incident response processes.
- Strengthen cybersecurity controls.
- Reduce future risks.
- Enhance organizational resilience.

Post-Incident Review Process

- Reviews shall normally occur within **ten (10) business days** after incident closure.
- Participants may include:
- Information Security Team
- IT Operations
- Incident Response Team
- Business Owners
- OT Operations Personnel
- Executive Management

Review Topics

- The review shall evaluate:
- Timeline of events
- Detection effectiveness
- Response effectiveness
- Communication effectiveness
- Impact assessment accuracy
- Recovery performance
- Control failures
- Root causes

Lessons Learned Report

- The report shall document:
- Incident summary
- Root cause analysis
- Business impact
- Operational impact
- Safety impact
- Actions taken
- Recommendations
- Corrective actions
- Responsible parties
- Target completion dates

Corrective Action Tracking

- Corrective actions shall be:
- Assigned to responsible owners.
- Tracked to completion.
- Verified by the Information Security Team.
- Reported to management.

Continuous Improvement

- Lessons learned findings shall be used to:
- Update security policies and procedures.
- Improve security monitoring capabilities.
- Strengthen employee awareness training.
- Enhance technical controls.
- Improve OT security measures.
- Update business continuity plans.
- Improve future incident response efforts.

Regulatory and Management Reporting

- Major incidents may require:
- Executive Management reporting.
- Board notification.
- Regulatory reporting.
- Customer or stakeholder notification, where legally required.

16. Business Continuity and Disaster Recovery

16.1 Business Continuity Planning

- **Policy Statement**

- Ethio-Djibouti Railway Share Company (EDRSC) shall establish, maintain, and regularly review a Business Continuity Management (BCM) program to ensure the continued delivery of critical railway, operational, administrative, and technology services during and after disruptive events.
- The Business Continuity Program shall support the resilience of railway operations, information systems, and critical business functions.

Objectives

- The Business Continuity Program shall:
- Ensure continuity of critical railway operations.
- Minimize disruption to passenger and freight services.
- Protect employees, customers, and assets.
- Maintain regulatory compliance.
- Reduce financial and operational impacts.
- Support rapid recovery following disruptions.

Scope

- Business Continuity Planning (BCP) shall apply to:
- Passenger operations
- Freight operations
- Railway control centers
- Signaling systems
- Communications systems
- Power and traction systems
- Information technology services
- Finance and administration functions
- Human resources services
- Customer service operations

Business Impact Analysis (BIA)

- EDRSC shall conduct a Business Impact Analysis (BIA) to:
- Identify critical business processes.
- Assess potential operational impacts.

- Determine recovery priorities.
- Define Recovery Time Objectives (RTOs).
- Define Recovery Point Objectives (RPOs).
- The BIA shall be reviewed at least annually or following major organizational changes.

Business Continuity Plans

- Each critical department shall maintain documented continuity plans that include:
- Critical activities and dependencies
- Roles and responsibilities
- Emergency contact information
- Alternative work arrangements
- Recovery procedures
- Escalation procedures
- Communication procedures

Crisis Management Team

- EDRSC shall establish a Crisis Management Team (CMT) consisting of:
- Chief Executive Officer (CEO)
- Chief Digital Officer (CDO)
- Operations Director
- Human Resources Manager
- Information Security Manager
- Communications Manager
- Railway Operations Representatives
- The Crisis Management Team shall coordinate organizational response during major disruptions.

Continuity Strategies

- Business continuity strategies may include:
- Alternative operating locations
- Remote working arrangements
- Redundant communication systems
- Backup operational facilities
- Vendor contingency arrangements
- Manual processing procedures
- High-availability technology solutions

Emergency Communications

- The organization shall maintain communication procedures for:

- Employees
- Customers
- Government authorities
- Railway regulators
- Vendors and suppliers
- Emergency response agencies

16.2 Disaster Recovery Planning

Policy Statement

- EDRSC shall maintain Disaster Recovery Plans (DRPs) to restore information systems, applications, data, and technology infrastructure following disruptive events affecting normal operations.

Objectives

- Disaster Recovery Planning shall ensure:
- Rapid restoration of critical systems.
- Protection of operational and business data.
- Support for railway operational continuity.
- Reduction of downtime and financial losses.
- Preservation of system integrity and security.

Disaster Recovery Scope

- Disaster Recovery Plans shall cover:
- Data centers
- Servers
- Applications
- Network infrastructure
- Cloud services
- Databases
- End-user systems
- OT infrastructure
- Communications systems

Disaster Scenarios

- Recovery plans shall address:
- Cyberattacks
- Ransomware incidents

- Hardware failures
- Software failures
- Power outages
- Telecommunications failures
- Natural disasters
- Human error
- Physical security incidents

Recovery Priorities

Priority	System Category
Priority 1	Train Control Systems
Priority 1	Signaling Systems
Priority 1	Railway Communication Systems
Priority 1	Operations Control Center Systems
Priority 2	Freight Management Systems
Priority 2	Passenger Service Systems
Priority 2	ERP and Financial Systems
Priority 3	Administrative Systems
Priority 3	Collaboration Platforms

Recovery Objectives

System Category	RTO	RPO
Train Control Systems	2 Hours	15 Minutes
Signaling Systems	2 Hours	15 Minutes
Communications Systems	4 Hours	30 Minutes
Freight Systems	8 Hours	1 Hour
Passenger Systems	8 Hours	1 Hour
ERP Systems	12 Hours	4 Hours
Email Services	12 Hours	4 Hours

Disaster Recovery Team

- The Disaster Recovery Team shall consist of:

- IT Manager
- Information Security Manager
- Systems Administrators
- Network Administrators
- Database Administrators
- Application Owners
- OT Support Personnel

Disaster Declaration

- Only designated management personnel, including the CEO, CDO, or delegated authority, may declare a disaster and initiate Disaster Recovery procedures.

16.3 Backup Management

Policy Statement

- EDRSC shall maintain backup procedures to ensure the availability, integrity, and recoverability of critical information and systems.

Backup Requirements

- Backup processes shall:
- Protect critical data and systems.
- Support business continuity objectives.
- Support disaster recovery requirements.
- Be automated where feasible.
- Be monitored regularly.

Data Subject to Backup

- The following shall be backed up:
- Databases
- Business applications
- Financial systems
- Human resources systems
- Email systems
- File servers
- Cloud-hosted information
- System configurations
- OT configurations
- Signaling and communication system configurations

Backup Schedule

Backup Type	Frequency
Incremental Backup	Daily
Full Backup	Weekly
Critical Database Backup	Daily or More Frequent
Configuration Backup	Weekly
OT Configuration Backup	Weekly

Backup Storage

- Backups shall be:
- Stored securely.
- Protected from unauthorized access.
- Encrypted where applicable.
- Maintained at an offsite location or approved cloud environment.
- Protected from ransomware and cyber threats.

Backup Security Controls

- Backup repositories shall:
- Use access controls.
- Require authentication.
- Be encrypted where appropriate.
- Be monitored for unauthorized access.
- Maintain audit logs.

Backup Retention

- Backup retention periods shall be determined based on:
- Business needs
- Regulatory requirements
- Contractual obligations
- Operational requirements

Backup Verification

- Backup success shall be:
- Monitored daily.
- Reviewed regularly.

- Investigated when failures occur.
- Reported to management when critical failures are identified.

16.4 Recovery Testing

Policy Statement

- EDRSC shall regularly test business continuity, disaster recovery, and backup recovery capabilities to verify effectiveness and readiness.

Objectives

- Recovery testing shall:
- Validate recovery procedures.
- Assess recovery capability.
- Identify weaknesses and gaps.
- Improve recovery readiness.
- Verify achievement of recovery objectives.

Types of Testing

Backup Restoration Testing

- Verify that:
- Data can be restored successfully.
- Backup integrity is maintained.
- Recovery times meet requirements.

Tabletop Exercises

- Simulate emergency scenarios through structured discussions and reviews.
- Examples:
- Ransomware attack
- Data breach
- Railway communication outage
- Control center disruption

Functional Testing

- Validate specific recovery processes including:
- Application recovery
- Network recovery

- User access restoration
- Communication procedures

Full Disaster Recovery Testing

- Validate end-to-end recovery capabilities, including:
- Alternate recovery sites
- Critical infrastructure recovery
- OT system recovery
- Railway operations support

Testing Frequency

Test Type	Frequency
Backup Recovery Test	Quarterly
Tabletop Exercise	Semi-Annually
Business Continuity Exercise	Annually
Disaster Recovery Test	Annually
OT Recovery Testing	Annually

Test Documentation

- All tests shall be documented including:
- Test objectives
- Scope
- Participants
- Results
- Issues identified
- Lessons learned
- Corrective actions

Corrective Actions

- Deficiencies identified during testing shall:
- Be documented.
- Be assigned to responsible owners.
- Have completion deadlines.
- Be tracked until closure.

Reporting

- Testing results shall be reported to:
- Chief Digital Officer (CDO)
- Executive Management
- Relevant Department Heads
- Internal Audit (where applicable)
- Critical findings shall be escalated immediately.

Continuous Improvement

- EDRSC shall use testing results, actual incidents, audits, and lessons learned to continuously improve:
- Business Continuity Plans
- Disaster Recovery Plans
- Backup strategies
- Crisis management procedures
- Recovery capabilities

17. Third-Party and Vendor Security

17.1 Vendor Risk Assessment

Policy Statement

- Ethio-Djibouti Railway Share Company (EDRSC) shall establish and maintain a Vendor Risk Management Program to identify, assess, monitor, and manage cybersecurity risks associated with third-party vendors, contractors, suppliers, consultants, service providers, and business partners.
- No third party shall be granted access to EDRSC information assets, systems, networks, cloud services, or operational technology environments without completing an appropriate risk assessment.

