ASIAN INFRASTRUCTURE INVESTMENT BANK

DIRECTIVE ON DIGITAL IDENTITY AND ACCESS MANAGEMENT

Sponsor: The Director General, Information Technology Department

Issuer: The President

Document Type: Directive

Information Classification Designation: Public

Effective Date: January 28, 2026

Document Reference Number: ILF-2026-010

Summary of Content: Guiding principles, key requirements, and high-level accountability structure to ensure effective and transparent management of digital identity and access in the Bank.

Related Documents: Directive on Information Technology Security for Bank Personnel

DIRECTIVE ON DIGITAL IDENTITY AND ACCESS MANAGEMENT

1. OVERRIDING OBJECTIVE

1.1 This Directive establishes the rules and directions for Identity and Access Management (IAM) at the Asian Infrastructure Investment Bank (AIIB or the Bank), to guide the management of digital identities and the control of access to the Bank's Information Technology (IT) Systems to prevent unauthorized access, protect sensitive information, and maintain operational efficiency.

1.2 The implementation and interpretation of this Directive shall seek to give effect to this overriding objective.

2. APPLICATION

2.1 This Directive applies to all Bank Personnel and all IT Systems of the Bank that require Identification, Authentication, and/or Authorization.

3. GENERAL PRINCIPLES

3.1 The use of Identity, Accounts and Access Rights shall align with the Bank's business goals while ensuring appropriate safeguards are in place.

3.2 Bank Personnel shall adhere to the principle of **Least Privilege** when using their Identity, Accounts and Access Rights to fulfill their job responsibilities. The principle of Least Privilege entails that Identity, Accounts and Access Rights shall be created or granted only when it is necessary for Bank Personnel to perform their job responsibilities, with valid business justification, and only for the duration required to fulfill their job responsibilities. Bank Personnel shall proactively notify relevant parties of any changes to their job responsibilities, to allow for the timely adjustment or revocation of Identity, Accounts and Access Rights that are no longer required.

3.3 Bank Personnel shall adhere to the principle of **Segregation of Duties** when using their Identity, Accounts and Access Rights to fulfill their job responsibilities. The principle of Segregation of Duties entails that job responsibilities which might lead to operational risks or a conflict of interest if performed by the same Bank Personnel should be identified, and the corresponding Account and Access Rights required to perform these duties should not be assigned to the same individual. For example, no Bank Personnel shall have the Access Rights to initiate and approve payment at the same time. Where exceptions are necessary, they shall be clearly documented, appropriate mitigation controls shall be put in place, and such exceptions must have the necessary approvals and be subject to periodic reviews.

3.4 All necessary governance and technical controls will be implemented to facilitate the efficient and appropriate implementation of this Directive.

4. DEFINITIONS

4.1 **Access Rights**: The permission granted to an Identity to perform specific actions on IT Systems, such as accessing data or executing operations.

4.2 **Account**: A unique identifier with credentials (e.g., password, security keys, digital certificates) assigned to an Identity for accessing IT Systems.

4.3 **Artificial Intelligence (AI)**: As defined in the Directive on Responsible AI Governance Framework.

4.4 **Authentication**: The process of verifying whether an Identity attempting to access an IT System is who they claim to be, accompanied by relevant credentials.

4.5 **Authorization**: The process of determining whether an Identity is allowed to access certain data or execute a particular operation.

4.6 **Bank Personnel**: As defined in the Code of Conduct for Bank Personnel.

4.7 **Birthright**: Inherent Access Rights automatically granted to a User based on their organizational positions or job profiles, requiring no additional request or approval processes.

4.8 **Business Administrative or Critical Account**: A type of Account with elevated Access Rights to perform essential control or business functions within IT Systems, such as managing Accounts and Access Rights, configuring key operational settings, approving high-value transactions, or performing critical activities in key financial reporting processes.

4.9 **Business Unit**: As defined in the Directive on Business Continuity.

4.10 **External Party**: Any entity, and any individual that may be working for an entity, that is not Bank Personnel, including but not limited to the following:

4.10.1 **Supplier:** As defined in the Directive on Corporate Procurement, it means a business entity that supplies Goods, Works, General Services or Consulting Services.

4.10.2 **Business Partner**: An institution or organization that collaborates with AIIB to advance shared strategic, developmental, or institutional objectives.

