PRIVILEGED USER ACCOUNT ACCESS POLICY

A. Policy objective:

The purpose of this policy is to ensure that no unauthorized user can access any of the SFO servers or Information Repositories 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 majority of users. 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 SFO Systems with their username and password before escalating their privileges. This creates an auditable trail of privilege escalation after logon.

B. Intended audience:

This policy covers all SFO staff, consultants and contractors who have knowledge of a root-user, super-user, or administrator password on any systems such as Laptops, Desktops, Workstations, servers, Handhelds, etc.. hereafter referred as SFO System.

C. Policy statement:

a. Staff Responsibilities and Accountability:

1. Only SFO IT staff 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 SFO System / Information repositories upon request.

2. 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

3. Whenever technically possible, gaining and using privilege access should be audited.

4. 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.

5. Privileged access may be used only to perform official job functions, which may include standard systems, database and other server administration related duties.

6. 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.

7. 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 Chief Information Officer in the form of an email or memorandum.

    - A user must not directly access any SFO System with an Admin ID / 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 Chief Information Officer on a periodic basis.
    - A user must never share their credentials with any other person.

- All the information a user has access to on any of the SFO System must be considered proprietary to SFO and must be fully protected at all times.
- Tampering of any data on any of the SFO System 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:

The Privileged User Account Access Policy was issued on 10 December 2020, will remain in force without time limit, and will be reviewed annually to ensure relevance.

E. Policy owner:

The Manager IT Security is responsible for the Privileged User Account Access Policy.

F. Change authority:

The Chief Information Officer and Chief information Security Officer have the authority to change the privileged user account access policy. The Chief Information Officer can give exception waivers.

G. Violations:

Any violation of this policy may result in disciplinary action, up to and including termination of employment. SFO Technology reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

H. Revision History

Version	Description	Revision Date	Review Date	Reviewer/Approver Name
1	Initial Version	10/12/2020	10/12/2020	Prince Joseph
2	Added version history, added clause G, Updated clause B, E and F.	10/08/2022	10/08/2022	Prince Joseph

SFO - 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 SFO System.

Print Name: ______________________________________

Signature: ______________________________________ Date: ____________

Authorized by:

Print Name: ______________________________________

Signature: ______________________________________ Date: ____________