EDW Application Account Guidelines and Procedures

Application (Service) Accounts

Application Accounts for Secure Access

Application accounts are designated credentials specifically created for use by a computer application or a group of related applications. Application accounts are particularly valuable in environments where scheduled applications, such as those retrieving data from the Data Warehouse, require secure and consistent access.

In many units, multiple technical staff may support a single application. Utilizing individual accounts in such cases often leads to the sharing of personal credentials, which directly contravenes University security policies. This practice compromises security, accountability, and auditability, emphasizing the importance of using application-specific accounts in these scenarios.

Maintaining Accountability and Security

A key purpose of the University policy is to ensure accountability by maintaining accurate records of the individual responsible for any activity associated with an application account. This is critical in the event of a security or confidentiality violation. To uphold this accountability, users are strictly prohibited from sharing usernames and passwords under any circumstances.

Guidance for Application Account Owners

Application accounts owners must familiarize themselves with relevant policies and best practices to ensure compliance and safeguard data. For further information, refer to the **Campus Administrative Manual** and the appropriate **University Privacy and Cyber Security Policy** documents. These resources provide detailed guidance on security policies, requirements, and best practices.

Guidelines

Issuance and Accountability of Application Accounts

AITS - Decision Support will issue application accounts to individuals for use with specific applications. Each account will be assigned a **single primary application account owner**, who is fully accountable for all activities conducted under the account, just as they are for their personal accounts.

In cases where multiple individuals support an application and require access to the application account, each must be identified to AITS - Decision Support as **secondary owners** or **technical contacts**. The primary owner is responsible for ensuring that secondary owners and technical contacts comply with University policies regarding the use of the application account.

It is **important to note** that the purpose of application account is not to serve as a shared account to circumvent the need for individual user accounts. Shared accounts are strictly prohibited under the **University Information Security Policy** and are a violation of established security protocols.

Unit Roles and Responsibilities

- **Security Compliance:**
  The individual assigned an application account is responsible for ensuring its use aligns with the

unit's security procedures. Applications accessing secured data from the Data Warehouse must have a defined security plan to maintain appropriate access as data transitions from the central database to local use. Units are responsible for periodically reviewing the effectiveness of their security plans.

- **Accountability:**
  As with personal accounts, the individual assigned an application account is fully accountable for all activities conducted under that account. This includes managing secured data shared through the application and maintaining the data's security classification during distribution, similar to responsibilities when sharing data via reports, spreadsheets, or other methods.

- **Reassignment of Primary Application Account Owner:**
  If the individual designated as the primary application account owner leaves the University or transfers to another department, the application account may remain active but must be reassigned to another individual within the unit. When reassigned, the password must be changed. Application accounts that have not been reassigned may be suspended or terminated during routine maintenance. Requests for reassignment should be processed through the **Unit Security Contact**.

- **Secondary Users:**
  Secondary users assigned to support an application using the application account have the same responsibilities to ensure proper use of secured data. All secondary users must be designated to **AITS - Decision Support**.

- **Security Practices for Account Credentials:**
  - Account names and passwords must not be hardcoded into programs or queries unless encrypted or otherwise secured.
  - Passwords for application accounts should be updated periodically. Account owners should document and follow local system-specific steps for password changes and ensure these are completed whenever the application account password is updated.

- **Data Security Compliance:**
  When sharing data with third parties (e.g., vendors or contractors), additional compliance requirements may apply, especially for sensitive data. The individual assigned the account must consult with their university's security office to verify compliance with requirements such as SOC 2 or HIPAA Business Associate Agreements.

- **Least Privilege Security Practices:**
  To minimize data exploitation risks, application accounts should follow least privilege principles. Units should request separate application accounts with tailored data access permissions for each integration rather than reusing highly privileged accounts across multiple business systems. Using distinct accounts reduces service interruption risks during password updates and enhances overall security.

Central Roles and Responsibilities

- Guidance on Security Status:

AITS is responsible for addressing questions regarding the security status of Data Warehouse data to enable units to:

- Implement appropriate security measures within their application's security plan.
- Ensure application account users handle data appropriately.

- Creation and Maintenance of Application Accounts:
  AITS creates application accounts based on the unit's needs. The initial review of the service, its roles, and procedures typically occurs once. If the unit changes the individuals or number of users involved, AITS assumes the established usage and processes remain consistent. Review of application functionality itself is beyond the scope of this policy. Requests to modify data access follow the same process as individual account access requests.

- Approval of Restricted or Protected Data Access:
  Data stewards affiliated with each University must review and approve access requests for restricted or protected data as appropriate.

- Policy Interpretation:
  The Information Technology Leadership Team (IT LT) and AITS will collaborate on interpretations of the University Information Security Policy concerning application accounts for the Data Warehouse.

- Audit and Oversight:
  The Office of University Audits may review the unit's controls over system access and information use, disclosure, modification, or loss as part of its auditing responsibilities for information security.

- Training and Monitoring Compliance:
  IT LT members are responsible for:
  - Providing procedures for data owners, data custodians, network and system administrators, and users.
  - Implementing procedures aligned with University Information Security policies and monitoring compliance with these policies.

- Deactivation of Inactive Accounts:
  AITS reserves the right to deactivate any application account with no connectivity for at least 24 months. Reactivation requires the Unit Security Contact to submit a new request for the account.