4.10.3 **Client**: An entity and its authorized representatives with whom AIIB builds long-term relationships in its core sectors, for the purposes of financing, advisory services, or other forms of strategic collaboration. These include Sovereign-backed Financing (e.g., member governments) and Nonsovereign-backed Financing (e.g., fund managers, state-owned enterprises) Clients, as outlined in the Operational Policy on Financing.

4.10.4 Other external parties which may include any individual who is not Bank Personnel but is engaged by the Bank for a defined purpose and duration, such as external auditors, guest speakers and interviewees.

4.11 **Identification:** The process of asserting or claiming an Identity by providing a unique identifier, such as a username or staff ID, as the initial step in access control.

4.12 **Identity**: The set of attribute values (e.g., names, email address, or staff ID) by which a User is recognizable and is sufficient to distinguish them from any other entity.

4.13 **Identity Authoritative Source**: A designated system, repository, or entity that serves as the primary and trusted source of accurate, verified, and up-to-date Identity information.

4.14 **Individual Consultant**: As defined in the Directive on Corporate Procurement, it means an individual who provides professional or advisory services.

4.15 **IT System**: A coordinated set of resources and procedures assembled to be interdependent and interact with each other to accomplish a set of specific functions, such as collection, processing, maintenance, use, sharing, dissemination, or disposition of information. For the purpose of this Directive, IT Systems refer to internally developed and third-party IT Systems managed by the Bank to support its business objectives.

4.16 **Multi-Factor Authentication (MFA)**: A security method that uses two or more factors to achieve Authentication. These factors include: (a) something you know (e.g., a password or PIN); (b) something you have (e.g., a software or hardware token); or (c) something you are (e.g., a biometric).

4.17 **Personal Data**: As defined in the Policy on Personal Data Privacy.

4.18 **Privileged Account**: A special type of Account with elevated Access Rights, enabling the execution of critical tasks such as software installation, system configuration, or access to sensitive data. Privileged Accounts can be further categorized into the following:

4.18.1 **Technical Administrative Account**: Also known as a System Administrative Account, it is a type of Privileged Account that has elevated Access Rights to allow for broad control in an IT System. An Account shall be classified as a Technical Administrative Account if it has the Access Rights to perform installation and upgrades, manage and configure settings, access or modify data, or other administrative tasks within an IT System.

4.18.2 **Break-Glass Account**: Also known as Fire ID, or Emergency Access Account, it is a highly privileged type of Technical Administrative Account that is used to provide emergency or exceptional access to IT Systems when normal access paths are unavailable or insufficient. It is typically used during system outages, security incidents, or disaster recovery scenarios to ensure continuity of business operations.

4.18.3 **Business Support Account**: A type of Privileged Account that is used to handle non-technical inquiries and support the business, commercial, or operational activities of a particular IT System.

4.18.4 **Technical Support Account**: A type of Privileged Account that is used to provide technical assistance related to system functionality, performance, configuration, troubleshooting, incident response, or other support tasks within an IT System.

4.19 **Role**: A specific Authorization level and its corresponding collection of Access Rights within an IT System, usually associated with an organizational position or job profile.

4.20 **Role-Based Access Control (RBAC)**: A model that enforces access control by associating permissions with Roles rather than individual Users. Users are then assigned to Roles instead of being granted individual Access Rights directly. This approach supports the principle of Least Privilege by managing Access Rights collectively.

4.21 **Service Account**: A type of Account used by processes or devices (i.e., non-human entities) to authenticate and interact with other IT Systems to perform tasks such as running automated processes, accessing data programmatically, or executing scheduled tasks without human intervention. If a Service Account is granted elevated Access Rights, it shall also be qualified as a Privileged Account.

4.22 **Shared ID**: As defined in the Directive on Information Technology Security for Bank Personnel.

4.23 **User**: A User is a natural person, for example, Bank Personnel or an External Party, who requires access to the IT Systems.

5. IDENTITY MANAGEMENT

5.1 An Identity for Bank Personnel shall be constructed using only the relevant minimum Personal Data required for the IAM purposes, such as legal names, employee numbers, and job titles. Such IAM-related Personal Data shall only be sourced from their respective Identity Authoritative Sources.

5.2 A unique identifier shall be assigned to each Bank Personnel upon joining the Bank. This unique identifier shall be a distinct value across the Bank to identify Bank Personnel and shall not be reused. Bank Personnel who leave then later rejoin the Bank will be assigned a new and unique identifier.

6. ACCOUNT AND ACCESS RIGHT MANAGEMENT

6.1 Accounts shall always be correlated to an Identity. Accounts not correlated to an Identity shall be disabled or removed in a timely manner. Accounts created for Bank Personnel shall only be activated on the official date of their appointment and shall be promptly disabled or removed following the end of service.

6.2 Accounts with Birthright can be created for Bank Personnel without the need for additional request or approval. Birthrights assigned to Bank Personnel shall be removed promptly when there are changes to their organizational position or job profile. Birthrights shall be defined based on business requirements and must be approved in advance and reviewed regularly by the relevant Business Focal(s) and IT Service Owner.

6.3 Any additional Accounts and Access Rights shall be requested and granted only when there is a valid business need, supported by a clearly documented purpose and usage period. Such requests shall be limited to the minimum Accounts and Access Rights required to perform the User's job responsibilities and validated through the appropriate approval processes. Wherever feasible, Access Rights should be granted on a just-in-time basis and removed once they are no longer required.

6.4 Requests for a Business Administrative or Critical Accounts shall be approved in writing by the Head of Business Unit. Approval through delegation or self-approval by Business Focals shall not be allowed.

6.5 Approval authority may be delegated to Bank Personnel with appropriate knowledge and responsibility through a formal endorsement, with the scope and duration of the delegation clearly defined. The delegation must not circumvent the principles of Least Privilege or Segregation of Duties.

6.6 Proper control mechanisms shall be established to ensure that Accounts and Access Rights adhere to the principles of Least Privilege and Segregation of Duties.

7. AUTHENTICATION AND AUTHORIZATION MANAGEMENT

7.1 Proper Authentication measures shall be required to access IT Systems. "Anonymous" access may only be used for access to public information or data on AIIB's public-facing IT Systems which require no explicit Authorization, such as the AIIB official website.

7.2 Additional Authentication measures, including MFA, shall be required in the following scenarios: (a) accessing IT Systems remotely; (b) accessing IT Systems from non-AIIB devices; (c) accessing IT Systems using Business Administrative or Critical Accounts; (d) performing privileged operations; (e) performing financial transactions; (f) performing password resets and Account recovery; and (g) other scenarios deemed necessary by IT Service Owners.

7.3 Fine-grained Access Rights shall be precisely and specifically defined. Where feasible, Authorization mechanisms such as RBAC shall be implemented to ensure that only authorized Users can perform specific operations or access sensitive data.

7.4 All Authentication and Authorization events, including login attempts, MFA enforcement, and privilege elevation, shall be logged and retained to support auditability and incident response.

8. PRIVILEGED ACCOUNTS AND SERVICE ACCOUNTS MANAGEMENT

8.1 Privileged Accounts and Service Accounts shall be named to reflect the nature of the Account and to distinguish them from non-privileged User Accounts. All provisions specified concerning Section 7 on Authentication and Authorization Management shall be applicable to all Privileged Accounts and Service Accounts.

8.2 Each Privileged Account or Service Account must be owned by a Bank Personnel, who is responsible for the proper use and review of the Account.

8.3 Privileged Accounts can be assigned to dedicated system administrators or support personnel to perform administrative or support tasks. Such ownership and assignment shall be updated in a timely manner and securely (e.g., via credential rotation) upon changes in job responsibilities or end of service of Bank Personnel.

8.4 Privileged Accounts shall be strictly used for their intended administrative or support purposes, and shall not be used for non-privileged access.

8.5 Privileged Accounts shall be used via the Bank's Privileged Access Management System (PAM), where technically feasible, to ensure the application of enhanced Authentication controls, such as more stringent password requirements, and session recordings. Additional Authentication measures such as, but not limited to, IP address restrictions shall be implemented if there is a need for higher security requirements.

8.6 Break-Glass Accounts shall only be used in emergency or exceptional scenarios. Credentials of Break-Glass Accounts shall be securely stored and require approval or dual control to retrieve.

8.7 Service Accounts shall not be used by Bank Personnel to directly authenticate into IT Systems for any purpose. Service Accounts shall be strictly used for their intended automated or programmatic purposes.

8.8 Bank-provided AI tools, AI agents, agentic AI solutions, and any associated Accounts they use for connection, integration, data access and processing, etc., shall be provisioned as Service Accounts. Direct use of User Accounts by AI is prohibited. AI shall not be authorized to perform privileged operations autonomously; such actions require human initiation and oversight.

8.9 Service Accounts shall be subject to proper Authentication controls, such as but not limited to enhanced password policies, credential vaulting, and IP address restrictions.

9. ACCOUNTS AND ACCESS RIGHTS RECERTIFICATION

9.1 Periodic reviews of Accounts and Access Rights shall be conducted by designated Bank Personnel, at least annually, to identify and remediate dormant Accounts and inappropriate Access Rights.

9.2 Reviews of Accounts and Access Rights shall be conducted by designated Bank Personnel based on predefined scenarios, such as reassignment, to promptly adjust these Accounts and Access Rights accordingly.

9.3 Periodic reviews of ownership, assignment, and Access Rights for Privileged Accounts shall be conducted by designated Bank Personnel, at least annually, to identify and mitigate unauthorized access.

9.4 Results of recertification, including any remediation actions, shall be documented and retained to support audit and compliance requirements.

10. RULES FOR EXTERNAL PARTIES

10.1 External Parties who need to access the IT Systems shall be required to comply with this Directive and relevant Instructions or Guidelines. Such requirement shall be incorporated by reference into the respective agreements, contracts, or terms and conditions governing their relationship with the Bank, as specified below:

10.1.1 For Suppliers, compliance shall be enforced through their respective contracts with the Bank. The Assignment Manager shall be responsible for ensuring compliance with this Directive.

10.1.2 For Business Partners and Clients, compliance shall be enforced through the agreements or contracts governing their relationship with the Bank. The Bank Personnel managing the agreements or contracts shall be responsible for ensuring compliance with this Directive.

10.1.3 For others, compliance shall be enforced through engagement protocols and/or terms and conditions governing their interactions with the Bank. The Bank Personnel sponsoring the engagement shall be responsible for ensuring compliance with this Directive.

10.2 External Parties shall not enable or facilitate unauthorized access to the IT Systems, by any entity or body, including commercial, political, or state organizations of any country.

10.3 Identity information, Authentication and Authorization processes for External Parties using the IT Systems shall, where feasible, be logically and technically segregated from those of Bank Personnel, to enhance security and limit the impact of potential compromises.

11. ROLES AND RESPONSIBILITIES

11.1 **Bank Personnel** are the Users of their Identity, Accounts and Access Rights, which enable them to perform their job responsibilities securely and efficiently. Bank Personnel are responsible for:

11.1.1 maintaining the accuracy of their IAM-related Personal Data.

11.1.2 requesting only Accounts and Access Rights that are (a) necessary to perform their job responsibilities; and (b) not in conflict with their job responsibilities.

11.1.3 using assigned Accounts provided by the Bank to access the IT Systems. Thus, Bank Personnel should (a) not use Accounts of other Bank Personnel; (b) not share their Accounts with anyone else; and (c) not use any Shared ID.

11.1.4 creating strong credentials compliant with the requirements of the Bank as outlined in relevant Directives, Instructions and/or Guidelines, and safeguarding them by ensuring passwords and other credentials are never written down, printed out, displayed in plain text, or shared with anyone else.

11.1.5 reporting to the Information Technology Department (ITD), without unnecessary delay, any observed or suspected IAM risks and issues, and proactively providing reasonable assistance in incident-handling activities.

11.1.6 completing IAM trainings as required by the Bank.

11.2 **Line Managers** or **Assignment Managers** are Bank Personnel who supervise and oversee the work of their reporting Bank Personnel or Suppliers during the assignment or contract. Within the context of IAM, Line Managers, Assignment Managers, and Bank Personnel who manage agreements, contracts or sponsor engagements with External Parties are responsible for:

11.2.1 maintaining the accuracy of IAM-related Personal Data for Bank Personnel reporting to them, including updates due to reassignment or end of service, as required by Staff Rules and supplementary Instructions and Guidelines.

11.2.2 maintaining the accuracy of IAM-related Personal Data for External Parties, including changes in personnel, through their incorporation by reference into their respective agreements/contracts.

11.2.3 reviewing and completing assigned tasks in IAM processes, such as: (a) approval of Accounts and Access Rights requests; and (b) periodic and scenario-based recertification of Accounts and Access Rights.

11.3 **Heads of Business Units** oversee the proper use of Identity, Accounts and Access Rights of Bank Personnel within their Business Units. Heads of Business Units are also the primary stakeholders for IT Systems developed to support their business needs, and owners of non-privileged User Accounts, Business Administrative or Critical Accounts, and Access Rights in these IT Systems. Within the context of IAM, Heads of Business Units are responsible for:

11.3.1 overseeing compliance with this Directive and adherence to IAM processes within their Business Units.

11.3.2 appointing Business Focals for IT Systems developed to support their business needs.

11.3.3 making informed decisions on IAM matters, and prioritizing IAM requirements based on business needs and operational impact.

11.3.4 reviewing and completing assigned tasks in IAM processes, such as: (a) approval of Business Administrative or Critical Accounts requests; and (b) recertifications of Business Administrative or Critical Accounts.

11.4 **Business Focals** are designated representatives and/or subject matter experts for the business areas of their Business Units, for which IT Systems are developed to support specific business needs. Business Focals understand the business requirements and work closely with IT Service Owners and the IAM Team to ensure proper design and implementation of IAM within IT Systems. Within the context of IAM, Business Focals are responsible for:

11.4.1 collaborating with relevant stakeholders to determine IAM requirements, such as classification of Business Administrative or Critical Accounts, Authentication and Authorization, in IT Systems.

11.4.2 reviewing and monitoring the design and implementation of IAM requirements in IT Systems.

11.4.3 reviewing and completing assigned tasks in IAM processes, such as: (a) approval of Accounts and Access Rights requests; and (b) periodic recertification of Accounts and Access Rights, including Business Support Accounts.

11.5 **IT Service Owners** are Bank Personnel who are responsible for managing an IT System throughout its lifecycle, ensuring delivery meets defined requirements and agreed levels, and driving continuous improvement. Within the context of IAM, IT Service Owners are responsible for:

11.5.1 incorporating IAM requirements into the design and implementation of IT Systems.

11.5.2 reviewing and completing assigned tasks in IAM processes, such as: (a) approval of Accounts and Access Rights requests; (b) periodic recertification of Accounts and Access Rights; and (c) periodic recertification of ownership, assignment, and Access Rights for Privileged Accounts.

11.5.3 overseeing the provision, assignment and revocation of Accounts and Access Rights in IT Systems, through automated processes or by designated Bank Personnel or External Parties.

11.5.4 monitoring and reviewing the provision, assignment, usage and revocation of Privileged Accounts and Service Accounts in IT Systems.

11.6 The **IAM Team** of ITD is responsible for:

11.6.1 monitoring the lifecycle of the Identities, and facilitating the processes for onboarding, reassignment, and offboarding.

11.6.2 monitoring the lifecycle of the Accounts, and facilitating the processes for creating, updating, reviewing, and disabling Accounts when appropriate.

11.6.3 implementing a centralized repository of Identity, Accounts and Access Rights information, and necessary technical controls to facilitate the efficient and appropriate implementation of this Directive.

11.6.4 defining and reporting IAM-related compliance matrices to senior management.

11.6.5 coordinating IAM-related issue handling activities and providing practical technical solutions.

11.6.6 developing and conducting IAM continuous education and training programs.

11.7 The **Human Resources Department (HRD)** is the owner of Identity Authoritative Sources for Staff, Secondees, Interns, as well as Outsourced Staff whose scheduled working location is Bank Headquarters. HRD is responsible for:

11.7.1 maintaining the accuracy of IAM-related Personal Data of Staff, Secondees, Interns, Outsourced Staff whose scheduled working location is Bank Headquarters, and all other employment categories of Bank Personnel managed by HRD, including updates due to reassignment or end of service, as required by the Staff Rules and supplementary Instructions and Guidelines.

11.7.2 propagating relevant changes of IAM-related Personal Data to the IAM Team and/or other relevant teams in ITD in a timely manner for execution of IAM related processes.

11.8 **Hub Offices** are the owners of Identity Authoritative Sources for Outsourced Staff whose scheduled working location is the respective Hub Offices. Hub Offices are responsible for:

11.8.1 maintaining the accuracy of IAM-related Personal Data of Outsourced Staff whose scheduled working location is the respective Hub Offices, including updates due to reassignment or end of service, as required by the Staff Rules, and supplementary Instructions and Guidelines.

