Information Technology Access Control Policy

Document Information

Version Number	1.0
Last Update	15/10/2022
Author	Matthew Coutts
File Name	Information Technology Access Control Policy
Document Title	Information Technology Access Control Policy
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	21/10/2022	Matthew Coutts		Matthew Coutts

Document Approval and Authorisation by Senior Management

Version	Issued Date	Date Last Reviewed	Approver
1.0	21/10/2022	20/10/2022	Matthew Coutts

1. Purpose

TEG is committed to and is responsible for ensuring the confidentiality, integrity, and availability of the data and information stored on its systems.

The purpose of this manual is to define the minimum standards required to ensure that user access is based upon authentication and authorisation, and that unauthorised access to systems and services is prevented.

It is the responsibility of all Information owners and System Owners to determine appropriate access controls, access rights and restrictions for their information and information systems. They must assure that access is provided only to authorised users and that unauthorised access is prevented.

Furthermore, it is important for all Company staff, contractors, or visitors using Company ICT resources to understand the need to ensure appropriate authorisation to any system or service provided by the Company.

Section 2 - Scope

The minimum standards outlined in this manual apply to all Company ICT services and systems.

Section 3 - Audience

These standards are primarily aimed at system administrators and technical staff, including Information Technology Services staff, who are responsible for the management of access controls for Company ICT services and systems. This includes third parties supporting Company IT systems.

Section 4 - Requirements

User Registration

A formal user registration and de-registration process should be implemented to enable assignment of access rights.

The following control objectives must be covered in the design of user registration procedures:

- the allocation of unique user identities.
- all Company accounts must be accountable to an individual (e.g., no shared or generic accounts).
- obtaining appropriate authorisation prior account creation.
- for staff, authorisation is provided by the hiring manager as part of the recruitment process.
- preserving segregation of duties.
- user acknowledgement of the policy regarding acceptable use, outlined in the Information Technology Conditions of Use Policy.
- no reissuing of user identities to new users.

All third parties requiring access to Company information assets must have an active Company sponsor. All user accounts provided to third parties must include an expiration date no greater than one (1) year from the date the access is granted.

User Access Provisioning

Access privileges are to be assigned through the use of the Role-Based Access Control (RBAC) model.

RBAC is an access control mechanism that permits system administrators to allow or disallow other user's access to objects under their control.

The "role" in RBAC refers to a system of user roles, which are assigned to user groups and their users. Roles are assigned permissions, which define what a user can or can't do within a system or on an object. Roles can be particular to an application or may be defined more broadly as a job function or user type within the Company and may be a superset of more granular roles.

Roles can be granted new permissions as new applications and systems are incorporated, and permissions can be revoked from roles as needed. This type of access simplifies management of privileges and permissions.

The following RBAC implementation standards apply:

- a user can only have access to an object (i.e., dataset) based on an assigned role.
- roles are to be defined based on a persona or job function. A persona is a profile that can be used to describe a type of user, e.g., staff, contractor, guest.
- permissions are defined based on role's authority, and responsibilities within a job function or of a persona.
- operations on an object, such as view, edit or delete, are invoked based on permissions assigned to a role.
- permissions configured on objects should only be based on roles, and not users.
- roles are designed and implemented based on the principle of least privileged.
- a role contains only the minimum number of permissions required.
- a user's account is assigned to a role that allows him or her to perform only what is required for that role.

Privilege Management

All access privileges will adhere to the following principles:

- Need to know – the legitimate requirement of a person to know, access, or possess sensitive information that is critical to the performance of the authorised job function.
- Least Privilege – every user and program must operate using the least set of privileges necessary to complete the authorised job function.
- Segregation of duties – the practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process.

Need to know is enforced through the User Access Provisioning process.

Least privilege and segregation of duties are achieved by:

- limiting the role of system administrator to the fewest number of individuals necessary to achieve adequate service.
- implementing fine grain access privileges for the performance of privilege tasks.
- separating system administrator accounts from regular user accounts.
- separating system administrator functions from audit and logging functions. System administrators must not have the ability to modify or de-activate logs of their own activities.

In addition to various regular end-user roles, programmers, developers and testers will have separate roles with different privileges to system administrator roles.

Review of User Access

Company information asset and IT asset owners must review user access rights on a regular basis to ensure that role changes, such as promotion, demotion, transfer, and termination are correctly reflected in all information systems under their management.

Removal or Adjustment of Access Rights

The access rights of all users to information and information processing facilities shall be removed upon termination of employment, contract or association with the Company, or adjusted upon change.

Passwords

Username and passwords are used to facilitate authorised access to Company information assets. These credentials are intended to protect data from unauthorised access and ensure that only authorised users have access.

All initial system and application passwords must be issued by Company staff through a secure means. Once a password has been issued, full responsibility for that account and associated password is transferred to the user. On first login all initial passwords will need to be changed, this will be an automated enforcement mechanism configured for all systems and applications to which users are being granted access.

Password Requirements

All passwords, including initial passwords, must be constructed and implemented according to the following rules:

- passwords must be at least 8 characters in length.
- passwords must include at least one uppercase and one lowercase letter, one number, and one special character (i.e., %,* or similar);

- passwords must not contain any user identifier, or any part of the user's name.
- passwords that are the same as the last 24 passwords that have been used must not be re-used.
- passwords must not contain common or banned words, i.e., those known to be commonly used, expected, or compromised, e.g.:
- passwords obtained from previous breach corpuses, i.e., passwords known to be compromised; or
- repetitive or sequential characters (e.g., 'aaaaaa', '1234abcd').

Password Protection

The following user account controls must be enforced for all systems:

- account lockout threshold: 5 invalid logon attempts.
- account lockout duration: 15 minutes.
- reset count lockout counter after 15 minutes.
- minimum password age: 1 day.

Users must be forced to change their password if their credentials are known or suspected to be compromised.

In the event that a password has been shared with Information Technology Services for troubleshooting scenarios, the password must be immediately changed after this work is complete.

In the event that an account or password is suspected to have been compromised, the incident must be reported to the IT Service Desk and the password must be changed immediately.

Mobile Device Passwords

All smart devices containing Company data (including email) must be secured with either:

- a 6-digit PIN; or
- a Biometric lock with a compliant backup password/PIN.

Privileged Accounts

The following clauses apply to all privileged accounts created for Company owned or managed systems, including but not limited to:

Privileged Personal Accounts - privileged accounts assigned to individual users (typically Company IT Support Staff). Examples include the following privileged groups: DBA, Server Administrator, Tenant Admin, Domain Admins.

Generic/Shared Administrative Accounts - privileged accounts that exist in virtually every device or software application. These accounts hold "super user" privileges and are often shared among Company IT Support staff. These accounts may be used by multiple users. Examples: Windows Administrator, UNIX root, Oracle SYS, SA.

Break Glass (Emergency) Accounts – break glass accounts are a type of Generic/Shared Administrative Account used by the Company when elevated privileges are required for business continuity, disaster recovery, or to fix urgent problems.

Service Accounts – these are privileged accounts that provide a security context to a running service, daemon or process, such as a file server, web server, e-mail server, etc., or are used by applications to access databases and other applications.

Privileged accounts provide a high degree of access to Company ICT resources and therefore pose a significant risk if used in an unauthorised manner.

As privileged accounts provide a significant level of control over Company ICT resources, individuals with access to these accounts are expected to exercise a high degree of caution.

All users with access to privileged accounts must maintain the confidentiality of any information that they have access to both during and after their employment with the Company.

Privileged Account Password Requirements

Privileged user access to any of the Company's ICT domains, services and systems must be authenticated using multi-factor authentication (MFA) unless there is a system limitation that prevents its use. Privileged credentials must only be used when performing tasks that specifically require those privileges. While performing normal activities, administrators must use a separate, unprivileged account.

All privileged account passwords, including initial passwords, must be constructed and implemented according to the following rules:

- password length – the password must be at least 14 characters long.
- password complexity – the password must include one uppercase and one lowercase character, one number and one special character (i.e., %,* or similar).
- password attributes – the password must not contain a user identifier or any part of the account owner’s name.
- password history – passwords that are the same as the last 24 passwords that have been used must not be re- used.
- password expiry – passwords must be changed immediately when a staff member who has accessed that password leaves their employment with the Company.
- minimum password age – 1 day.
- account lockout threshold – 5 invalid logon attempts.
- account lockout duration – 15 minutes.
- reset account lockout counter after 15 minutes.
- group or shared passwords are prohibited (unless an exception is approved). The only exceptions to this are.
- ‘Break-glass’ accounts, which must not be used for day-to-day support.
- ‘test’ accounts, which may be shared during pre-production phases.

default passwords of any system, network resource, application or database etc., must be changed either during the installation process or immediately thereafter.

Break-Glass Accounts

Passwords for break-glass accounts should be machine generated and held in the Company's approved Privileged Account Management (PAM) platform to ensure they remain available to system administrators.

A break-glass procedure defining the roles and responsibilities for use of break glass accounts should be created by each relevant System Owner or Information owner.

- When a break-glass account is used, access to the privileged account must be:
- limited to the minimum amount of time necessary.
- associated to a change, problem or incident number/ticket.
- recorded by the specific database, system or application; and
- logged in an auditable record (which identifies the individual User who 'broke the glass'), such as within the PAM platform, for later review.

After a break-glass procedure has been completed, the password for the break glass account must be changed.

Password Expiry and Multi-Factor Authentication (MFA)

If a company-ID or privileged account is protected with MFA, then there is no requirement to expire the associated password.

If a company-ID or privileged account is not protected with MFA, then the requirement for password expiry will be based on the data classification that a company-ID is authorised to access based on the roles that it has been assigned:

Specialty Devices

Due to the wide variety of specialty devices and their frequently limited capabilities, particularly with regard to password management, specialty devices such as fax machines, printers, physical access control equipment, copy machines, phones, etc. are not subject to these requirements unless those devices are used to store or protect Highly Restricted information or perform highly critical functions.

Service Account and Simple Network Management Protocol (SNMP) Community Name Requirements

- The password length and complexity requirements for service accounts and SNMP community names are increased to allow for less frequent expiration. This ensures that key services are not disrupted due to regular change.
- Service accounts must not be shared between applications or services, i.e., a separate account must be created for each application and service.
- Using a standard user account or Uni-ID to run system services is prohibited.
- End users and administrators are not permitted to remotely or interactively log in using service account credentials except as required to support or troubleshoot the specific service:
- password and SNMP community name length – must be a minimum of 15 characters long.

- password and SNMP community name complexity – must include at least one uppercase and one lowercase character, one number and one special character (i.e., %,!,* or similar);
- password and SNMP community name attributes – must not contain a user identifier or any part of a name.
- password and SNMP community name reuse – must not be use passwords or community names that are identical or substantially similar to those that have been previously used.
- password expiry – generally never, but the password must be changed when someone leaves the Company who would know or had used the password.

Secure Shell (SSH) Keys

SSH keys are a common way to connect to Unix\Linux based computers. Whilst they can provide a convenient and secure means of connection, the Company does not currently have appropriate processes to ensure the security of their use across a user's lifecycle at the Company, e.g., SSH keys may not be reliably disabled when a user leaves the Company.

As such, the use of SSH keys for authentication is prohibited.

Password Management Software

Passwords must not be written down or stored in clear text, although password management software may be used. Special care should be taken to secure the password tool, as it will grant access to all passwords.

The password manager tool must employ encryption at AES256 or SHA2 or stronger. The password used to access this application must also be very strong and unique, and meet the requirements of a Service Account Password.

Use of cloud-based password management tools is forbidden unless MFA is used.