The Cherpalcheri
Co-Operative Urban Bank

PRIVILEGED USER ACCESS POLICY

Sl. No.	Particulars	Date	Remarks
1.	Policy approved date	13-03-2025	Res. No. 21
2.	Last reviewed date		
3.	Next review date	13-03-2026	
4.	Calendar of review	12 Months	

THE CHERPALCHERI CO-OPERATIVE URBAN BANK LTD., NO. 1696

1. Introduction

Privileged User IDs, by definition, allow their users to perform actions over and above the standard actions available to a normal user account. As such, it is vital that these User IDs are maintained, reviewed and removed in a timely fashion. This maintenance prevents them from being left active inappropriately, with the consequent risk of misuse by a user who no longer requires access (or has left), or increased risk of compromise by an external attacker.

This document describes how a bank shall manage privileged User IDs on systems for which it is responsible.

2. Scope

This policy applies to:

- Users on CBS, network equipment and other electronic devices managed by Information Technology Department (hereinafter referred to as it's abbreviated form ITD)
- All privileged Users, including operating system, hypervisor, application, and network device.
- Any server that ITD manages[1] or is responsible for, including physical storage severs, data centers or cloud servers which are managed by third parties on behalf of ITD.
- Any software on these servers. In this document, "software" shall be taken to include firmware, BIOS, hypervisor, operating system, driver, library, middleware, application, service, and other digital capabilities.

3. Dependencies

Documents which rely upon this policy:

- Vulnerability Management Guidance for ITD servers.

Documents which this policy relies on:

- Information Security Policy
- Cyber Security Policy

4. Stakeholders

The following roles, or their nominated representatives, should be involved in the review of this document.

- Head of Information Security
- Head(s) of Server Management team(s)
- Service Owner(s) for Server Service(s)
- Chair of Security Working Group

5. Accountable Roles

Department Heads shall ensure that servers and/or software which are managed by their staff are compliant with this policy.

Service Operational Managers shall ensure that systems which support their service are compliant with this policy, but may delegate operational activities to members of their Service Virtual Teams.

Service Operational Managers will ensure that the responsibilities of System Custodians as defined within this policy, the Information Security Policy, secondary policies and guidelines will be met.

Service Owners are ultimately accountable for the security of their service.

6. Definitions

Privileged Users: accounts which permit super-user access, or access allowing actions greater than those granted to standard user IDs. These user IDs may be tied to a user, or to an application.

Privileged account custodian (PAC): the individual who is responsible for the usage of a specific privileged account.

7. Policy statements

7.1. Authorisation

1) Only authorised PACs (privileged account custodians) shall be permitted to hold privileged users.

2) Authorisations shall be specific to a given privileged account[2].

3) Each PAC shall be authorised (or de-authorised) by their line manager and the system custodian.

4) The Service Owner is responsible for specifying any additional rules relating to the authorisations process for systems supporting their service (e.g. background checks for certain services).

5) Privileged User IDs must not be shared[3]

6) Authorisations should be based on a valid business requirement and time limited.

7.2. Usage

1. Privileged User IDs shall be used by their assigned PAC only.
2. Passwords for privileged User IDs shall not be shared; only the PAC shall know the password.
3. Line managers are responsible for ensuring that User IDs are used in compliance with bank policies.
4. Passwords for privileged User IDs shall be of a strength suitable for their intended purpose, based on the Service Risk Assessment.

7.3. Retention

1) Privileged User IDs which are no longer required shall be disabled immediately, and deleted within three months.
2) <Check what the Password and Account policies say about password changes on service User IDs and sysadmin User IDs> Passwords for privileged User IDs shall be changed no less often than once per 150 days.
3) Service Owners are responsible for approving password lifespans for systems supporting their service, based on their Service Risk Assessment.

7.4. Documentation

1) The system custodian shall manage and maintain records of authorised PACs, which shall indicate their name, role, and justification for privileged access, system(s) to which they have privileged access, date of authorisation and details of the authorising role.
2) The system custodian shall manage and maintain a record of reviews of access rights.
3) Records shall be stored in a location agreed between the system custodian and their line manager.

7.5. Monitoring

1) All privileged account usage shall be logged.

2) Logs of privileged account usage shall be stored in a location to which the PAC does not have access.

7.6. Review

1) Privileged User IDs shall be reviewed by the system custodian at least every 6 months to verify that:

   a) User IDs are still required
   b) Access is only available to authorised PACs
   c) Authorisations are valid

2) SOMs shall annually check records to ensure that reviews have been carried out for all of the systems supporting their service, and that processes have been followed appropriately.

7.7. Non-compliance

1) Non-compliance shall be followed up by the relevant line manager in combination with the SOM(s) affected.
2) Serious non-compliance, including that affecting systems holding personal data or data classified at Highly Confidential, shall also be reported to the Information Security Group.

8. Sanctions

This policy statement does not form part of a formal contract of employment with the bank, but it is a condition of employment that employees will abide by the regulations and policies made by the bank.

[1] Including maintenance, upgrades, etc.
[2] No blanket authorisations e.g. "root privilege for all Linux systems".
[3] For instance, the root account cannot be used to provide a group of staff privileged access. Each person needs a separate privileged account.

Policy approved

Chairman Director General Manager