# Guidelines on User Access Management

User Access Management is the process of creating, managing, and securing user accounts on software systems. It ensures that only authorized personnel can access government systems, protects sensitive data, and maintains accountability. This section outlines the mandatory procedures, standards, and best practices that every government institution must follow to manage user access effectively.

## Authorized Access [Mandatory]

Ensure that only legitimate, authorized users can access government software applications according to their job roles and responsibilities.

**Step-by-Step Procedures:**

- Define user roles and responsibilities before granting access.
- Submit an Access Request Form approved by the user's supervisor or department head.
- The IT administrator reviews the request for necessity, role alignment, and risk.
- Access is granted based on the principle of least privilege (users only get access needed to perform their duties).
- Maintain a user access register with details of all users, roles, and permissions.

| Do's | Don'ts | Practice |
|---|---|---|
| Do verify each user's identity before granting access. | Don't grant administrative rights unless necessary. | Implement role-based access control (RBAC). |
| Do review access rights periodically (every 3–6 months). | Don't approve access requests without written authorization. | Automate access approval and logging through identity management tools. |
| | | Require annual user access recertification. |

## Termination of User Accounts [Mandatory]

Prevent unauthorized access from former employees, contractors, or temporary users.

**Procedures:**

- HR or department heads must immediately notify the IT department when an employee resigns, transfers, or is terminated.
- IT staff must disable or delete the user account within 24 hours of notification.
- Remove associated access rights, including email, VPN, cloud services, and databases.
- Transfer or archive the user's data according to the institution's data retention policy.
- Conduct quarterly audits to detect dormant or unauthorized accounts.

| Do's | Don'ts | Practice |
|---|---|---|
| Do confirm account termination with written acknowledgment from HR. | Don't leave inactive accounts enabled. | Use an automated deprovisioning system linked to HR exit workflows. |
| Do maintain a record of all deactivated accounts. | Don't reuse deleted usernames without clearance. | |

## Third-Party Access [Mandatory]

Ensure that external vendors or partners access government software systems securely and temporarily.

**Procedures:**

- Require third parties to sign a Confidentiality and Non-Disclosure Agreement (NDA).
- Access must be formally requested and approved for a specific purpose and time frame.
- Create a dedicated account for the third party with limited privileges and log all activities.
- Monitor sessions in real time, especially for production environments.
- Disable access immediately after task completion.

| Do's | Don'ts | Practice |
|---|---|---|
| Do verify the identity and legitimacy of all third-party users. | Don't provide administrative credentials. | Use a secure remote access gateway or jump server for vendor sessions. |
| Do audit third-party access logs monthly. | Don't allow shared or unmonitored VPN connections. | |

## Generic or Shared User Accounts [Mandatory]

Maintain accountability by ensuring all actions on systems are traceable to an individual user.

**Procedures:**

- Prohibit creation of shared or generic accounts.
- All users must have unique credentials.
- If a shared account is unavoidable, document who used it, when, and for what purpose.
- Implement enhanced logging and multi-factor authentication (MFA) for such accounts.

| Do's | Don'ts | Practice |
|---|---|---|
| Do maintain accountability records for exceptional shared access. | Don't use shared accounts for daily operations | Integrate systems with centralized directory services (e.g: Active Directory) to enforce identity traceability. |

## Securing Login Credentials [Mandatory]

Protect user credentials from unauthorized disclosure or misuse.

**Procedures:**

- Users must create strong passwords according to institutional policy.
- Never write passwords on paper or share them verbally or electronically.
- Change passwords immediately if a breach is suspected.
- IT teams should encrypt passwords in storage and transmission.

| Do's | Don'ts | Practice |
|---|---|---|
| Do use password managers approved by the IT department. | Don't reuse passwords across systems. | Implement automatic password rotation for privileged accounts. |
| Do lock your screen when away from your workstation | Don't disclose login credentials via email or chat. | |

## Password Policies [Mandatory]

Ensure consistent and secure password management across all systems by following the Standards (based on NIST SP 800-63B):

- Minimum length: 8–12 characters.
- Must include uppercase, lowercase, numbers, and special characters.
- Password expiry: every 90 days (or use continuous monitoring if MFA is enforced).
- Lockout after three (3) failed attempts.

**Procedures:**

- IT administrators configure password policies in all systems.
- Users are informed during onboarding.
- Systems log password change history for auditing.

| Do's | Don'ts | Practice |
|---|---|---|
| Do encourage use of passphrases. | Don't force frequent unnecessary password changes (unless a breach occurs). | Adopt adaptive authentication where risk-based password validation is applied. |

## Multi-Factor Authentication (MFA) [Mandatory]

Enhance security by requiring more than one factor of authentication.

**Procedures:**

- Implement MFA for all high-privilege accounts and sensitive applications.
- Combine at least two of the following:
- Something you know (password).
- Something you have (security token or code).
- Something you are (biometric trait).
- Provide users with setup guidance and recovery options.

| Do's | Don'ts | Best practice |
|---|---|---|
| Do enforce MFA for VPN, email, and system admin logins. | Don't allow exceptions without written approval from IT Security. | Regularly review and update MFA settings to ensure only authorized users have active access. |

## Biometrics [Recommended]

Add an additional layer of user authentication to enhance security and convenience.

**Procedures:**

- Implement biometric authentication (fingerprint, face, or iris recognition) in systems supporting it.
- Ensure compliance with Rwanda's Data Protection and Privacy Law for biometric data handling.
- Provide alternative authentication for users who opt out of biometrics.
- Store biometric templates securely using encryption and hashing techniques.

| Do's | Don'ts | Practice |
|---|---|---|

| | | |
|---|---|---|
| Do inform users about how their biometric data is used and stored. | Don’t use biometric data for non-authentication purposes. | Combine biometric authentication with MFA for sensitive or high-security systems. |
| Do restrict biometric data access to authorized security personnel only. | | |

Revision #2
Created 14 October 2025 08:42:27 by RISA
Updated 14 October 2025 09:02:37 by RISA