Objectives

- Vendor risk assessments shall:
- Protect EDRSC information assets.
- Protect railway operational and safety-critical systems.

- Reduce supply chain cybersecurity risks.
- Ensure compliance with legal and regulatory requirements.
- Verify third-party cybersecurity capabilities.

Scope

- Vendor assessments shall apply to third parties that:
- Access EDRSC networks.
- Process EDRSC information.
- Host EDRSC data.
- Provide cloud services.
- Support railway operational systems.
- Manage critical infrastructure.
- Provide software or hardware products.
- Deliver managed security or IT services.

Vendor Risk Classification

- Vendors shall be classified according to the level of risk they present.

Risk Level	Description
Critical	Supports railway operations, OT systems, critical infrastructure, or hosts sensitive data
High	Has access to Confidential or Restricted information
Medium	Limited access to business systems or Internal information
Low	No access to sensitive information or critical systems

Assessment Areas

- Vendor assessments shall evaluate:

Governance and Security Management

- Information security policies
- Security organization and governance
- Executive oversight

Access Control

- User access management

- Privileged access controls
- Multi-Factor Authentication (MFA)

Security Operations

- Monitoring capabilities
- Incident response procedures
- Vulnerability management practices

Data Protection

- Encryption controls
- Data handling procedures
- Backup management

Compliance

- Regulatory compliance
- Security certifications
- Audit reports

Business Continuity

- Disaster recovery capabilities
- Service resilience
- Recovery testing

Security Certifications

- Where appropriate, vendors should demonstrate compliance with recognized standards such as:
- ISO/IEC 27001
- ISO/IEC 22301
- SOC 1
- SOC 2
- PCI DSS
- NIST Frameworks

Assessment Frequency

Vendor Risk Level	Review Frequency
Critical	Annually
High	Annually

Medium	Every Two Years
Low	As Needed

Approval Requirements

- Critical and High-risk vendors shall require:
- Information Security Team review
- Business Owner approval
- Chief Digital Officer (CDO) approval where appropriate

17.2 Third-Party Access Controls

Policy Statement

- Access granted to third parties shall be controlled, monitored, reviewed, and limited to authorized business purposes in accordance with the principle of least privilege.

Access Authorization

- Third-party access shall:
- Be formally requested.
- Have documented business justification.
- Be approved by the asset owner.
- Undergo security review.
- No vendor shall receive access without documented authorization.

Access Principles

- Third-party access shall be based on:
- Need-to-know
- Least privilege
- Segregation of duties
- Time-bound authorization

Account Management

- Third-party user accounts shall:
- Be uniquely assigned.
- Not be shared.
- Be traceable to an individual.
- Have expiration dates where appropriate.

- Generic or shared vendor accounts are prohibited unless specifically approved and documented.

Authentication Requirements

- Third-party access shall require:
- Strong passwords
- Multi-Factor Authentication (MFA)
- Secure authentication mechanisms

Remote Access Requirements

- Remote access by vendors shall:
- Use approved VPN solutions.
- Be encrypted.
- Be monitored and logged.
- Be disabled when not required.

Privileged Access

- Vendor privileged access shall:
- Be approved by management.
- Be monitored continuously.
- Be reviewed quarterly.
- Be removed immediately when no longer required.

Operational Technology (OT) Access

- Access to:
- Signaling systems
- Train control systems
- SCADA systems
- Railway communication systems
- shall require:
- Additional management approval
- Security review
- Operational coordination
- Continuous monitoring

Access Review

- Third-party access rights shall be reviewed:
- Quarterly for critical systems

- Upon contract changes
- Upon personnel changes
- Prior to contract renewal

Access Termination

- Access shall be revoked immediately when:
- Services are completed.
- Contracts expire.
- Access is no longer required.
- Security concerns arise.

17.3 Contractual Security Requirements

Policy Statement

- All contracts involving access to EDRSC information, systems, applications, networks, or operational technology environments shall include cybersecurity and information security requirements.

Contract Security Clauses

- Contracts shall address:

Confidentiality

- Third parties shall protect EDRSC information from unauthorized disclosure, modification, or misuse.

Information Security Compliance

- Third parties shall comply with:
- EDRSC Cybersecurity Policy
- Applicable security standards
- Regulatory requirements

Data Protection

- Contracts shall clearly define:
- Data ownership
- Data handling obligations
- Data retention requirements
- Secure disposal procedures

Incident Reporting

- Third parties shall:
- Notify EDRSC immediately of security incidents.
- Cooperate during investigations.
- Provide incident details and mitigation plans.
- Recommended notification period:
- Critical incidents: Immediate notification
- Other incidents: Within 24 hours

Right to Audit

- EDRSC reserves the right to:
- Conduct security assessments.
- Request evidence of compliance.
- Review security controls.
- Monitor contractual obligations.

Personnel Security

- Third parties shall ensure:
- Personnel are appropriately vetted.
- Personnel receive security awareness training.
- Access permissions are controlled and monitored.

Business Continuity Requirements

- Critical vendors shall maintain:
- Business Continuity Plans
- Disaster Recovery Plans
- Cyber Incident Response Plans
- Evidence of testing may be required upon request.

Termination Requirements

- Upon contract termination, vendors shall:
- Return EDRSC information assets.
- Remove EDRSC information from their systems.
- Revoke access permissions.
- Provide written certification of data destruction where applicable.

17.4 Supply Chain Security

Policy Statement

- EDRSC shall implement controls to manage cybersecurity risks arising from the supply chain, including hardware suppliers, software providers, service providers, telecommunications providers, cloud service providers, and operational technology vendors.

Objectives

- Supply chain security controls shall:
- Protect critical infrastructure.
- Prevent supply chain attacks.
- Ensure integrity of products and services.
- Reduce operational and cybersecurity risks.

Supplier Security Management

- EDRSC shall:
- Assess supplier security practices.
- Monitor supplier performance.
- Review supplier risk profiles.
- Identify critical dependencies.

Hardware Security Requirements

- Hardware suppliers shall provide assurance regarding:
- Product authenticity
- Secure manufacturing processes
- Secure delivery methods
- Vulnerability disclosures
- Equipment shall be obtained only from approved suppliers.

Software Security Requirements

- Software vendors shall:
- Provide security updates.
- Maintain vulnerability management programs.
- Disclose known security vulnerabilities.
- Support secure software development practices.
- Software used within critical railway environments shall undergo security review prior to deployment.

Operational Technology Supply Chain Security

- Special attention shall be given to suppliers supporting:
- Signaling systems
- Train control systems
- SCADA systems
- Communication infrastructure
- Power and traction systems
- EDRSC shall perform enhanced due diligence for these suppliers.

Supply Chain Monitoring

- The Information Security Team shall monitor:
- Vendor security notifications
- Vulnerability advisories
- Threat intelligence reports
- Supplier security incidents
- Critical supply chain risks shall be reported to Executive Management.

Secure Procurement Requirements

- Procurement processes shall include:
- Security requirements definitions
- Vendor security evaluations
- Risk assessments
- Contractual security obligations
- Cybersecurity requirements shall be considered before procurement approval.

Supply Chain Incident Management

- In the event of a supply chain cybersecurity incident, EDRSC shall:
- Assess potential impact.
- Activate incident response procedures.
- Coordinate with affected suppliers.
- Implement containment measures.
- Monitor recovery activities.
- Conduct post-incident reviews.

Compliance

- Failure of vendors or suppliers to comply with contractual cybersecurity requirements may result in:
- Corrective action requests

- Suspension of access privileges
- Contractual penalties
- Contract termination
- Legal action where applicable

18. Security Awareness and Training

18.1 Employee Security Awareness

Policy Statement

- Ethio-Djibouti Railway Share Company (EDRSC) shall establish and maintain a cybersecurity awareness program to ensure that all employees, contractors, consultants, and temporary staff understand their cybersecurity responsibilities and contribute to the protection of organizational information assets, railway operational systems, and critical infrastructure.
- Cybersecurity awareness is a shared responsibility and is an essential component of EDRSC's security culture.

Objectives

- The Security Awareness Program shall:
- Promote a cybersecurity-conscious culture.
- Reduce the likelihood of human error.
- Improve employee understanding of cyber threats.
- Protect sensitive information and critical systems.
- Support compliance with regulatory and contractual obligations.
- Improve incident detection and reporting.

Scope

- Security awareness requirements apply to:
- Permanent employees
- Temporary employees
- Contractors
- Consultants
- Interns
- Third-party personnel with access to EDRSC systems or facilities

Awareness Program Requirements

- The Information Security Team shall develop and maintain a formal awareness program that includes:
- Cybersecurity policies and procedures

- Data protection and privacy requirements
- Password and authentication practices
- Phishing and social engineering awareness
- Incident reporting procedures
- Acceptable use requirements
- Remote working security
- Physical security awareness
- Railway operational technology (OT) security awareness

Mandatory Training

- All personnel shall complete:

New Employee Training

- Within thirty (30) days of joining EDRSC.
- Topics include:
- Cybersecurity responsibilities
- Information classification
- Password security
- Incident reporting
- Acceptable use requirements

Annual Refresher Training

- All employees shall complete annual cybersecurity awareness training.
- Training records shall be maintained by Human Resources and the Information Security Team.

