Draft 6.7 Termination of Access IT Policy

Purpose:

The purpose of this policy is to establish guidelines and procedures for terminating access to the organization's IT systems, network, and data, for employees, contractors, consultants, and other authorized users, when their access is no longer required, or when their employment or engagement with the organization is terminated.

Scope:

This policy applies to all employees, contractors, consultants, and other authorized users who have access to the organization's IT systems, network, and data.

Policy:

Access to the organization's IT systems, network, and data may be terminated at any time and will be carried out in accordance with the organization's security policies and procedures.

The employee's manager or the authorized personnel responsible for managing the contractor, consultant, or other authorized is responsible for providing immediate written notification of terminations to the IT department or other designated personnel responsible for revoking or disabling access.

When an employee, contractor, consultant, or other authorized user's employment or engagement is terminated, their access to the organization's IT systems, network, and data will be revoked or disabled immediately.

All access credentials, including usernames, passwords, and other authentication methods will be deactivated, or deleted, upon termination of employment.

The IT department or other designated personnel will be responsible for revoking or disabling access to the organization's IT systems, network, and data upon termination of employment, contract, or engagement or as otherwise required.

The IT department or other designated personnel will confirm that access has been revoked or disabled.

Any equipment or devices such as laptops, smartphones, or tablets, that were issued to the employee, contractor, consultant, or other authorized user, will be collected, and returned to the IT department or other designated personnel upon request.

The IT department or other designated personnel will ensure that all data and software licenses belonging to the organization are removed from any equipment or devices returned by the employee, contractor, consultant, or other authorized user.

The organization will maintain a record of access termination for each employee, contractor, consultant, or other authorized user.

Exceptions:

Exceptions to this policy may be granted, on a temporary basis, by the IT department or other designated personnel in cases where access is required to complete a specific task or project after termination of employment, contract, or engagement. Any exceptions must be authorized in writing and will be subject to the organization's security policies and procedures and will be reviewed regularly to ensure that access is till required.

Enforcement:

Any violation of this policy may result in disciplinary action, up to and including termination of employment, contract, or engagement, and may also result in legal action in accordance with applicable laws and regulations.

Review:

This policy will be reviewed and updated as needed, but at least annually, by the IT department or other designated personnel responsible for managing access to the organization's IT systems, network, and data.