Information Technology Security Access Policy

Document Name	Document Version Number	Review Date
Information Technology Security Access Policy	1.0.1	October 2024
Date Adopted	**Minute Number**	**Status**
21 October 2020	5737	Re Adopted, No Alterations

Purpose

This policy enhances the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of Council which must be managed with care. All information has a value to the Council. However, not all of this information has an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.

Formal procedures must control how access to information is granted and how such access is changed.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

Scope

This policy applies to all Councillors, Staff, and Volunteers, of the Council (including system support staff with access to privileged administrative passwords), contractual third parties and agents of the Council with any form of access to Greater Hume Shire Council's information and information systems.

Definitions

Access control rules and procedures are required to regulate who can access Greater Hume Shire Council's information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing Council information in any format, and on any device.

Policy Content

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

When an employee leaves the Council, their access to computer systems and data must be suspended at the close of business on the employee's last working day.

It is the responsibility of the Director/Manager to request the suspension of the access rights via the Information Technology Coordinator by way of completion of the relevant forms and Information Technology Security Access Procedure.

Links to Policy
Records Management Policy
Bring Your Own Device Policy
Internet, Email and Computer Use Policy
Communications Policy
Fraud Control Policy
Volunteer Policy
Social Media Policy

Links to Procedure
Information Technology Security Access Procedure
Records Management Procedure
Privacy Management Plan

Links to Forms
CORP - Personnel Security Access Internal
CORP - Personnel Security Access External
CORP - Personnel Security Access Internal
CORP - Personnel Security Access External
CORP - Personnel Security Access Exiting
CORP - Personnel Security Access InfoXpert - Specific Access
CORP - Personnel Security Access Mobile Phone/Device
CORP - Personnel Security Access VPN Remote Access
CORP - Personnel Security Access Website
CORP - Personnel Security Access Sub Form – Authority
CORP - Personnel Security Access Sub Form – InfoXpert
CORP - Personnel Security Access Sub Form – Network
CORP - Personnel Security Access Sub Form - Single Access
CORP - Personnel Security Access Sub Form – Reflect

References
NIL

Responsibility
All Staff
IT Coordinator

Document Author
Manager Corporate Services

Relevant Legislation
Nil.

Associated Records
Nil.