Employee Responsibilities

- Employees shall:
- Complete all mandatory cybersecurity training.
- Follow cybersecurity policies and procedures.
- Protect passwords and authentication credentials.
- Identify and report suspicious activities.
- Protect company information from unauthorized access.
- Participate in awareness exercises and assessments.

Awareness Communications

- Security awareness messages may be distributed through:
- Email notifications

- Posters and signage
- Newsletters
- Intranet announcements
- Awareness campaigns
- Workshops and seminars

Training Records

- The organization shall maintain records including:
- Participant names
- Training dates
- Completion status
- Assessment results
- Outstanding training requirements

Non-Compliance

- Failure to complete mandatory training may result in:
- Restricted system access
- Escalation to management
- Disciplinary action in accordance with company policies

18.2 Specialized Security Training

Policy Statement

- EDRSC shall provide specialized cybersecurity training to personnel whose roles require advanced knowledge and responsibilities related to cybersecurity, information technology, operational technology, and critical railway operations.

Objectives

- Specialized training shall:
- Improve technical cybersecurity capabilities.
- Enhance incident response readiness.
- Support secure system administration.
- Protect safety-critical railway systems.
- Address emerging cybersecurity threats.

Personnel Requiring Specialized Training

- Specialized training shall be provided to:

Information Security Personnel

- Topics may include:
- Security operations
- Threat intelligence
- Incident response
- Digital forensics
- Vulnerability management
- Risk management
- Security monitoring and SIEM operations

Network Administrators

- Topics may include:
- Network security
- Firewall management
- IDS/IPS administration
- Secure remote access
- Network monitoring

System Administrators

- Topics may include:
- Secure system configuration
- Patch management
- Identity and access management
- Backup and recovery
- Endpoint protection

Application Developers

- Topics may include:
- Secure Software Development Lifecycle (SSDLC)
- Secure coding practices
- Application security testing
- OWASP Top 10 vulnerabilities
- API security

Operational Technology (OT) Personnel

- Topics may include:
- OT cybersecurity fundamentals

- SCADA security
- Signaling system security
- Train control system protection
- Industrial network security
- Railway cyber resilience

Executive Management

- Topics may include:
- Cybersecurity governance
- Risk management
- Regulatory obligations
- Crisis management
- Incident response leadership

Training Frequency

- Specialized training shall be conducted:
- Upon assignment to relevant roles
- Annually thereafter
- When significant technologies are introduced
- Following significant cybersecurity incidents

Professional Development

- Employees in cybersecurity-related roles are encouraged to pursue relevant professional certifications, such as:
- CISSP
- CISM
- CISA
- CompTIA Security+
- CEH
- ISO 27001 Lead Implementer
- GIAC Certifications
- Microsoft Security Certifications

Training Evaluation

- Effectiveness of specialized training shall be evaluated through:
- Assessments
- Practical exercises
- Simulations

- Knowledge testing
- Performance evaluations

18.3 Phishing Awareness Programs

Policy Statement

- EDRSC shall implement an ongoing Phishing Awareness Program to educate personnel on identifying, avoiding, and reporting phishing and social engineering attacks.
- Because phishing remains one of the most significant cybersecurity threats, all personnel shall actively participate in phishing awareness activities.

Objectives

- The Phishing Awareness Program shall:
- Improve employee ability to recognize phishing attacks.
- Reduce successful compromise of user credentials.
- Minimize malware infections.
- Improve reporting of suspicious emails and messages.
- Strengthen organizational resilience against social engineering attacks.

Covered Threat Types

- Training shall address:

Email Phishing

- Fraudulent emails designed to:
- Steal credentials
- Deliver malware
- Obtain sensitive information

Spear Phishing

- Targeted attacks directed at specific employees, departments, or executives.

Business Email Compromise (BEC)

- Fraudulent communications impersonating:
- Executives
- Suppliers
- Customers

- Business partners

Smishing

- Phishing attacks delivered through:
- SMS messages
- Mobile messaging applications

Vishing

- Voice-based phishing attempts conducted through telephone calls.

Phishing Awareness Content

- Employees shall be trained to identify:
- Suspicious senders
- Unexpected attachments
- Malicious links
- Urgent payment requests
- Requests for passwords
- Requests for confidential information
- Spoofed email addresses
- Social engineering techniques

Phishing Simulations

- The Information Security Team shall conduct periodic phishing simulation exercises.
- Simulation objectives include:
- Measuring employee awareness
- Identifying vulnerable groups
- Improving training effectiveness
- Evaluating organizational readiness

Recommended Frequency

Activity	Frequency
Phishing Awareness Training	Annually
Phishing Simulations	Quarterly
Awareness Communications	Monthly
Targeted Remedial Training	As Needed

Reporting Suspicious Emails

- Employees shall immediately report suspected phishing emails using approved reporting mechanisms.
- Reports should include:
- Sender information
- Email subject
- Screenshots where applicable
- Description of suspicious activity
- Employees shall not:
- Open suspicious attachments.
- Click suspicious links.
- Respond to suspicious messages.
- Forward suspicious emails to unauthorized recipients.

Performance Metrics

- The Information Security Team shall track:
- Training completion rates
- Phishing simulation results
- Employee reporting rates
- Click-through rates
- Incident trends
- Results shall be used to improve awareness programs and reduce organizational risk.

Continuous Improvement

- EDRSC shall regularly review and improve awareness programs based on:
- Incident trends
- Threat intelligence
- Audit findings
- Simulation results
- Regulatory requirements
- Industry best practices

19. Compliance and Legal Requirements

19.1 Regulatory Compliance

Policy Statement

- Ethio-Djibouti Railway Share Company (EDRSC) shall comply with all applicable laws, regulations, regulatory directives, contractual obligations, industry standards, and cybersecurity requirements relevant to its operations in Ethiopia, Djibouti, and other jurisdictions in which it conducts business.
- Compliance shall be integrated into the organization's cybersecurity governance, risk management, and operational processes.

Objectives

- The Regulatory Compliance Program shall:
- Ensure adherence to applicable legal and regulatory requirements.
- Protect the confidentiality, integrity, and availability of information assets.
- Support safe and secure railway operations.
- Minimize legal, financial, and reputational risks.
- Demonstrate due diligence and accountability.

Applicable Regulatory and Legal Requirements

- EDRSC shall identify and maintain an inventory of applicable requirements, including but not limited to:

National Laws and Regulations

- Ethiopian cyber and digital regulations.
- Djibouti regulatory requirements applicable to railway operations.
- Labor and employment laws.
- Data protection and privacy regulations.
- Telecommunications regulations.
- Commercial and contractual laws.

International Standards and Frameworks

- EDRSC may adopt and align with:
- ISO/IEC 27001 Information Security Management Systems
- ISO/IEC 27002 Information Security Controls
- ISO/IEC 22301 Business Continuity Management
- NIST Cybersecurity Framework (CSF)
- CIS Critical Security Controls

Railway Industry Requirements

- Where applicable, EDRSC shall comply with:
- Railway safety regulations
- Critical infrastructure protection requirements
- Transportation and operational resilience standards
- Railway cybersecurity guidance and best practices

Compliance Responsibilities

Board of Directors

- Provide oversight for compliance activities.
- Review significant regulatory risks.

Executive Management

- Ensure resources are available to achieve compliance objectives.
- Review compliance reports and audit findings.

Chief Digital Officer (CDO)

- Maintain cybersecurity compliance programs.
- Coordinate compliance assessments.
- Report compliance status to management.

Department Managers

- Implement and maintain compliance controls within their areas.
- Support audit and assessment activities.

Employees

- Comply with applicable laws, policies, and procedures.
- Report suspected compliance violations.

Compliance Assessments

- Periodic assessments shall be performed to verify compliance with:
- Policies
- Standards
- Regulations
- Contractual requirements

- Security controls
- Non-compliance findings shall be documented and addressed through corrective action plans.

Regulatory Reporting

- Where required by law or regulation, EDRSC shall report:
- Cybersecurity incidents
- Data breaches
- Regulatory violations
- Operational disruptions
- Reports shall be coordinated through designated management and legal representatives.

19.2 Internal Audits

Policy Statement

- EDRSC shall conduct periodic internal audits to evaluate the effectiveness of cybersecurity controls, regulatory compliance, governance processes, and risk management activities.

Objectives

- Internal audits shall:
- Verify compliance with policies and standards.
- Assess effectiveness of cybersecurity controls.
- Identify improvement opportunities.
- Validate risk management activities.
- Support continuous improvement.

Audit Scope

- Internal audits may cover:
- Information security governance
- Access management
- Network security
- Endpoint security
- Cloud security
- Operational technology (OT) security
- Data protection and privacy
- Incident response
- Business continuity and disaster recovery
- Third-party security management

Audit Frequency

- Internal cybersecurity audits shall be performed:
- Annually at a minimum.
- Following major incidents.
- Following significant organizational changes.
- As directed by Executive Management or the Board.

Audit Responsibilities

- **Internal Audit Function**

- Responsible for:
- Planning audits.
- Conducting independent assessments.
- Reporting findings.
- Monitoring corrective actions.

Information Security Team

- Responsible for:
- Providing requested information.
- Supporting audit activities.
- Implementing corrective actions.

Audit Findings Classification

Classification	Description
Critical	Significant control failure requiring immediate action
High	Major weakness requiring prompt remediation
Medium	Moderate issue requiring corrective action
Low	Minor issue or improvement opportunity

Corrective Actions

- Audit findings shall:
- Be assigned to responsible owners.
- Include remediation deadlines.
- Be tracked to closure.
- Be verified by Internal Audit.

Audit Reporting

- Audit results shall be reported to:
- Chief Digital Officer (CDO)
- Executive Management
- Audit Committee (where applicable)
- Board of Directors

19.3 External Audits

Policy Statement

- EDRSC shall cooperate with authorized external audits, assessments, inspections, and certification activities to demonstrate compliance with legal, regulatory, contractual, and industry requirements.

Objectives

- External audits shall:
- Validate compliance status.
- Provide independent assurance.
- Support certification efforts.
- Identify improvement opportunities.
- Enhance stakeholder confidence.

Types of External Audits

- EDRSC may undergo:

Regulatory Audits

- Conducted by competent government authorities and regulators.

Certification Audits

- Examples include:
- ISO/IEC 27001 certification audits
- ISO/IEC 22301 audits
- Other recognized certification assessments

Customer and Partner Audits

- Where contractually required, customers or partners may perform security reviews and assessments.

Independent Security Assessments

- Conducted by external consultants or cybersecurity specialists.

Audit Preparation

- Departments shall:
- Maintain accurate documentation.
- Retain required records.
- Support auditor requests.
- Respond to audit findings promptly.

Audit Findings Management

- All external audit findings shall:
- Be documented.
- Receive risk assessment.
- Have assigned corrective actions.
- Be tracked through completion.

Confidentiality

- Information provided during audits shall:
- Be protected appropriately.
- Be shared only with authorized auditors.
- Comply with contractual and legal requirements.

Reporting

- Significant external audit findings shall be reported to:
- Chief Executive Officer (CEO)
- Chief Digital Officer (CDO)
- Executive Management
- Board of Directors

19.4 Records Management

Policy Statement

- EDRSC shall establish and maintain records management practices to ensure that information records are created, maintained, protected, retained, archived, and disposed of in accordance with business, legal, regulatory, and operational requirements.

Objectives

- Records management shall:
- Preserve organizational knowledge.
- Support legal and regulatory compliance.
- Protect sensitive information.
- Support operational and business activities.
- Facilitate investigations and audits.

Scope

- Records may include:

Business Records

- Contracts
- Financial records
- Procurement documents
- Management reports

Human Resources Records

- Employee files
- Payroll records
- Training records

Security Records

- Incident reports
- Audit reports
- Vulnerability assessments
- Risk assessments
- Access review reports

Operational Records

- Railway operation logs
- Maintenance records
- Signaling records
- SCADA logs
- Communications records

Record Classification

- Records shall be classified according to:
- Public
- Internal
- Confidential
- Restricted
- Appropriate safeguards shall be applied based on classification.

Record Retention Requirements

- Records shall be retained according to approved retention schedules and applicable regulatory requirements.

Record Type	Minimum Retention Period
Security Incident Reports	5 Years
Audit Reports	5 Years
Risk Assessments	5 Years
Access Logs	12 Months
Security Logs	12 Months
Employee Records	7 Years
Financial Records	10 Years
Contracts	10 Years After Expiration
Railway Operational Records	As Required by Regulation
OT Security Logs	24 Months

Record Protection

- Records shall be protected through:
- Access controls
- Encryption where appropriate
- Backup procedures
- Physical security controls
- Monitoring and logging

Archiving

- Archived records shall:
- Remain accessible when required.
- Maintain integrity and authenticity.

- Be protected from unauthorized modification.

Secure Disposal

- When retention periods expire, records shall be disposed of securely using approved methods, including:
- Secure shredding
- Secure wiping
- Physical destruction
- Cryptographic erasure
- Disposal activities shall be documented where required.

Legal Holds

- Where litigation, investigation, audit, or regulatory action is anticipated or active, relevant records shall be preserved until authorized for release by Legal Counsel and Executive Management.

Compliance Monitoring

- The Information Security Team, Legal Department, Internal Audit, and Records Management personnel shall periodically review compliance with records management requirements.
- Failure to comply with records management requirements may result in disciplinary action and potential legal or regulatory consequences.

20. Acceptable Use Policy

20.1 Use of Organizational Systems

Policy Statement

- Ethio-Djibouti Railway Share Company (EDRSC) provides information technology (IT), operational technology (OT), communication systems, networks, applications, devices, and information resources to support business operations and railway services. These resources shall be used responsibly, securely, ethically, and in accordance with organizational policies and applicable laws.
- All users are responsible for protecting EDRSC systems and information from unauthorized use, disclosure, alteration, damage, or loss.

Scope

- This policy applies to:
- Employees
- Contractors
- Consultants
- Vendors
- Temporary staff
- Third parties with authorized access to EDRSC resources

Authorized Use

- Organizational systems shall be used primarily for:
- Official business activities
- Railway operational activities
- Customer service functions
- Administrative activities
- Approved training and research
- Job-related communications
- Limited personal use may be permitted provided it:
- Does not interfere with work responsibilities.
- Does not consume excessive resources.
- Does not violate laws, regulations, or company policies.
- Does not introduce cybersecurity risks.

User Responsibilities

- Users shall:
- Use organizational systems responsibly.
- Protect their login credentials.
- Lock devices when unattended.
- Report security incidents immediately.
- Follow cybersecurity policies and procedures.
- Protect sensitive information from unauthorized disclosure.
- Use only approved software and services.

Prohibited Activities

- Users shall not:
- Access systems without authorization.

- Share user accounts or passwords.
- Install unauthorized software or applications.
- Disable security controls.
- Circumvent security measures.
- Use organizational resources for illegal purposes.
- Attempt to gain unauthorized access to systems or data.
- Create, distribute, or knowingly transmit malicious software.
- Engage in activities that disrupt system availability or performance.
- Use company resources for personal commercial activities.

Monitoring Notice

- All use of EDRSC systems may be monitored, logged, and reviewed to:
- Ensure legal compliance.
- Protect organizational assets.
- Detect security threats.
- Investigate misconduct.
- Support operational activities.
- Users should have no expectation of privacy when using company-owned systems except where protected by applicable law.

Operational Technology (OT) Systems

- Users of:
- Signaling systems
- Train control systems
- SCADA systems
- Railway communication systems
- shall only perform authorized activities and strictly follow operational and safety procedures.
- Unauthorized modification of OT systems is strictly prohibited.

20.2 Internet and Email Usage

Policy Statement

- Internet and email services are provided to support EDRSC business activities and railway operations. Users shall use these services responsibly and securely to reduce cybersecurity risks and maintain organizational productivity.

Internet Usage Requirements

- Users shall:

- Access websites necessary for business purposes.
- Exercise caution when downloading files.
- Verify the legitimacy of websites before sharing information.
- Report suspicious websites or online activities.

Prohibited Internet Activities

- Users shall not:
- Visit malicious or illegal websites.
- Download unauthorized software.
- Circumvent web filtering controls.
- Access unauthorized file-sharing services.
- Use anonymizing services or unauthorized VPNs.
- Participate in activities that may expose EDRSC to cybersecurity risks.

Email Usage Requirements

- EDRSC email accounts shall primarily be used for official business communications.
- Users shall:
- Use professional and appropriate language.
- Verify recipients before sending information.
- Protect sensitive information using approved safeguards.
- Report suspicious emails immediately.

Email Security Requirements

- Users shall:
- Exercise caution when opening attachments.
- Avoid clicking suspicious links.
- Verify unusual requests for payments or sensitive information.
- Report phishing attempts promptly.
- Use approved encryption methods when transmitting sensitive information.

Prohibited Email Activities

- Users shall not:
- Send offensive, discriminatory, or inappropriate content.
- Forward confidential information to unauthorized recipients.
- Use personal email accounts for company business without authorization.
- Open suspicious attachments without verification.
- Share login credentials via email.

Mass Email Communications

- Mass email distribution to employees or external recipients shall require appropriate authorization and business justification.

Email Retention

- Business-related emails shall be retained and managed in accordance with EDRSC Records Management and Data Retention requirements.

20.3 Social Media Usage

Policy Statement

- EDRSC recognizes the value of social media for communication, stakeholder engagement, and public awareness. Employees shall use social media responsibly and in a manner that protects the reputation, security, confidentiality, and interests of EDRSC.

Scope

- This policy applies to:
- Official EDRSC social media accounts.
- Employee use of social media where EDRSC is referenced.
- Social media activities conducted using EDRSC resources.

Authorized Use

- Only designated and authorized personnel may:
- Create official EDRSC social media accounts.
- Publish official company statements.
- Respond to media inquiries through social media.
- Represent EDRSC publicly online.

Employee Responsibilities

- Employees using social media shall:
- Protect confidential information.
- Respect intellectual property rights.
- Maintain professional conduct.
- Avoid misrepresenting EDRSC positions.
- Follow applicable laws and company policies.

- Employees expressing personal opinions shall ensure that such opinions are not presented as official positions of EDRSC.

Prohibited Activities

- Users shall not:
- Disclose Confidential or Restricted information.
- Share security-sensitive information.
- Publish information about cybersecurity incidents without authorization.
- Share details of railway operational systems or infrastructure.
- Post information that could endanger operational safety.
- Make unauthorized statements on behalf of EDRSC.
- Engage in harassment, discrimination, or inappropriate behavior.

Protection of Sensitive Information

- The following information shall not be disclosed through social media without proper authorization:
- Customer data
- Employee information
- Financial information
- Security procedures
- Network architecture information
- Signaling system information
- Train control system information
- Incident response activities
- Internal reports and documents

Official Social Media Management

- Official social media accounts shall:
- Be approved by management.
- Use strong authentication controls.
- Utilize Multi-Factor Authentication (MFA).
- Be monitored regularly.
- Be protected against unauthorized access.

