**New User Credential Commissioning Document**

**1. Introduction**

Defines the process for creating and managing user credentials securely.

**2. Purpose**

Ensures credential provisioning follows security policies and regulatory compliance.

**3. Scope**

Applies to all users, systems, and remote connections requiring authentication.

**4. New User Credential Commissioning Process**

**4.1 Request & Approval**

* **Request Form Submission:** The new user or their manager submits a credential request form to the IT department.
  + The form should include the user's name, department, line manager, and required access.
  + **Acceptable Use Policy:** The user must acknowledge and agree to the company's Acceptable Use Policy as part of the request form submission.
* **Approval Confirmation:** An authorized manager reviews and approves the request.
  + The manager verifies the request details and signs off on the approval.

**4.2 Credential Creation**

* **Validation of Details:**
  + **Cost Centre:** Ensure the cost centre is accurate and has the necessary budget allocation.
  + **Department Association:** Confirm the user's department and its validity.
  + **Line Manager:** Validate the line manager's authorization.
  + **Basic Services Required:** Identify the basic services needed, such as email and internet access.
  + **Assigned Role:** Determine the user's role and associated permissions.
  + Cross-check the details with HR records and the corporate directory.
  + **Vulnerability Management Procedures:** Ensure that any software or systems the new user will access have been assessed for vulnerabilities and are compliant with security policies.
* **Create Requests for Basic Services:**
  + **Network Username:** Assign a unique network username.
  + **Password Construction Guidelines:** Ensure the initial password meets the company's password construction guidelines (e.g., minimum length, complexity requirements, expiration policy).
  + **Email Account:** Set up the user's email account.
  + **Collaboration Tools:** Provide access to collaboration tools like Teams or Slack.
  + **Basic Internet Access:** Ensure internet access is enabled.
  + **Time Reporting Access:** Grant access to time reporting systems.
  + **Intranet Access:** Provide access to the company's intranet.
  + **Training System Access:** Enrol the user in mandatory training programs.
  + Use automated provisioning systems to set up these services.
* **Create Requests for Role-Based Application Access:** If specified, create requests for role-based application access.
  + Provide access to specific applications or databases based on the user's role.
  + **Acceptable Use Policy:** Ensure the user understands and agrees to the acceptable use of role-based applications.

**4.3 Secure Delivery**

* **Validation of Fulfilment:** Validate that all requested services have been provisioned in accordance with Operational Level Agreements (OLAs).
  + Check provisioning logs and confirm that all services are active and accessible.
  + **Information Logging Standards:** Ensure that all access and provisioning activities are logged in accordance with the company's information logging standards.
* **Track Completion:** Track the completion of all service fulfilments.
  + Maintain a checklist or project management tool to monitor progress.
  + **Information Logging Standards:** Maintain accurate logs of the provisioning process for auditing and compliance purposes.
* **Secure Credential Storage:** Deposit credential details in a secure location.
  + Store passwords and sensitive information in an encrypted password manager.
  + **Password Construction Guidelines:** Ensure the storage method complies with password security best practices.

**4.4 Onboarding & Training**

* **Notification of Completion:** Notify the line manager that the credential provisioning is complete and credentials are available.
  + Send an email notification with the details of the provisioned services.
  + **Acceptable Use Policy:** Include a reminder about the Acceptable Use Policy and any relevant security guidelines.

**4.5 Access Review**

* Periodically review user access to ensure it aligns with current roles and responsibilities.
  + **Information Logging Standards:** Ensure regular audits and reviews of access logs to detect and address any anomalies.

**4.6 Offboarding**

* Disable credentials when they are no longer needed or if the user leaves the organization.
  + **Vulnerability Management Procedures:** Ensure the removal of access to all sensitive systems and data to prevent unauthorized access.

**5. Roles & Responsibilities**

| **Role** | **Responsibility** |
| --- | --- |
| IT Security Team | Manage credentials and security policies. |
| HR Department | Verify employment status and approvals. |
| Department Head | Submit and justify access requests. |
| New User | Complete training and follow policies. |

**6. Compliance & Audit**

Ensure compliance with regulatory standards, review logs, and investigate anomalies.

**7. Document Review & Updates**

Review annually and update to align with security best practices.

# Flowchart

Notify Line Manager (IT Department)

Deposit Credential Details in Secure Location (IT Department)

Track Completion of All Fulfilments (IT Department)

Validate Fulfilment of Requests (IT Department)

Create Requests for Role-Based Application Access (IT Department)

Create Requests for Basic Services (IT Department)

Validation of Details (IT Department)

Approval Confirmation

(Authorized Manager)

Request Form Submission (Hiring Manager)