Policy Title	Policy and Procedures for Information Security Identity Access Management
Document Identifier	PPM/IDAM/2024
Previous title (if any)	N/A
Policy objective	Identity and Access Management (IDAM) is critical for authenticating users and ensuring that user access to information and ICT systems is commensurate with their role and business requirements. This policy is written to provide principles for issuing and managing user accounts to access software and other ICT systems.
Target audience	This policy applies to: ● all UNFPA personnel responsible for managing UNFPA information systems and applications. ● all UNFPA locations (in the cloud and on premise).
Risk control matrix	Control activities that are part of the process are detailed in the Risk Control Matrix within section VI of this policy.
Checklist	N/A
Effective date	4 October 2024
Revision History	N/A
Mandatory review date	4 April 2026
Policy owner unit	Information Technology Solutions Office (ITSO)
Approval	Link to signed approval template

INFORMATION SECURITY IDENTITY AND ACCESS MANAGEMENT POLICY

TABLE OF CONTENTS

I. Purpose

The purpose of this policy is to establish guiding principles for authenticating users and provisioning, maintaining, revalidating and revoking access to UNFPA data and information systems. UNFPA information systems includes user workstations, servers, network devices, cloud services (such as cloud drives and e-mail) and applications (including the Enterprise Resource Planning (ERP) system, and other custom developed applications).

Properly controlling and protecting access to UNFPA data and information systems greatly reduces the risk of unauthorized access, incidents and data leakage or loss.

This policy must be read in conjunction with the UNFPA Information Security Policy that describes:

- general UNFPA principles related to the protection of data confidentiality, integrity and availability.
- roles and responsibilities of all personnel in security of the data they have been granted access to.

II. Policy

A. General access control requirements

1. System owners must ensure all UNFPA information systems have access controls in place (as per the procedures section below) to ensure that information is not improperly disclosed, modified, or deleted.

2. System owners must ensure access controls are used to limit access to applications, data and functions based on the least privilege and ‘need to know’ principles to perform official duties.

B. Shared, generic and non-user accounts

3. Where technically feasible, administrators of information systems shall disable access to all default or generic user accounts. Where not technically feasible to disable, the default accounts:

   a. should be renamed and
   b. must have their passwords changed at installation.

4. Administrators of information systems shall prohibit the use of shared accounts to ensure accountability.

C. User provisioning and deprovisioning[1] for accounts in UNFPA's corporate directory

Provisioning

5. ITSO is responsible for provisioning and deprovisioning all UNFPA accounts for any individual who:

   a. has a UNFPA staff contract or a contract for service with UNFPA (i.e., non-staff personnel, including consultants, interns, volunteers, etc.) which has a duration greater than 30 days; or

   b. works in an official capacity for an entity that has been contracted by UNFPA to perform service for UNFPA (for example employees of vendors, personnel of other UN agencies engaged to perform services for UNFPA, etc.):
   or

   c. is a UN Board of Auditor (BoA), whenever required.

6. Either DHR or the hiring manager of the individual must request ITSO or the directory focal point to formally request the provisioning of an account by registering the user in UNFPA's corporate directory.

7. ITSO, or the relevant directory focal point, should only register users in the corporate directory after a letter of appointment or contract with UNFPA has been signed.

8. Please note, only for staff, directory focal points can register a user up to a week before the user's start date to facilitate on-boarding.

9. It is the responsibility of ITSO or the directory focal point to verify the users identity before receiving credentials and ensure the registration process captures the following:

   a. A unique electronic identifier to facilitate accountability and traceability of user access.
   b. The user's first and last name.
   c. A contractual classifier to identify whether the individual is staff or non-staff.
   d. The user's officially registered working location and department (as per contract).
   e. The user's contact details (e.g., external e-mail address and telephone number).
   f. Manager.
   g. Start date.
   h. End date.

[1] Provisioning is the process of creating and configuring user accounts or access rights in a system or network, while deprovisioning is the process of revoking or removing access rights and privileges from a user account within a system or network.

10. Once the user is registered in the corporate directory, ITSO provisions the account by activating the account and assigning privileges to it, based on its profile in the corporate directory.

11. Whenever possible, administrators of information systems should grant access to data and information systems via user groups (or roles), and not grant directly to individual accounts.

12. Where technically feasible, regular user accounts must not be used when configuring system-level resources (e.g., clusters, connections to back-end, etc.) and instead privileged or service accounts must be used.

Deprovisioning

13. ITSO -or the directory focal point when applicable- may suspend any user account(s) that are inactive for more than 30 days based on its risk assessment. In these instances, the account is not deprovisioned; it will need to be re-activated by ITSO or the directory focal point before it can be used again.

14. ITSO or the directory focal person should deprovision user accounts by removing it from UNFPA's corporate directory on the day of the user's contract end date or on the day of separation from UNFPA (if earlier than the contract end date).