Monitoring and Enforcement

- EDRSC reserves the right to investigate social media activities that:
- Violate organizational policies.
- Create cybersecurity risks.
- Damage the company's reputation.

- Expose sensitive information.

Policy Violations

- Violations of this Acceptable Use Policy may result in:
- Verbal or written warnings.
- Suspension of access privileges.
- Disciplinary action.
- Contract termination.
- Legal action where applicable.

21. Physical and Environmental Security

21.1 Physical Access Controls

Policy Statement

- Ethio-Djibouti Railway Share Company (EDRSC) shall implement physical security controls to protect personnel, information assets, operational technology (OT) systems, railway infrastructure, and facilities from unauthorized access, damage, theft, disruption, or interference.
- Physical security controls shall be commensurate with the sensitivity and criticality of the assets being protected.

Objectives

- Physical access controls shall:
- Prevent unauthorized access to facilities and assets.
- Protect critical railway and information systems.
- Safeguard employees, contractors, and visitors.
- Support business continuity and operational resilience.
- Ensure compliance with security and regulatory requirements.

Protected Areas

- Physical security controls shall be applied to:
- Data centers
- Operations Control Centers
- Signaling facilities
- Telecommunications rooms
- Server rooms
- Network equipment rooms

- Power and traction control facilities
- Archives and records storage areas
- Security Operations Centers (SOC)
- Administrative offices

Access Authorization

- Access to restricted areas shall:
- Be granted only to authorized personnel.
- Be based on job responsibilities.
- Be approved by designated management.
- Be reviewed periodically.

Physical Access Mechanisms

- EDRSC may implement:
- Access cards and badges
- Smart cards
- Biometric authentication
- PIN-based access systems
- Security guards
- Turnstiles
- Security checkpoints

Visitor Management

- Visitors shall:
- Sign in upon arrival.
- Present valid identification.
- Be issued visitor badges.
- Be escorted in restricted areas.
- Return visitor badges upon departure.
- Visitor logs shall be retained for audit and investigative purposes.

Access Monitoring

- Access to critical facilities shall be monitored through:
- CCTV surveillance
- Electronic access control systems
- Visitor registers
- Security patrols
- Access logs

- Access records shall be reviewed periodically.

Key Management

- Physical keys shall:
- Be controlled and inventoried.
- Be issued only to authorized personnel.
- Be returned when no longer required.
- Be replaced when compromise is suspected

Physical Security Incidents

- Any incidents involving:
- Unauthorized entry
- Forced access
- Theft
- Vandalism
- Suspicious activity
- shall be reported immediately to Security Management and the Information Security Team.

21.2 Data Center Security

Policy Statement

- EDRSC shall protect data centers and critical technology facilities against unauthorized access, environmental hazards, equipment failure, and physical threats that could affect information systems and railway operations.

Data Center Access Control

- Access to data centers shall:
- Be restricted to authorized personnel.
- Require management approval.
- Be recorded and monitored.
- Be reviewed regularly.

Security Measures

- Data centers shall be protected through:
- Physical barriers

- Secure doors and locks
- CCTV surveillance
- Intrusion detection systems
- Security personnel
- Access logging

Environmental Controls

- Data centers shall maintain appropriate environmental conditions including:

Temperature Control

- Air conditioning systems
- Environmental monitoring

Humidity Control

- Humidity monitoring systems
- Environmental alarms

Fire Protection

- Fire detection systems
- Smoke detection systems
- Fire suppression systems
- Emergency response procedures

Water Protection

- Leak detection systems
- Protection against flooding
- Appropriate drainage systems

Power Protection

- Critical facilities shall maintain:
- Uninterruptible Power Supplies (UPS)
- Backup generators
- Power monitoring systems
- Redundant electrical systems where applicable

Facility Monitoring

- Data center facilities shall be monitored continuously for:
- Security incidents
- Environmental failures
- Power outages
- Equipment failures
- Fire and safety risks

Maintenance Activities

- Maintenance personnel shall:
- Be authorized and supervised.
- Follow established procedures.
- Record maintenance activities.
- Report any security concerns immediately.

Data Center Audits

- Periodic inspections and audits shall verify:
- Access control effectiveness.
- Environmental control functionality.
- Compliance with security requirements.
- Physical security readiness.

21.3 Equipment Protection

Policy Statement

- EDRSC shall protect information processing equipment, communication systems, operational technology equipment, and supporting infrastructure from theft, damage, loss, misuse, and environmental threats.

Equipment Security Requirements

- The organization shall ensure:
- Equipment is physically secured.
- Equipment is protected from unauthorized access.
- Equipment is maintained according to manufacturer requirements.
- Equipment is protected throughout its lifecycle.

Equipment Placement

- Critical equipment shall be located in secure areas and protected from:
- Unauthorized access
- Environmental hazards
- Excessive heat
- Moisture
- Dust
- Electromagnetic interference

Portable Equipment Protection

- Portable devices including:
- Laptops
- Tablets
- Smartphones
- Storage media
- shall be:
- Physically secured.
- Protected with passwords and encryption.
- Never left unattended in public areas.
- Reported immediately if lost or stolen.

Operational Technology Equipment

- Special protection measures shall apply to:
- Signaling equipment
- Train control systems
- SCADA components
- Communications infrastructure
- Power management systems
- Protection measures may include:
- Restricted access areas
- Tamper-evident controls
- CCTV monitoring
- Environmental protection systems

Equipment Maintenance

- Maintenance activities shall:
- Follow approved procedures.
- Be performed by authorized personnel.

- Protect sensitive information.
- Be documented and recorded.

Equipment Disposal

- Prior to disposal, transfer, or reuse, equipment shall:
- Have all data securely removed.
- Be sanitized according to approved standards.
- Be approved by the asset owner.
- Have disposal records maintained.

Equipment Protection During Transport

- Equipment being transported shall:
- Be securely packaged.
- Be protected from theft and damage.
- Be tracked where appropriate.
- Follow approved transport procedures.

22. Policy Compliance and Enforcement

22.1 Monitoring Compliance

Policy Statement

- EDRSC shall monitor compliance with this Cybersecurity Policy and supporting standards, procedures, and guidelines to ensure the effective protection of organizational assets and railway operations.

Compliance Activities

- Compliance may be monitored through:
- Internal audits
- External audits
- Security assessments
- Vulnerability assessments
- Penetration testing
- Access reviews
- Security monitoring
- Management reviews

Responsibilities

- Department Managers shall:
- Promote policy compliance.
- Address identified deficiencies.
- Support corrective actions.
- The Information Security Team shall:
- Monitor policy compliance.
- Conduct compliance assessments.
- Report findings to management.

22.2 Policy Violations

Policy Statement

- Any violation of this Cybersecurity Policy shall be investigated and addressed according to EDRSC disciplinary procedures and applicable legal requirements.

- **Examples of Violations**

- Policy violations may include:
- Sharing passwords
- Unauthorized access to systems
- Installation of unauthorized software
- Failure to report security incidents
- Unauthorized disclosure of information
- Bypassing security controls
- Misuse of organizational systems
- Violations of data protection requirements

Reporting Violations

- Employees shall report suspected violations to:
- Immediate supervisors
- Human Resources
- Information Security Team
- Ethics or Compliance Office

Investigation Process

- All suspected violations shall:
- Be documented.

- Be investigated fairly and objectively.
- Preserve evidence where applicable.
- Maintain confidentiality.

22.3 Disciplinary Actions

Policy Statement

- Individuals found to have violated cybersecurity requirements may be subject to disciplinary action proportional to the severity and impact of the violation.

Possible Actions

- Disciplinary measures may include:

- **Employees**

- Verbal warning
- Written warning
- Mandatory retraining
- Suspension of access privileges
- Suspension from duty
- Termination of employment

Contractors and Vendors

- Suspension of access
- Contractual penalties
- Contract termination
- Legal action where appropriate

Serious Violations

- The following may result in immediate disciplinary action and legal escalation:
- Intentional unauthorized access
- Theft of information
- Deliberate security breaches
- Sabotage of systems
- Fraudulent activities
- Disclosure of Restricted information

Appeals

- Individuals subject to disciplinary actions may appeal through established EDRSC grievance and disciplinary procedures.

22. Policy Compliance and Enforcement

22.1 Monitoring Compliance

Policy Statement

- Ethio-Djibouti Railway Share Company (EDRSC) shall establish mechanisms to monitor, assess, and verify compliance with this Cybersecurity Policy, supporting standards, procedures, legal requirements, and regulatory obligations.
- Compliance monitoring shall ensure that cybersecurity controls are implemented effectively, operating as intended, and continuously improved to protect EDRSC's information assets, railway operations, and critical infrastructure.

Objectives

- Compliance monitoring shall:
- Verify adherence to cybersecurity policies and standards.
- Identify control weaknesses and non-compliance issues.
- Support risk management activities.
- Ensure regulatory and contractual compliance.
- Promote accountability and continuous improvement.

Compliance Monitoring Activities

- Compliance may be monitored through:
- Internal audits
- External audits
- Security assessments
- Vulnerability assessments
- Penetration testing
- Risk assessments
- Access reviews
- Security monitoring activities
- Management reviews
- Regulatory inspections

Responsibilities

- **Chief Digital Officer (CDO)**

- The CDO shall:
- Oversee cybersecurity compliance activities.
- Review compliance reports.
- Ensure corrective actions are implemented.
- Report significant compliance issues to Executive Management.

Information Security Team

- The Information Security Team shall:
- Conduct compliance assessments.
- Monitor security controls.
- Track remediation activities.
- Maintain compliance records.
- Generate compliance reports.

