

PRIVILEGED USER ACCOUNT ACCESS POLICY

Version number	Review date	Reviewed by	Approval date	Approved by	Summary of Changes	Next review date
1.0	Jul 2012	G. Price	Jul 2012	J. Ilag	Baseline	
2.0	Dec 2015	G. Price	Jan 2016	J. Ilag	Emphasized difference between standard users and privileged users in policy objective	Jul 2017

A. Policy objective:

1. The purpose of this policy is to ensure that no unauthorized user can access UNFPA servers with privileged accounts. A privileged user is a user who has been allocated powers within the computer system which are significantly greater than those available to the standard user. A privileged user account may have access to confidential data and includes system and database administrators and supervisors. This policy is also intended to ensure that users log on to UNFPA servers with their privileged username and password before escalating their access rights. This creates an auditable trail of privilege escalation after logon.

B. Intended audience:

2. This policy covers all UNFPA MIS staff, consultants and contractors who have knowledge of a root-user, super-user, or administrator password on any UNFPA servers.

C. Policy statement:**a. Staff Responsibilities and Accountability:**

3. Only MIS Branch staff, consultants and contractors who have traditionally performed systems administration duties, and are responsible for maintaining software applications or systems can have privileged access on some or all of the UNFPA servers upon request.
4. Privileged access shall be granted to individuals only after they have read this policy, obtained the approval of their supervisor, and signed a **Privileged Access Agreement Form**
5. Whenever technically possible, gaining and using privilege access should be audited.
6. If methods other than privileged access will accomplish an action, those methods must be used unless the burden of time or resources required clearly justifies using privileged access.
7. Privileged access may be used only to perform official job functions, which may include standard systems, database and other server administration related duties.

8. Individuals with privileged access shall take necessary precautions to protect the confidentiality of information encountered in the performance of their duties. If, during the performance of their duties, individuals with privileged access are inadvertently exposed to information that might indicate inappropriate use, they must consult their supervisor.
9. Preconditions to obtain the privileged account access for the servers are listed as following. Exceptions to any of these conditions can only be permitted after obtaining prior authorization from the MIS Chief in the form of an email or memorandum.
 - A user must not directly access any UNFPA server with a Super User ID and Password unless deemed absolutely necessary by the supervising officer. Direct Super Access can only be obtained through the dedicated console.
 - A user must not elevate their regular privileges to a higher level unless absolutely necessary. Every attempt to elevate privileges will be logged and reported to the MIS Chief on a periodic basis.
 - A user must never share their credentials with any other person.
 - All the information a user has access to on UNFPA servers must be considered proprietary to UNFPA and must be fully protected at all times.
 - Tampering of any data on any of the UNFPA servers is strictly forbidden and will result in disciplinary actions.
 - A user must not read or copy any information that is stored on the server.
 - A user must not grant/revoke access to any other user.
 - A user must not change any privileged account credentials.
 - A user must not install any software or patch on the server. Any installation must be fully endorsed and must follow the Change Control procedure.
 - A user must not run any command or application that may inadvertently affect the server performance.
 - A server must not be shut down or rebooted by a user unless deemed absolutely necessary.
 - Unless deemed necessary the server configuration must not be tampered by a member. Any changes to the server must be logged in the Configuration Management Database.
 - The user must understand the importance and criticality of each of the servers under their domain and must ensure that the system executes the operational capability under acceptable standards.

D. Policy date:

10. The Privileged User Account Access Policy (originally approved and issued on 18 July 2012 with subsequent revisions as shown in the beginning of this document) will remain in force without time limit, and will be reviewed annually to ensure relevance.

E. Policy owner:

11. The Technology Services Section Chief is responsible for the Privileged User Account Access Policy.

F. Change authority:

12. The MIS Chief, Technology Services Section Chief and Business Services Section Chief have the authority to change the privileged user account access policy. The MIS Chief, Technology Services Section Chief, Business Services Section Chief, and the Director of DHR can give exception waivers.



Privileged Access Agreement Form

1. I have read this Privileged User Account Access Policy.
2. I agree to comply with the provisions of this Privileged User Account Access Policy.
3. I understand that, after agreeing to comply with the provisions of this Privileged User Account Access Policy, failure to follow the provisions may result in administrative penalties up to and including termination of employment.
4. I also agree to provide full cooperation during any investigation concerning security matters which may have occurred in any of the UNFPA Servers.

Print Name: _____

Signature: _____ Date: _____

Authorized by:

Print Name: _____

Signature: _____ Date: _____