Whistleblowing Solutions AB, Access management policy

Version	Approved	Date	Approver	Key changes
1.0	Approved	2022-01-19	Klas Karlsson	Created

1. Policy statement

Protecting access to IT systems and applications is critical to maintain the integrity of the Whistleblowing Solutions AB technology and data and prevent unauthorized access to such resources. Access to Whistlelink systems must be restricted to only authorized users or processes, based on the principle of strict need to know and least privilege.

2. Background

Access controls are necessary to ensure only authorized users can obtain access to all Whistleblowing Solutions AB information and systems. Access controls manage the admittance of users to system and network resources by granting users access only to the specific resources they require to complete their job-related duties.

3. Policy Objective

The objective of this policy is to ensure Whistleblowing Solutions has adequate controls to restrict access to systems and data.

4. Scope

This policy applies to:

- All stakeholders with access to any Whistleblowing Solution system
- All employees, consultants, contractors, agents, and authorized users accessing Whistleblowing Solutions IT systems and applications.
- All IT systems or applications managed by Whistleblowing Solutions that store, process or transmit information, including network and computer hardware, software, and applications, mobile devices, and telecommunication systems.

5. Definitions

- "Access Control" is the process that limits and controls access to resources of a computer system.
- "Users" are employees, consultants, contractors, agents and authorized users accessing Whistleblowing Solutions AB IT systems and applications.
- "System or Application Accounts" are user ID's created on IT systems or applications, which are associated with specific access privileges on such systems and applications.
- "Privileged Accounts" are system or application accounts that have advanced permissions (as compared to regular user account permissions) on such systems or applications. Examples of user accounts with privileges include: administrative and super user accounts.
- "Access Privileges" are systems permissions associated with an account, including permissions to access or change data, to process transactions, create or change settings, etc.
- "Administrator Account" is a user account with privileges that have advanced permissions on an IT system that are necessary for the administration of this system. For example, an administrator account can create new users, change account permissions, modify security settings such as password settings, modify system logs, etc.
- "Application and Service Accounts" are user accounts that are not associated with a person but an IT system, an application (or a specific part of an application) or a network service.
- "Nominative User Accounts" are user accounts that are named after a person.
- "Non-disclosure Agreement" is a contract between a person and Whistleblowing Solutions stating that the person will protect confidential.

6. Guiding Principles – General Requirements

- Whistleblowing Solutions AB will provide access privileges to Whistlelink technology (including networks, systems, applications, computers and mobile devices) based on the following principles:
    - Need to know – users or resources will be granted access to systems that are necessary to fulfil their roles and responsibilities.
    - Least privilege – users or resources will be provided with the minimum privileges necessary to fulfil their roles and responsibilities.
- Requests for users' accounts and access privileges must be formally documented and appropriately approved.
- Requests for special accounts and privileges (such as vendor accounts, application and service accounts, system administration accounts, shared / generic accounts, test accounts and remote access) must be formally documented and approved by the system owner in User Account access document (current owner Information Security manager)
- Application and service accounts must only be used by application components requiring authentication; access to the passwords must be restricted to authorized IT administrators or application developers only.
- Where possible, Whistleblowing Solutions AB will set user accounts to automatically expire at a pre-set date. More specifically,
    - When temporary access is required, such access will be removed immediately after the user has completed the task for which the access was granted.

    - User accounts assigned to contractors will be set to expire according to the contract's expiry date.
- Access rights will be immediately disabled or removed when the user is terminated or ceases to have a legitimate reason to access Whistleblowing Solutions AB.
- A verification of the user's identity must be performed by Support or designate before granting a new password.
- Existing user accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges. Examples of accounts with excessive privileges include:
    - An active account assigned to external contractors, vendors or employees that no longer work for Whistleblowing Solutions AB.
    - An active account with access rights for which the user's role and responsibilities do not require access. For example, users that do not have authority or responsibility to approve expenses should not have access with approval permissions within a financial system.
    - System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not an administrator.
- All access requests for system and application accounts and permissions will be documented using the Excel document in place.

7. Guiding Principles – Privileged Accounts

- A nominative and individual privileged user account must be created for administrator accounts (such as "first_name.last_name"), instead of generic administrator account names.
- Privileged user accounts can only be requested by managers or supervisors and must be appropriately approved.
- A nominative and individual privileged user account must be created for administrator accounts (such as "first_name.last_name"), instead of generic administrator account names.
- Privileged user accounts can only be requested by managers or supervisors and must be appropriately approved.

8. Guiding Principles – Shared User Accounts

- Where possible, the use of specific network domain "security groups" should be used to share common access permissions across many users, instead of shared accounts
- Shared user accounts are only to be used on an exception basis with the appropriate approval. This includes general user accounts such as "guest" and "functional" accounts
- When shared accounts are required:
    - Passwords will be stored and handled in accordance with the Password Policy (Lastpass and shared without password visibility).
    - The use of shared accounts will be monitored where possible and revoked when no longer needed.

9. Vendor or Default User Accounts

Where possible, all default user accounts will be disabled or changed. These accounts include “guest”, “temp”, “admin”, “Administrator”, and any other commonly known or used default accounts, as well as related default passwords used by vendors on “commercial off-the shelf” systems and applications.

10. Test Accounts

- Test accounts can only be created if they are justified by the relevant business area or project team and approved by the application owner, through a formal request to the information Security Manager
- Test accounts will be disabled / deleted when they are no longer necessary.

11. Contractors and Vendors

- Contracts with contractors / vendors will include specific requirements for the protection of data. In addition, contractor / vendor representatives will be required to sign a Non-disclosure Agreement (“NDA”) prior to obtaining approval to access Whistleblowing Solutions systems and applications.
- Prior to granting access rights to a contractor / vendor, the Information Security manager must verify the requirements of Section 11.1 have been complied with.
- Whistleblowing Solutions will maintain a current list of external contractors or vendors having access to Whistlelink systems.

12. Access Control Requirements

- All users must use a unique ID to access Whistlelink systems and applications. Passwords must be set in accordance with the Password Policy.
- Alternative authentication mechanisms that do not rely on a unique ID and password must be formally approved.
- Access to Whistlelink systems and applications must use two-factor authentication where possible.
- System and application sessions must automatically lock after 15 minutes of inactivity.

13. Roles and Responsibilities

Stakeholders	Responsibilities
CEO	Approve and formally support this policy
CTO	Develop and maintain this policy. Review and approve any exceptions to the requirements of this policy. Take proactive steps to reinforce compliance of all stakeholders with this policy.
Contract Administrators	Ensure that the responsibilities and security obligations of each party to the contractual relationship are outlined in the contract

	executed between Whistleblowing Solutions and the contractor/sub-contractor.
All users (Employees and contractors)	Report all non-compliance instances with this policy (observed or suspected) to their Supervisor or Company employee as soon as possible.