15. UNFPA directory focal points may, subject to approval by the head of unit, request an extension for a user to retain a non-privileged account for up to 30 days after the contract end date.

16. ITSO archives all user email accounts when the account is deprovisioned in UNFPA's corporate directory:
    a. ITSO shall maintain the archive for a minimum period of six months.
    b. ITSO will make the archives accessible upon written request for audit and investigation purposes only.

D. User authentication

17. User authentication should be enabled with multi-factor authentication (MFA). Multi-factor authentication entails two or more of the following:
    a. Something the user has: any physical object in the possession of the user, such as a security token (USB stick), a bank card, a key, etc.
    b. Something the user knows: certain knowledge only known to the user, such as a password, PIN, etc.

c. Something the user is: some physical characteristic of the user (biometrics), such as a fingerprint, eye iris, voice, typing speed, pattern in key press intervals, etc.

18. Any system that provides the ability for a user to log-on (including administrative access to servers and network equipment) using a password, change or reset a password shall be configured by the administrator of information systems to:

a. Enforce the use of individual credentials to maintain accountability.
b. Enforce a choice of quality passwords in accordance with password complexity requirements (detailed below).
c. Enforce password change every ninety (90) days. If the user account has multi-factor authentication enabled, it is not mandatory to enforce password expiration.
d. Require an old password in order to change it.
e. Force users to change temporary passwords at the first log-on.
f. Not display passwords on the screen when being entered.
g. Encrypt and store password files separately from application system data.
h. Store and transmit passwords in protected (encrypted or hashed) form.
i. Provide measures to detect repeated login failures and lock accounts in response.

19. Administrators of information systems should enforce strong passwords for authentication systems. Examples of strong password criteria could include:

a. Contain ten (10) characters or more.
b. Contain characters from three of the following four-character classes:
   i. English uppercase characters (i.e. a-z).
   ii. English lowercase characters (i.e. A-Z).
   iii. Base 10 digits (i.e. 0-9).
   iv. Punctuation and other characters (i.e. !@#$%^&*()_+|~-=\`{}[]:";'<>?,./).

E. Privileged access

20. UNFPA users who are directly responsible for system management, administration, and/or security are considered to have privileged access.

21. Administrators of all UNFPA information systems must restrict privileged access to the minimum number of individuals required to effectively manage the system, to be responsible for administration of the system and to monitor security. In addition, they should only grant the minimum level of privilege required to perform the official duties.

22. The manager must submit a written request to the administrator of the respective system in order to grant privileged access for UNFPA personnel who require such access to perform their official duties.

23. Upon receipt of a request, ITSO or the relevant field office information technology officer must provide them with a different account with the appropriate level of privilege to be used solely for the purpose in which it was assigned. This privileged account must not be used for tasks that can be achieved with a standard user account (e.g., email access, intranet access, VPN access, etc.).

24. Owners of information systems must ensure privileged accounts:

    a. are recorded in an inventory.
    b. are secured with Multi Factor Authentication (MFA).
    c. undergo a user review process at intervals not exceeding 12 months. (Revalidation of user access permissions must be documented).
    d. be reassessed or revoked upon changes to job duties.
    e. usages are tamper-proof logged.

25. Managers must review privileged accounts provisioned to their personnel prior to their staff going on extended leave, loan or secondment for greater than 30 days.

F. User access logging and account reviews

26. Administrators of critical information systems must ensure all access attempts are logged, including their own and the ones related to privileged users, and relevant security events monitored

27. Administrators of information systems must enable controls to ensure system users cannot modify critical production data without an audit trail and will generate a detailed log that will record and track all changes.

28. System owners must review the list of active user accounts on a regular basis to confirm the validity of accounts.

G. Monitoring and inspections

29. UNFPA has a strong commitment to information security. In line with the overall Information Security Policy, any violation of the provisions of this policy, shall be reported to the Information Security Team and any allegations of wrongdoing should be reported to OAIS.

30. Routine technical monitoring is conducted by ITSO as per the provisions of this policy or a field office focal point designated by ITSO.

31. Non-routine monitoring ("inspection") may be initiated by ITSO if, at any time, there is reason to believe that there is a risk that will significantly interfere with or impact the operations of UNFPA.

32. An annual report on the monitoring activities performed and any findings is sent to the Information and Communication Technology (ICT) Board.

III. Procedures

A. General access control and user provisioning

33. Access controls shall be implemented by administrators of information systems through enabling at least one or more of the below controls:

    a. Single sign on (SSO) with UNFPA's corporate identity management solution, where feasible, to enhance user experience and reduce the number of user credentials UNFPA personnel are required to maintain.
    b. Multi-Factor Authentication (MFA)[2] where systems or devices support it.
    c. *Passwordless* authentication where feasible.