Department Managers

- Department Managers shall:
- Ensure compliance within their areas of responsibility.
- Support audit and assessment activities.
- Address identified deficiencies promptly.

Employees and Contractors

- All personnel shall:
- Comply with cybersecurity policies and procedures.
- Cooperate with compliance reviews and audits.
- Report known or suspected non-compliance.

Compliance Reporting

- Compliance status reports shall be prepared:

Corrective Actions

- Where non-compliance is identified:
- Findings shall be documented.
- Root cause analysis shall be performed.
- Corrective actions shall be assigned.
- Completion dates shall be established.
- Remediation shall be tracked to closure.

22.2 Policy Violations

Policy Statement

- Any violation of this Cybersecurity Policy, associated standards, procedures, or legal requirements shall be investigated, documented, and addressed appropriately.
- All personnel are responsible for reporting known or suspected violations.

Examples of Policy Violations

- Violations may include, but are not limited to:

Access Control Violations

- Sharing passwords
- Using another person's account
- Unauthorized access to systems or information
- Circumventing authentication controls

Information Security Violations

- Unauthorized disclosure of Confidential or Restricted information
- Improper handling of sensitive data
- Failure to protect information assets

Technology Misuse

- Installation of unauthorized software
- Use of unauthorized cloud services
- Use of unauthorized external storage devices
- Bypassing security controls

Incident Management Violations

- Failure to report cybersecurity incidents
- Failure to report lost or stolen devices
- Concealing cybersecurity events or breaches

Operational Technology Violations

- Unauthorized access to signaling systems
- Unauthorized changes to train control systems
- Unauthorized modification of SCADA environments
- Breach of railway operational security procedures

Compliance Violations

- Failure to complete mandatory cybersecurity training
- Failure to follow approved procedures
- Failure to implement required security controls

Reporting Violations

- Violations may be reported through:
- Immediate supervisors
- Department Managers
- Human Resources
- Information Security Team

- Internal Audit
- Ethics and Compliance Channels
- Reports may be treated confidentially in accordance with company policies and applicable laws.

Investigation Process

- All reported violations shall:
- Be documented.
- Be reviewed and assessed.
- Be investigated by appropriate personnel.
- Preserve relevant evidence.
- Maintain confidentiality where appropriate.
- Determine root cause and impact.
- Recommend corrective actions.

Violation Classification

Escalation Requirements

- Critical violations shall be immediately escalated to:
- Chief Digital Officer (CDO)
- Executive Management
- Chief Executive Officer (CEO)
- Legal Counsel (where applicable)

22.3 Disciplinary Actions

Policy Statement

- Individuals who violate cybersecurity policies, standards, procedures, contractual obligations, or applicable laws may be subject to disciplinary action proportionate to the severity, intent, frequency, and impact of the violation.

Principles

- Disciplinary actions shall:
- Be fair and consistent.
- Follow due process.
- Be documented.
- Consider intent, negligence, and impact.

- Comply with labor laws and contractual obligations.

Employee Disciplinary Actions

- Depending on the severity of the violation, disciplinary measures may include:

Minor Violations

- Examples:
- Failure to complete required training
- Accidental policy non-compliance
- First-time minor procedural violations
- Possible actions:
- Verbal counseling
- Written warning
- Mandatory retraining

Moderate Violations

- Examples:
- Repeated policy violations
- Failure to follow security procedures
- Unauthorized software installation
- Possible actions:
- Formal written warning
- Temporary suspension of access privileges
- Performance improvement measures

Serious Violations

- Examples:
- Unauthorized access attempts
- Disclosure of sensitive information
- Bypassing security controls
- Failure to report known incidents
- Possible actions:
- Suspension from duties
- Loss of privileged access
- Final written warning
- Disciplinary hearing

Severe Violations

- Examples:
- Intentional security breaches
- Theft of information
- Fraudulent activities
- Sabotage of systems
- Insider threats
- Compromise of railway safety systems
- Possible actions:
- Immediate termination of employment
- Legal action
- Referral to law enforcement authorities
- Financial recovery actions where applicable

Contractor and Vendor Sanctions

- Contractors, consultants, and vendors may be subject to:
- Suspension of access privileges
- Corrective action requirements
- Contractual penalties
- Contract termination
- Legal action
- Removal from approved supplier lists

Recovery of Organizational Assets

- Where violations involve organizational assets, EDRSC may require:
- Return of equipment
- Return of credentials
- Return or destruction of information
- Verification of compliance actions

Appeals Process

- Individuals subject to disciplinary action shall have the right to appeal through established EDRSC grievance and disciplinary procedures.
- Appeals shall be reviewed by appropriate management and Human Resources personnel.

Record Keeping

- Records of policy violations and disciplinary actions shall:

- Be maintained securely.
- Be treated as Confidential information.
- Be retained in accordance with Records Management requirements.
- Be available for audit and legal purposes where required.

Continuous Improvement

- Lessons learned from policy violations shall be used to:
- Improve cybersecurity awareness programs.
- Strengthen security controls.
- Update policies and procedures.
- Reduce future compliance risks.
-

Report Type	Frequency
Operational Compliance Reports	Monthly
Cybersecurity Compliance Reports	Quarterly
Executive Compliance Reports	Quarterly
Board-Level Compliance Reports	Annually

Severity	Description
Low	Minor violation with limited impact
Medium	Violation affecting operations or policy compliance
High	Significant breach of cybersecurity controls
Critical	Serious violation affecting safety, security, business operations, or regulatory obligations

23. Policy Exception Management

23.1 Exception Request Process

Policy Statement

- Ethio-Djibouti Railway Share Company (EDRSC) recognizes that, under exceptional circumstances, temporary deviations from cybersecurity policies, standards, procedures, or control requirements may be necessary to support business operations, railway services, regulatory obligations, or technical constraints.
- All exceptions shall be formally documented, risk assessed, approved, monitored, and reviewed prior to implementation.
- Unauthorized exceptions are strictly prohibited.

Objectives

- The Exception Management Process shall:
- Ensure deviations from security requirements are properly controlled.
- Minimize cybersecurity risks arising from policy exceptions.
- Maintain accountability and management oversight.
- Support business continuity while protecting information assets and railway operations.
- Ensure exceptions remain temporary and justified.

Scope

- This process applies to exceptions relating to:
- Cybersecurity policies
- Security standards
- Security procedures
- Access control requirements
- Cloud security requirements
- Network security controls
- Endpoint security controls
- Data protection requirements
- Operational Technology (OT) security controls
- Third-party security requirements

Circumstances for Requesting an Exception

- Exceptions may be requested when:
- Technical limitations prevent compliance.
- Business requirements necessitate a temporary deviation.
- Operational requirements require alternative controls.
- Vendor product limitations exist.
- Emergency operational situations occur.
- Regulatory or contractual obligations create conflicts.
- Exceptions shall not be used to permanently avoid compliance requirements.

Exception Request Submission

- All exception requests shall be submitted using the Cybersecurity Exception Request Form.
- The request shall include:

Requestor Information

- Name

- Department
- Position
- Contact information

Exception Details

- Policy or control requiring exception
- Description of the requested exception
- Business justification
- Systems or assets affected
- Duration of the exception

Risk Assessment Requirements

- Before approval, the Information Security Team shall conduct a risk assessment that includes:
- Threat analysis
- Vulnerability analysis
- Business impact assessment
- Operational impact assessment
- Safety impact assessment
- Regulatory impact assessment
- For railway operational environments, safety implications shall be assessed as part of the approval process.
-

Compensating Controls

- Where an exception is granted, compensating controls shall be identified and implemented.
- Examples include:
- Increased monitoring
- Additional logging
- Temporary network restrictions
- Enhanced access reviews
- Physical security enhancements
- Manual control procedures

Documentation Requirements

- The Information Security Team shall maintain an Exception Register containing:
- Exception ID
- Date submitted
- Requestor

- Business owner
- Risk rating
- Approval status
- Compensating controls
- Approval date
- Expiration date
- Review dates

Emergency Exceptions

- In urgent operational situations requiring immediate action:
- Temporary exceptions may be authorized by designated management.
- Risk assessments shall be completed as soon as practical.
- Formal approval documentation shall be completed within five (5) business days.
- Emergency exceptions shall not bypass safety-related controls without executive approval.

Sample Exception Request Form

- **Exception ID:** _____
- **Requestor:** _____
- **Department:** _____
- **Date Submitted:** _____
- **Policy/Control Reference:** _____
- **Business Justification:**

- **Affected Systems/Assets:**
- **Requested Duration:**
- **Compensating Controls:**
- **Risk Assessment Rating:**
- ☐ Low
- ☐ Medium
- ☐ High
- ☐ Critical

23.2 Approval and Review of Exceptions

Policy Statement

- All cybersecurity exceptions shall be approved by the appropriate authority based on the level of risk and potential impact to EDRSC's operations, information assets, railway infrastructure, and regulatory obligations.
- Approved exceptions shall be periodically reviewed to ensure they remain necessary and appropriate.

Approval Requirements

- No exception shall become effective until:
- Risk assessment has been completed.
- Compensating controls have been identified.
- All required approvals have been obtained.
- Exception documentation has been recorded.

Approval Authority Matrix

Risk Level	Approval Authority
Low	Department Manager
Medium	Department Head
High	Chief Digital Officer (CDO)
Critical	CEO and Executive Management

Additional Approval Requirements

- The following exceptions require Information Security Team review regardless of risk level:
- Access control exceptions
- Encryption exceptions
- Cloud security exceptions
- Third-party security exceptions
- Data protection exceptions
- Network security exceptions

Operational Technology (OT) Exceptions

- Exceptions involving:
- Signaling systems
- Train control systems
- SCADA systems
- Railway communication systems

- Power control systems
- shall require:
- Information Security Team approval
- Operational Department approval
- Safety review
- Chief Digital Officer approval
- For Critical-risk exceptions, CEO approval shall also be required.

