TEG Administrative Account Policy

Document Information

Version Number	1.0
Last Update	17/10/2022
Author	Matthew Coutts
File Name	Cyber Security Policy and Procedure
Document Title	Cyber Security Policy and Procedure
Document Owner (Role Position)	Global Head of Enterprise Technology, Risk and Cyber Security
Responsible Executive (Role Position)	Chief Technology Officer

Document Revision History

Version	Issue Date	Author	Comments	Approved By
1.0	17/10/2022	Matthew Coutts		Matthew Coutts

Document Approval and Authorisation by Senior Management

Version	Issued Date	Date Last Reviewed	Approver
1.0	20/10/2022	20/10/2022	Matthew Coutts

1.0 Purpose

TEG maintains several databases, applications and systems that contain or have access to private, sensitive and/or confidential information. To ensure that the information maintained within these systems remain secure, users should be granted access to these systems on a need to have basis only. That is, users should be granted access to a system only if that access is required for the performance of their job role and the level of access does not exceed that which will be necessary for the performance of that job role.

2.0 Service Level Agreement

Enterprise Technology Services will endeavor to process account requests within three business day of receipt. However, please note that during busy periods and depending on staff availability, it can take up to five business days to process some account requests.

3.0 Account Request Procedures

The following procedures should be followed when requesting for access to the following specific systems:

3.1 Active Directory based User Account (e.g., TEG Corporate Identity)

To request a TEG corporate identity for our active directory environment, please log a job in the Enterprise Technology heldesk

3.2 Ticketing Platform User Account

To request a ticketing platform user account, please log a job in for Systems Support in Jira

3.3 Cloud Platform User Account

To request a cloud platform user account (e.g., AWS), please log a job in for Technical Operations in Jira.

4.0 Privileged Access

Privileged Access will only be automatically granted to those users who require it as part of their role and/or function. This would typically fall to members of the Enterprise Technology and Technical Operations teams.

4.1 Super User Access (e.g. Domain Administrator, Root user, etc

Super User access (where the access permissions will grant access to everything within that environment such as a Domain Administrator or Root for a unix or database environment) can only be granted with the approval of the Global Head of Enterprise Technology, Risk, and Cyber Security.