34. System owners shall maintain a record (with complete audit trail) of all users who have been approved to access restricted information through one or more of the following records:

    a. approvals via email,
    b. approvals via service desk request

35. Administrators of information systems shall maintain a record of the date when access is provisioned for approved users through annotating a note to the respective record documenting approval of user access.

36. Administrators of information systems shall restrict use of shared accounts through limiting issuance of passwords to single users.

B. User account management

37. System owners shall review user accounts through the following activities:

    a. extract a list of user accounts from the system.
    b. cross reference each user with UNFPA human resource records and other contract records to validate the user is currently engaged by UNFPA (through a staffing or other contract).
    c. the business need for retaining each privileged user account must be individually validated by the system owner.
    d. the "last activity" date for privileged users is to be reviewed by the administrator of the information system. Where a privileged account has been inactive for more than 30 days, the owner of the inactive account will be notified before the account is disabled.

[2] Where single sign on cannot be feasibly implemented for an ICT system, alternate authentication controls equivalent in strength to UNFPA's corporate identity management solution shall be implemented.

C. Logging and monitoring

38. Information system administrators must configure the system to retain logs of all access attempts and other user activities, through either:

    a. integrating system logs with the UNFPA Security Information and Event Monitoring (SIEM) platform.
    b. configuring local retention of system logs and establishing a monitoring procedure.

D. Exceptions

39. Exceptions to this policy shall be managed as such:

    a. Any deviation from information security policies shall be documented and submitted for review by the information security officer via the e-mail infosec@unfpa.org.
    b. Approval of exceptions will be undertaken by the Director ITSO, in consultation with the Director of the requesting entity, and:
        - will be time bound based
        - ITSO director will be in charge of assessing the risk level for the requested exception and in case it exceeds the risk appetite in the UNFPA Risk Appetite Statement, the general escalation process will be activated as per the Enterprise Risk Management policy
        - documentation of approval will be retained in the central document repository.

IV. Other

A. Definitions

Term	Definition
System owner	The stakeholder who may experience business-related losses in the event of an operational or malicious incident affecting a specific application. This is usually a business stakeholder whose business need has a fulfillment dependency on the system
Third-party partner	External organization that collaborates with UNFPA through a contractual agreement to provide digital services.
Administrator of information systems	An administrator of information systems is a user appointed by the system owner to administer and support the system. This is usually a

	technical member of the ITSO team but may also be a staff member of ITSO or a third-party partner that was appointed by ITSO.
Passwordless authentication	Passwordless authentication is an authentication method that allows a user to gain access to an application or information technology system without entering a password or answering security questions.
Information security officer	Information Security Officers are professionals in charge of protecting UNFPA information systems from security threats.
Access restricted information	Information protected - to prevent unauthorized use, disclosure, modification, or destruction - by security measures, only accessible to authorized users or systems
UNFPA's corporate identity management solution	UNFPA corporate identity management solution is the solution that manages digital identities and ensures secure and authorized access to corporate resources.
Manager	Manager of the resource as indicated in the UNFPA Organizational Chart

B. Related documents

40. The following related documents should be referenced for additional context.

#	Document	Location
1	UNFPA Information Security Policy	UNFPA website
2	UNFPA Oversight Policy	UNFPA website
3	Disciplinary Framework	UNFPA website
4	UNFPA Internal Control Framework (ICF)	UNFPA website
5	Enterprise Risk Management	UNFPA website

V. Process Overview Flowchart(s)

No overview flow chart applicable.

VI. Risk Control Matrix

Risk Description	First Line of Defense Controls			Second Line of Defense Controls		
	Control Activity Description	Reference (Policy section, paragraph or Control #)	Who performs	Control Activity Description	Reference (Policy section, paragraph or Control #)	Who performs
Lack of enforcement of this policy within UNFPA's department and offices leads to inappropriate access to UNFPA information systems	System owners must ensure all UNFPA information systems have access controls in place	Section II, A	ITSO	Monitoring compliance to this policy	Section II, G	Information and Communicati on Technology (ICT) Board
UNFPA personnel have access to ICT resources not related to their job duties	Access to ICT resources is provided on the basis of documentation attesting to access needs (need to know and least privilege principles)	Section II, C	ITSO	Monitoring compliance to this policy	Section II, G	Information and Communicati on Technology (ICT) Board

Risk Description	First Line of Defense Controls			Second Line of Defense Controls		
	Control Activity Description	Reference (Policy section, paragraph or Control #)	Who performs	Control Activity Description	Reference (Policy section, paragraph or Control #)	Who performs
Users continue to have access to ICT resources after leaving UNFPA	When personnel leave UNFPA, deprovisioning is done and a periodical access review is performed	Section II, C and F	ITSO	Monitoring compliance to this policy	Section II, G	Information and Communication Technology (ICT) Board
Login attempts from an unauthorized source	Login attempts are logged and monitored	Section II, F and Section III, C	ITSO	Monitoring compliance to this policy	Section II, G	Information and Communication Technology (ICT) Board