Exception Validity Period

- All approved exceptions shall have a defined expiration date.
- Maximum recommended periods:

Risk Level	Maximum Duration
Low	12 Months
Medium	12 Months
High	6 Months
Critical	3 Months

- Extensions require re-evaluation and approval.

Periodic Review Requirements

- Approved exceptions shall be reviewed:

Risk Level	Review Frequency
Low	Annually
Medium	Semi-Annually
High	Quarterly
Critical	Monthly

- Reviews shall verify:
- Business justification remains valid.
- Risks remain acceptable.
- Compensating controls remain effective.
- Expiration dates are appropriate.

Exception Renewal

- If an exception remains necessary beyond its expiration:
- A new request shall be submitted.
- A new risk assessment shall be performed.

- Existing compensating controls shall be reviewed.
- Appropriate approvals shall be obtained.
- Automatic renewal is prohibited.

Exception Revocation

- EDRSC reserves the right to revoke an approved exception when:
- Business justification no longer exists.
- Risk increases beyond acceptable levels.
- Compensating controls fail.
- Regulatory requirements change.
- Security incidents arise related to the exception.
- Upon revocation, the affected system or process shall be brought into compliance as soon as practicable.

Reporting and Oversight

- The Information Security Team shall maintain and report:
- Number of active exceptions
- Expired exceptions
- Exception trends
- High and Critical-risk exceptions
- OT-related exceptions
- Exception compliance status
- Exception reports shall be provided:
- Quarterly to Executive Management
- Annually to the Board of Directors

Compliance

- Failure to comply with the Policy Exception Management process may result in:
- Revocation of access privileges
- Escalation to management
- Audit findings
- Disciplinary action
- Contractual penalties for third parties

24. Policy Review and Maintenance

24.1 Policy Review Schedule

Policy Statement

- Ethio-Djibouti Railway Share Company (EDRSC) shall establish, maintain, and periodically review all cybersecurity policies, standards, procedures, guidelines, and supporting documentation to ensure their continued effectiveness, relevance, and compliance with business, operational, legal, regulatory, and security requirements.
- Cybersecurity policies shall be reviewed regularly to address evolving cyber threats, technological advancements, operational changes, audit findings, and lessons learned from security incidents.

Objectives

- The policy review process shall ensure:
- Policies remain current and effective.
- Security requirements align with business objectives.
- Regulatory and legal requirements are reflected.
- New technologies and threats are addressed.
- Organizational responsibilities remain clearly defined.
- Continuous improvement opportunities are incorporated.

Review Triggers

- Policy reviews shall occur under the following circumstances:

Scheduled Reviews

- Annual cybersecurity policy review.
- Periodic review of standards, procedures, and guidelines.

Event-Driven Reviews

- Reviews shall also occur following:
- Major cybersecurity incidents.
- Significant security breaches.
- Regulatory changes.
- Organizational restructuring.
- Technology transformations.
- Major system implementations.
- Changes to railway operational environments.
- Audit recommendations.
- Material changes to business objectives.

Review Frequency

Document Type	Minimum Review Frequency
Cybersecurity Policy	Annually
Information Security Standards	Annually
Security Procedures	Annually
Incident Response Plan	Annually
Disaster Recovery Plan	Annually
Business Continuity Plan	Annually
OT Security Standards	Annually
Third-Party Security Policy	Annually
Access Control Standards	Annually

Roles and Responsibilities

Chief Digital Officer (CDO)

- The CDO shall:
- Oversee policy review activities.
- Ensure timely completion of reviews.
- Recommend policy updates.
- Present significant changes to Executive Management.

Information Security Team

- The Information Security Team shall:
- Coordinate policy reviews.
- Monitor regulatory and threat changes.
- Draft revisions and updates.
- Maintain document repositories.

Policy Owners

- Policy Owners shall:
- Review assigned documents.
- Confirm accuracy and relevance.
- Identify required changes.
- Participate in approval processes.

Executive Management

- Executive Management shall:
- Review major policy revisions.
- Approve strategic cybersecurity policy changes.
- Ensure alignment with business objectives.

Policy Review Documentation

- Each review shall document:
- Review date
- Reviewer names
- Summary of changes
- Reason for update
- Approval details
- Effective date
- Review records shall be retained in accordance with EDRSC Records Management requirements.

24.2 Version Control

Policy Statement

- EDRSC shall maintain formal version control procedures for all cybersecurity policies and related documentation to ensure document integrity, traceability, accountability, and availability.

Objectives

- Version control shall:
- Ensure only approved documents are used.
- Maintain historical records of changes.
- Support audits and regulatory reviews.
- Prevent unauthorized document modification.
- Ensure users access the most current version.

Version Numbering Convention

- The following version numbering standard shall be used:

Version	Description
1.0	Initial Release
1.1	Minor Revision
1.2	Minor Revision

2.0	Major Revision
3.0	Major Revision

Document Control Requirements

- Each cybersecurity document shall contain:
- Document title
- Policy owner
- Version number
- Approval authority
- Effective date
- Review date
- Classification level
- Document status

Version History Register

- A document revision history shall be maintained.

- **Sample Version History**

Version	Date	Description of Change	Prepared By	Approved By
1.0	01-Jan-2026	Initial Release	Information Security Team	CEO
1.1	15-Jun-2026	Updated Access Control Requirements	CDO	CEO
2.0	01-Jan-2027	Annual Policy Review and Major Update	Information Security Team	CEO

Document Repository

- Approved cybersecurity documents shall:
- Be stored in an authorized document management system.
- Be backed up regularly.
- Be protected against unauthorized access.
- Be accessible to authorized personnel.

Obsolete Documents

- Superseded documents shall:
- Be clearly marked as obsolete.
- Be removed from active use.
- Be archived securely.
- Be retained for audit and legal purposes.

Document Approval

- All cybersecurity policies and major revisions shall receive formal approval before publication.

Approval Authority

Document Type	Approval Authority
Cybersecurity Policy	CEO
Security Standards	CDO
Security Procedures	CDO
Guidelines	Information Security Manager

24.3 Continuous Improvement

Policy Statement

- EDRSC shall continuously improve its cybersecurity governance, policies, standards, procedures, controls, and capabilities to address evolving cyber threats, operational requirements, technological changes, and regulatory obligations.
- Continuous improvement shall form an integral component of the Information Security Management Program.

Objectives

- Continuous improvement activities shall:
- Enhance cybersecurity maturity.
- Reduce organizational cyber risk.
- Improve security control effectiveness.
- Strengthen resilience of railway operations.
- Improve incident detection and response.

- Support regulatory compliance.
- Promote security awareness across the organization.

Sources of Improvement

- Cybersecurity improvements may arise from:

Security Incidents

- Lessons learned from:
- Cybersecurity incidents
- Data breaches
- Malware events
- OT cybersecurity incidents
- Near-miss events

Audit Findings

- Results from:
- Internal audits
- External audits
- Regulatory inspections
- Compliance reviews

Risk Assessments

- Findings from:
- Enterprise risk assessments
- Vulnerability assessments
- Penetration testing
- Threat assessments

Security Monitoring

- Information from:
- SIEM systems
- Security Operations Center (SOC)
- Threat intelligence services
- Endpoint monitoring systems

Business and Technology Changes

- Examples:
- Cloud migration projects
- New railway technologies
- Infrastructure modernization
- New applications
- Digital transformation initiatives

Continuous Improvement Cycle

- EDRSC shall utilize the following improvement process:

Plan

- Identify weaknesses and opportunities.
- Define improvement objectives.
- Develop action plans.

Implement

- Deploy approved improvements.
- Assign responsibilities.
- Allocate necessary resources.

Monitor

- Measure effectiveness.
- Track implementation progress.
- Monitor performance indicators.

Review

- Assess outcomes.
- Evaluate risk reduction.
- Identify additional improvements.

Key Performance Indicators (KPIs)

- The Information Security Team shall monitor and report on cybersecurity performance using metrics such as:
- Number of cybersecurity incidents.
- Mean time to detect incidents.

- Mean time to respond to incidents.
- Vulnerability remediation rates.
- Patch compliance rates.
- Audit finding closure rates.
- Security awareness completion rates.
- Phishing simulation failure rates.
- OT security event trends.
- Third-party risk assessment completion rates.

Management Review

- Executive Management shall conduct an annual review of the cybersecurity program covering:
- Policy effectiveness.
- Risk management performance.
- Cybersecurity incidents.
- Compliance status.
- Audit findings.
- Resource adequacy.
- Strategic security initiatives.
- Continuous improvement opportunities.

Reporting

- The Information Security Team shall prepare periodic improvement reports containing:
- Improvement initiatives completed.
- Outstanding corrective actions.
- Cybersecurity performance metrics.
- Emerging risks.
- Recommendations for enhancement.
- Reports shall be submitted to:
- Chief Digital Officer (CDO)
- Executive Management
- Board of Directors

Continuous Improvement Register

- The Information Security Team shall maintain an Improvement Register documenting:
- Identified improvement opportunities
- Source of recommendation
- Responsible owner
- Target completion date
- Status of implementation

- Verification results

Compliance

- Failure to maintain or review cybersecurity policies and controls may result in:
- Increased cybersecurity risk.
- Audit observations.
- Regulatory non-compliance.
- Operational disruptions.
- Increased exposure to cyber threats.

