Administrative Access Policy

Overview:

Certain members of the **<<INSERT ORG NAME>>** staff may have the need for administrative access privileges. The fact that these administrative access users have a higher level of access means that granting, controlling, managing, and monitoring these accounts is extremely important to the security program and must be used appropriately. The Administrative Access Policy prohibits using a **<<INSERT ORG NAME**>> system without proper authorization granted through the HR department or departmental management. It further prohibits attempts to bypass system security without the explicit permission from management.

Scope:

This policy applies to all associates, interns, contractors, and third-party users who have been granted administrative access to **<<INSERT ORG NAME>>** 's systems.

Purpose:

The purpose of this policy is to define the responsibilities and acceptable use of administrative access to critical systems within the organization, including but not limited to **<<INSERT APPLICATION NAMES>>** and any additional system relevant to each department's responsibilities. Administrative access users are expected to use their access solely for tasks related to their job responsibilities and to uphold the highest standards of security and confidentiality.

Policy Guidelines:

- Administrative access:
    - Must be used strictly for authorized purposes related to the user's job role and responsibilities
    - Must not be used to gain unauthorized knowledge, make unauthorized changes, or access data/non-public information that is outside the scope of the user's specific job responsibilities
    - Must not be used to satisfy personal curiosity about an individual, system, practice, or other type of entity

- Administrative access users:
    - Must not share their credentials (usernames, passwords, multi-factor authentication codes, etc.) with any other individual, regardless of their role within the organization
    - Are responsible for ensuring that their login credentials are secure and must immediately report any suspected compromise of their credentials to their direct management
    - Must respect the confidentiality of all data accessed in the course of their duties/employment and must not use administrative access to expose or otherwise disclose non-public information to unauthorized persons (unless specifically permitted by a relevant authority)
    - Must ensure compliance with all applicable laws, regulations, and organizational policies regarding data security and privacy
    - Must report any suspicious or unauthorized actions within the system or of other users to direct management immediately

- Must be aware of the impact of any changes made to the systems and seek necessary approvals when required

Violation of The Administrative Access Policy:
<<INSERT ORG NAME>> reserves the right to monitor and audit the activities of all administrative access users to ensure compliance with this policy. Administrative access users must cooperate with any internal or external audits and investigations. Any associate who has been found to misuse their administrative access and/or responsibilities, including but not limited to unauthorized access, data breaches, not reporting suspicious activity/violations of other users, or sharing of confidential information, may be subject to deactivation of their administrative access and/or disciplinary action, up to and including termination of employment.

Acknowledgment:
All administrative access users must sign and acknowledge their understanding of this policy, their agreement to comply with its terms, and their awareness of the consequences of non-compliance.

First and Last Name:

Signature:

Today's Date: