1. Purpose and Scope

The purpose of this policy is this policy defines the requirements for the management of database user accounts and access to critical databases.

This policy is applicable globally.

2. Change History

Revision	Date	Author	Revision History
2.1	01/18/2017	Huan Do	Changed Template
2.2	04/18/2018	Huan Do	No changes
2.3	08/06/2018	Jeff Gibson	6.1.2.4 – added Database to resource list 6.1.3 – changes 6.2.1 – added monthly privileged access review 6.8 – clarified ID requirements 6.9 – clarified privileged access accounts

3. References

3.1. Principles: see **GITP-001 Global IT Policy Manual Principles** document.

3.2. Definitions: see **GITP-002 Global IT Policy Definitions** document.

3.3. Compliance: All employees, contractors and consultants are required to comply with the policies. An employee found to have violated any Brink's policy may be subject to disciplinary action, up to and including termination of employment. If a contractor violates a Brink's policy, Brink's may pursue its remedies under the contract, including without limitation, termination of the contract. Management should seek guidance from Human Resources and the Legal Department on these issues.

4. Authorization

This policy is authorized by:

Mustapha Kebbeh
Director, IT Security
Brink's, Incorporated

Policy Owner: Jeff Gibson, IT Global Director, Infrastructure Architecture

5. Roles and Responsibilities

5.1.1. Users: Responsible for all activity that is performed with their user account. User accounts must not be utilized by anyone other than the individual to whom they are issued.

6. Policy Statement

6.1. Account Creation.

6.1.1. All new database user account requests must be approved by the users Manager.

6.1.2. User account requests must include the following information, at a minimum:

6.1.2.1. User Account description.
6.1.2.2. Manager's name.
6.1.2.3. Access required.
6.1.2.4. Database resources to which the account will require access (i.e. Database, Role or privilege).

6.1.3. The Business System Owner or IT Application Owner must approve all access to their respective database resources.

6.1.4. Database user's accounts should be created with the least privileges required to perform their respective job function.

6.1.5. All database User IDs must be unique to each individual user in the database.

6.1.6. A User ID and password must be required to access the database (unless when authenticating through application or operating system).

6.2. Account Review & Revocation.

6.2.1. IT Management must review all database accounts on a quarterly basis, accounts with access that is considered privileged must be reviewed monthly. Evidence of such reviews must be maintained in a verifiable manner, and must also include a review of all generic and administrative accounts.

6.2.2. When a database user account is no longer needed, it must be immediately reported due to the local system support group, or IT Manager acting in this capacity, so that the account may be secured.

6.2.3. Database User Accounts will be terminated for any of the following reasons:

6.2.3.1. Access is no longer required by the user.

6.2.3.2. Account usage is abused and/or is a threat to the system.

6.2.3.3. User accounts with 90 days or more inactivity.

6.3. Account Creation.

6.3.1. New Database user account requests must be submitted to the local system support group with all required information. In smaller IT environments, a single IT Manager may be the one acting as system support and administration.

6.3.2. The system support group opens a tracking ticket for the account request. In lieu of a formal ticket tracking system, a less robust method for tracking Add/Change/Delete requests may be used. Examples include an Excel spreadsheet or manual log, as long as the method used is appropriate for the size and complexity of the environment.

6.3.3. The system support group assigns the account request to the appropriate Database Administrator.

6.3.4. The Database Administrator obtains management approval for the new user account if it was not submitted with the original request.

6.3.5. Database Administrator generates a password for the user account based, at a minimum, on the password requirements.

6.3.6. Database Administrator forwards the account name and password to the owner of the account and closes the tracking ticket for the account request. The account name is sent to the account requestor separately.

6.4. Account Termination Procedure.

6.4.1. An Account termination request is submitted to the system support group. In smaller IT environments, a single IT Manager may be the person acting as a system support and system administrator.

6.4.2. The system support group opens a tracking ticket for the account termination. In lieu of a formal ticket tracking system, a less robust method for tracking Add/Change/Delete requests may be used. Examples include an Excel spreadsheet or manual log, as long as the method used is appropriate for the size and complexity of the environment.

6.4.3. The system support group assigns the account request to the appropriate database administrator and obtains management approval for the account termination if it was not submitted with the original.

6.4.4. The database administrator reviews the impact of the termination of the user account to ensure there are no adverse side effects and disables the user account to process the request.

6.4.5. The database administrator then closes the tracking ticket for the account termination.

6.5. Requests for new Database User Accounts are documented and approved by a level of authority appropriate to the respective Country or Entity.

6.6. Database Generic accounts, including system accounts and other shared accounts such as those used in operations, must be documented and approved by Management.

6.7. Database Administrative access must be limited to authorized database administrators only. All accounts with administrative rights must be documented and approved by IT Management.

6.8. All Database IDs are unique to the User and require a valid password to log into the database (unless authentication is performed directly through the application or in other cases the operating system).

6.9. Default passwords for all database privileged access administrative accounts have been changed.

7. Appendices

7.1. Not Applicable