25. Appendices

Sample Contents

- Asset Classification Matrix
- Password Standards
- Incident Severity Classification
- Security Contacts Directory
- Vendor Security Assessment Questionnaire
- Risk Assessment Methodology
- Cybersecurity Roles and Responsibilities Matrix

Example Cybersecurity Policy Approval Statement

Policy Owner: Chief Information Security Officer (CISO) / Chief Digital Officer (CDO)

Approved By: Chief Executive Officer (CEO)

Effective Date: //____

Review Date: //____

Version: 1.0

Approval Statement:

This Cybersecurity Policy establishes the minimum security requirements for protecting the organization's information assets. Compliance with this policy is mandatory for all employees, contractors, consultants, vendors, and third parties who access organizational information systems and data.

This structure is suitable for a medium-to-large enterprise and can be adapted for ISO 27001 certification, NIST CSF alignment, banking, telecom, government, or nonprofit organizations.

Appendices for Ethio-Djibouti Railway Share Company (EDRSC) Cybersecurity Policy

Appendix A: Cybersecurity Roles and Responsibilities Matrix

Role	Responsibilities
Board of Directors	Approve cybersecurity strategy, risk appetite, and provide oversight.
CEO	Ensure adequate resources and executive sponsorship for cybersecurity.
Chief Digital Officer (CDO)	Lead cybersecurity governance, risk management, compliance, and security programs.
IT Manager	Implement security controls, manage infrastructure, and ensure operational security.
Information Security Manager	Monitor threats, perform risk assessments, manage incidents, and ensure policy compliance.
OT/Signaling Manager	Secure railway operational technology, signaling, SCADA, and control systems.
Network Administrator	Manage network security devices and monitoring systems.
System Administrator	Secure servers, databases, operating systems, and backups.
Department Managers	Ensure staff comply with cybersecurity policies.
Employees	Follow policies, protect information assets, and report incidents.
Contractors	Comply with security requirements and contractual obligations.
Vendors	Maintain security controls and notify EDRSC of incidents affecting services.
Internal Audit	Independently assess cybersecurity controls and compliance.

RACI Matrix

Activity	Board	CEO	CDO	IT	Business Units
Security Strategy	A	C	R	C	I
Risk Assessment	I	C	A/R	R	C
Incident Response	I	C	A	R	C

Access Reviews	I	I	A	R	C
Policy Management	I	C	A/R	C	I

R = Responsible, A = Accountable, C = Consulted, I = Informed

Appendix B: Information Classification Standard

Classification Levels

Public

Information approved for public disclosure.

Examples

- Annual reports
- Published press releases
- Public railway schedules
- Marketing materials

Internal

Information intended only for EDRSC personnel.

Examples

- Internal procedures
- Organization charts
- Internal correspondence

Confidential

Information whose disclosure may negatively impact EDRSC.

Examples

- Financial reports
- Procurement data

- Personnel records
- Customer contracts

Restricted

Highly sensitive information whose compromise may impact railway safety or critical operations.

Examples

- Signaling system configurations
- SCADA configurations
- Railway control center information
- Network architecture diagrams
- Security incident reports
- Encryption keys

Data Handling Requirements

Classification	Storage	Transmission	Sharing
Public	No restriction	No restriction	Approved for public use
Internal	Company systems	Company email	Internal personnel
Confidential	Protected storage	Encryption required	Authorized personnel only
Restricted	Encrypted storage	Strong encryption required	Strictly need-to-know basis

Appendix C: Password Standard

Password Requirements

Standard User Accounts

- Minimum 12 characters
- Combination of upper and lower case letters
- At least one number
- At least one special character
- Must not contain employee name or username

Privileged Accounts

- Minimum 15 characters
- Unique password for each system
- MFA mandatory

Password Management Rules

Employees shall not:

- Share passwords
- Write passwords on paper
- Store passwords in unsecured files
- Reuse passwords across systems

Employees should:

- Use approved password managers
- Report suspected password compromise immediately
- Change passwords following compromise

Multi-Factor Authentication (MFA)

Mandatory for:

- VPN access
- Administrative access
- Cloud services
- Finance systems
- Email systems
- Remote access

Appendix D: Cybersecurity Incident Reporting Form

Section 1: Reporter Information

Name: _____

Department: _____

Email: _____

Phone Number: _____

Date Reported: _____

Section 2: Incident Details

Date of Incident: _____

Time of Incident: _____

Location/System Affected:

Section 3: Type of Incident

☐ Malware Infection

☐ Phishing Attempt

☐ Unauthorized Access

☐ Data Breach

☐ Denial of Service Attack

☐ System Failure

☐ Insider Threat

☐ Lost or Stolen Device

☐ OT/SCADA Incident

☐ Other

Specify:

Section 4: Incident Description

Provide detailed description:

Section 5: Impact Assessment

Affected Systems:

Business Impact:

Operational Impact:

Safety Impact:

Section 6: Immediate Actions Taken

Information Security Team Use Only

Incident ID: _____

Severity:

☐ Critical

☐ High

☐ Medium

☐ Low

Assigned Investigator:

Appendix E: Supplier Security Assessment Questionnaire

General Information

Vendor Name: _____

Service Provided: _____

Assessment Date: _____

Governance

1. Do you maintain an Information Security Program?

☐ Yes ☐ No

2. Do you have an Information Security Policy?

☐ Yes ☐ No

3. Is cybersecurity oversight assigned to senior management?

☐ Yes ☐ No

Compliance

4. Are you certified against any of the following?

☐ ISO 27001

☐ SOC2

☐ NIST

☐ Other

Specify:

Access Control

5. Do you enforce MFA?

☐ Yes ☐ No

6. Are privileged accounts monitored?

☐ Yes ☐ No

Vulnerability Management

7. Are vulnerability scans performed regularly?

☐ Yes ☐ No

8. Is annual penetration testing conducted?

☐ Yes ☐ No

Incident Management

9. Do you maintain incident response procedures?

☐ Yes ☐ No

10. Can incidents affecting EDRSC be reported within 24 hours?

☐ Yes ☐ No

Data Protection

11. Is sensitive information encrypted at rest?

☐ Yes ☐ No

12. Is sensitive information encrypted in transit?

☐ Yes ☐ No

Assessment Result

☐ Approved

☐ Approved with Conditions

☐ Rejected

Appendix F: Railway Operational Technology (OT) Security Standard

Objective

Protect railway operational technology environments from cyber threats while ensuring operational safety and reliability.

In Scope Systems

- Signaling Systems
- SCADA Systems
- Power Distribution Systems
- Traffic Management Systems
- CCTV Systems
- Train Communication Networks
- Control Center Systems

Security Requirements

Network Segmentation

OT networks shall be separated from IT networks through:

- Firewalls
- Demilitarized Zones (DMZ)
- Access Control Lists

Remote Access

Remote access shall:

- Be approved in advance
- Use MFA
- Be monitored and logged

Change Management

Changes to OT systems shall:

- Be formally approved
- Be risk assessed
- Be tested before deployment

Logging and Monitoring

All critical OT systems shall:

- Generate security logs
- Retain logs for at least 12 months
- Report anomalies to SOC personnel

Backup Requirements

Configuration backups shall occur:

- Weekly for critical systems
- Monthly validation testing

Appendix G: Business Continuity and Disaster Recovery Framework

Objectives

Ensure continuity of railway operations during emergencies.

Recovery Priorities

Priority	System
Priority 1	Train Control Systems
Priority 1	Signaling Systems
Priority 1	Communication Systems
Priority 2	Freight Operations
Priority 2	Passenger Systems
Priority 3	Corporate Systems

Recovery Targets

System Type	RTO	RPO
Train Control	2 Hours	15 Minutes
Signaling	2 Hours	15 Minutes
Communications	4 Hours	30 Minutes
ERP Systems	8 Hours	4 Hours
Email Services	12 Hours	4 Hours

Backup Requirements

- Daily Incremental Backups
- Weekly Full Backups
- Monthly Recovery Testing
- Offsite Backup Storage
- Annual Disaster Recovery Exercises

Crisis Management Team

- CEO
- CDO
- Operations Director
- IT Manager
- Communications Officer
- Security Manager

Appendix H: Cybersecurity Risk Assessment Methodology

Risk Assessment Process

Step 1: Asset Identification

Identify:

- Information assets
- Systems
- OT infrastructure
- Data repositories

Step 2: Threat Identification

Examples:

- Ransomware
- Insider threats
- State-sponsored attacks
- Supply-chain attacks
- Power outages
- OT system compromise

Step 3: Vulnerability Identification

Determine weaknesses such as:

- Unpatched systems
- Weak passwords
- Misconfigurations
- Inadequate monitoring

Step 4: Risk Analysis

Likelihood Scale

Score	Description
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

Impact Scale

Score	Description
1	Insignificant
2	Minor
3	Moderate
4	Major
5	Severe

Risk Formula

Risk Score = Likelihood × Impact

Risk Matrix

Score	Risk Level
1-4	Low
5-9	Medium
10-16	High
17-25	Critical

Treatment Options

- Mitigate
- Transfer

- Avoid
- Accept

Reporting Requirements

- Quarterly risk reviews
- Annual enterprise cybersecurity risk assessment
- Executive reporting to management
- Immediate escalation of Critical risks

Document Control

Version	Date	Description	Approved By
1.0	YYYY-MM-DD	Initial Release	CEO
1.1	TBD	Annual Review	CEO

End of Appendices for Ethio-Djibouti Railway Share Company Cybersecurity Policy.