A black and white logo

Description automatically generated

Metropolis Transit corporation

Human Resource security policy.

Contents

[**Policy Statement** 2](#_Toc149923664)

[Prior to Employment 2](#_Toc149923665)

[During Employment 2](#_Toc149923666)

[Management Responsibilities 3](#_Toc149923667)

[New Joiners. 3](#_Toc149923668)

[Transfer. 3](#_Toc149923669)

[Disciplinary Process. 3](#_Toc149923670)

[Access Review. 3](#_Toc149923671)

[End of Employment. 4](#_Toc149923672)

[**Owner of the policy** 5](#_Toc149923673)

[**Compliance** 5](#_Toc149923674)

[Procedure 5](#_Toc149923675)

[Measurement 5](#_Toc149923676)

[**Update and Review the policy** 5](#_Toc149923677)

# **Policy Statement**

## Prior to Employment

* + 1. The organization shall conduct appropriate personnel background checks “screening and vetting” under Jordan laws and regulations.
    2. Such background and screening checks shall include at least:
       1. Identity checks through documents such as a passport or Jordanian ID.
       2. Validation of qualifications and certifications.
       3. Evidence of previous employment, where applicable.
       4. All the organization staff shall sign a Non-Disclosure Agreement (NDA).
    3. As part of a non-disclosure agreement, the individual shall confirm to ensure confidentiality of organization information during their association with Metropolis afterward.

## During Employment

* + 1. All the organization staff understand their duties & responsibilities and job expectations in terms of job security matters, to reduce the risk of theft, fraud, or misuse of computing facilities, and to apply security following established policies and procedures.
    2. Security roles and responsibilities of staff shall include at least the requirement to:
       1. Protect assets from unauthorized access, disclosure, modification, destruction, or interference.
       2. Execute particular security processes or activities.
       3. Ensure responsibility is assigned to the individual for actions taken.
       4. Report security events or potential events or other security risks to the Information Security Section.
       5. It is the responsibility of the organization employees and contractors to report any suspicious activity.

## Management Responsibilities

* + 1. Direct Managers shall ask all users who are working under their supervision to apply security policies and procedures.
    2. Direct Managers are responsible for reporting any observed behavioral changes of the staff under supervision that may lead to a security violation/breach.
    3. Direct Managers shall ensure that staff vacations do not affect the availability and performance of services.

## New Joiners.

* + 1. Information Technology Department is responsible for the creation of a new user for Active Directory and Email as well as creating Access Card for new joiners.

## Transfer.

* + 1. Once a staff is transferred within the organization or changed the responsibility of the staff, HR shall immediately start the transferring process.

## Disciplinary Process.

* + 1. HR shall inform employees of the disciplinary actions that may be taken against them if they violate policies, disclose 'Secret or confidential' information, or attempt to exploit any vulnerability to gain access to or extract information that the person is not authorized to view or process.

## Access Review.

* + 1. The HR Department, in coordination with the InfoSec Section, should ensure that every access authorized is evaluated by the asset owner at least once a year.

## End of Employment.

* + 1. In case of a staff member is leaving the organization, the HR Department shall immediately inform the Information Technology Department to revoke/disable the access using traceable.
    2. Leave can be due to one of the below types but is not limited to:
       1. Resignation.
       2. End of contractor/consultant contract.
       3. Termination.
       4. Retirement.
       5. Death.
       6. Law case: Condemned, convicted, or sentenced with a law case.
       7. IS Incident: Breaching policies or procedures.
    3. Where applicable, a clearance process shall be initiated by HR, where at least the below shall be performed to return the organization information.
       1. Users shall return all assets in their custody and leavers’ access shall be revoked before signing the exit clearance form.
       2. Hand over all information assets including technology and telecommunication devices/equipment.
       3. Hand over all documents.
       4. HR Department shall inform staff on notice period that all ‘Secret or confidential’ information shall not be disclosed during the period identified in the NDA.
       5. If the person is terminated, the access shall be immediately revoked, and the terminated staff shall be escorted by physical security personnel outside the organization premises.

# **Owner of the policy**

The owner of the policy is Human Resource team that their responsibility focuses on the Enforcement and Consequences by working beside the ISO to enforce security policies and address violations They should establish clear consequences for policy violations and ensure consistent enforcement. As well as providing security awareness and training programs.

# **Compliance**

## Procedure

The HR security policy should clearly outline the steps employees and relevant personnel need to take to ensure compliance with ISO27001 as well as PCI-DSS to protect the credit card data when buying bus ticket. This might include instructions on how to handle sensitive data, maintain secure access, and report security incidents. This might involve using tools or systems for data collection, surveys, or periodic assessments.

## Measurement

The compliance with the policy will be measured based on KPI, which they will be for the HR the percentage of employees who have completed security training, the number of reported security incidents, or the status of access control reviews. The compliance is audited frequently and should be supervised by the CISO and HR team by random check.

# **Update and Review the policy**

Specify who is responsible for maintaining and updating the HR security policy. This could be the Chief Information Security Officer (CISO) and the HR manager that is conducted annually or whenever change occur in the organization or the regulations and standards that the organization want to comply with.

If there is a need to update that should follow a specific procedure:

1. Initiation of Updates:

Anyone within the organization can propose updates to the operational management policy. This could be based on changes in technology, regulatory requirements, security threats, or feedback from employees or stakeholders.

1. Review Proposal:

A review committee or designated individuals responsible for policy updates should evaluate the proposed changes. This review committee may include representatives from IT, IT security, compliance, and other relevant departments.

1. Impact Assessment:

Assess the potential impact of the proposed changes on the organization, including its operational procedures and responsibilities. Consider the benefits, risks, and resource implications of the updates.

1. Drafting Updates:

If the proposed changes are approved during the review, draft the updated sections of the policy. Ensure that the language is clear, specific, and aligned with the organization's goals and regulatory requirements.

1. Approval Process:

Clarify the approval process, including the individuals or roles responsible for granting final approval. This could be the CIO, CISO, or other relevant executive roles. All proposed changes should be reviewed and approved before implementation.

1. Documentation and Communication:

Maintain comprehensive documentation throughout the update process. This documentation should include records of discussions, decisions, impact assessments, and approvals, communicate the changes to all relevant stakeholders. This could involve distributing the revised policy, conducting training sessions, or providing awareness campaigns to ensure that employees understand the changes.

1. Implementation:

Implement the approved changes in line with the policy updates. Ensure that all operational procedures and responsibilities are aligned with the updated policy.

1. Monitoring and Auditing:

Establish monitoring and auditing procedures to ensure that the updated policy is effectively implemented and that compliance is maintained. Regularly review and assess compliance with the new policy.

1. Feedback Mechanism:

Provide a mechanism for employees and stakeholders to provide feedback on the updated policy. This feedback can be valuable for ongoing improvement and ensuring that the policy remains effective.

1. Review Schedule:

Specify how often the updated policy will be reviewed for further updates. This could be done annually or at other intervals as necessary, and track changes to the policy over time.