11.8.2 propagating relevant changes of IAM-related Personal Data to the IAM Team and/or other relevant teams in ITD in a timely manner for execution of IAM related processes.

11.9 The **Corporate Procurement Division (CPD)** of the **Facilities and Administration Services Department (FAS)** is the owner of Identity Authoritative Sources for Individual Consultants. CPD is responsible for:

11.9.1 maintaining the accuracy of IAM-related Personal Data of Individual Consultants, including updates due to reassignment or end of service.

11.9.2 propagating relevant changes of IAM-related Personal Data to the IAM Team and/or other relevant teams in ITD in a timely manner for execution of IAM related processes.

11.10 The **Corporate Secretariat (SEC)** is the owner of Identity Authoritative Sources for Board Officials, including members of the Board of Governors, the Board of Directors, External Members of the Audit and Risk Committee, as well as the members of the International Advisory Panel (IAP). SEC is responsible for:

11.10.1 ensuring that access for Board Officials and IAP members is managed in accordance with the Bank's governance protocols, including provisions related to the commencement and cessation of service, delegation arrangements, and confidentiality obligations.

11.10.2 facilitating access to IT Systems by Board Officials and IAP members, in accordance with the principles of Least Privilege and Segregation of Duties, and in coordination with IT Service Owners and the IAM Team.

11.10.3 maintaining the accuracy of IAM-related Personal Data of Board Officials and IAP members, including updates due to procedures as outlined in the Bank's Articles of Agreement.

11.10.4 coordinating with the IAM Team and/or other relevant teams in ITD to propagate relevant changes of IAM-related Personal Data and oversee corresponding adjustments to Access Rights for Board Officials and IAP members in a timely manner.

11.11 The **Sanctions Panel Secretariat** is the owner of Identity Authoritative Sources for the Chair and External Members of the Sanctions Panel. The Sanctions Panel Secretariat is responsible for:

11.11.1 ensuring that access for the Chair and External Members of the Sanctions Panel is managed in accordance with the Bank's governance protocols, including provisions related to the commencement and cessation of service, delegation arrangements, and confidentiality obligations.

11.11.2 facilitating access to IT Systems by the Chair and External Members of the Sanctions Panel, in accordance with the principles of Least Privilege and Segregation of Duties, and in coordination with IT Service Owners and the IAM Team.

11.11.3 maintaining the accuracy of IAM-related Personal Data of the Chair and External Members of the Sanctions Panel, including updates due to procedures as outlined in the Bank's Policy on Prohibited Practices.

11.11.4 coordinating with the IAM Team and/or other relevant teams in ITD to propagate relevant changes of IAM-related Personal Data and oversee corresponding adjustments to Access Rights for the Chair and External Members of the Sanctions Panel in a timely manner.

11.12 The **Vice President and Chief Administration Officer (VPCAO)**, with technical advice and support from and facilitated by the Director General, ITD, has the authority to require ITD to impose restrictions or temporarily remove access for Bank Personnel and External Parties, including any related Privileged Accounts and Service Accounts, under the following circumstances:

11.12.1 as part of administrative decisions, or

11.12.2 to give effect to a determination by or recommendation of the Chief Ethics Officer to do so made pursuant to the Internal Legal Framework applicable to the mandate of the Ethics Office (ETH) (including as it relates to fact-finding or investigation procedures and to protection against retaliation), or

11.12.3 as part of critical or high IT and cyber incident management activities.

12. IMPLEMENTATION

The VPCAO shall introduce, if necessary, any related Instruction or Guideline to ensure the effective implementation of this Directive. The Director General, ITD, shall provide necessary support for the application and implementation of this Directive.

13. APPLICATION AND WAIVER

The VPCAO shall make all final decisions regarding the application of this Directive, including whether to grant a waiver thereof, in accordance with Section 4.8 of the Directive on the Internal Legal Framework.

ANNEX 1: ACCOUNT OWNERSHIP

Type of Account	Owner of Account	User(s) of Account
Business Administrative or Critical Account	Head of Business Unit	Designated user from Business Unit
Business Support Account	Head of Business Unit	Designated support personnel
Technical Administrative Account	IT Service Owner	Designated system administrator
Technical Support Account	IT Service Owner	Designated support personnel
Service Account	IT Service Owner	Used by processes or devices (i.e., non-human entities)