CP.65 ICT Security Access

Responsible Department	Corporate Services
Resolution Number	C.5153
Resolution Date	16/10/2024
Next Scheduled Review	2026/27
Related Shire Documents	Council Policy CP.3 Code of Conduct for Councillors, Committee Members and Candidates Management Policy MP.1 Code of Conduct – Employees, Volunteers, Contractors and Agency Staff Working from Home Agreement Council Policy CP. 63 ICT Remote Access Management Council Policy CP.64 ICT Cybersecurity Incident Management
Related Legislation	*OAG Information Systems Audit Local Government 2021/22*

OBJECTIVE

This policy outlines the guidelines and procedures for granting, managing and revoking user access to information technology resources within the Shire. This policy is designed to ensure the security, confidentiality and integrity of the Shire's data while providing the appropriate access to authorised users.

SCOPE

This policy applies to Council Members, employees, contractors, volunteers, vendors and third-party users who access the Shire's information systems and resources.

POLICY

1. Access Control

- User access to information systems and resources will be granted based on the principle of least privilege. Council Members, employees and other users will only receive the minimum level of access necessary to perform their job functions.
- All access rights and privileges will be reviewed and approved by the ICT department or designated system administrator upon consultation with the relevant Executive Manager or the Executive Management Team (EMT) if

required.

- Access requests should be submitted through the authorised channels and will be subject to verification and approval based on roles and responsibilities.
- Access to sensitive or critical systems will require higher levels of approval.

2. User Account Management

- User accounts will be created for authorised Council Members, employees and contractors during onboarding. Accounts for temporary users, such as vendors or consultants, will be created and managed on an as-needed basis.
- User account provisioning and de-provisioning will follow a defined process to ensure timely updates when users change roles, leave the organisation or no longer require access.
- Password policies will be enforced for all user accounts, requiring regular password changes, strong passwords, and the prohibition of sharing or writing down passwords.
- 2 Factor Authentication is required to set up.
- Inactive user accounts will be reviewed and disabled or deleted in accordance with established procedures.

3. Monitoring and Auditing

- User access and privilege changes will be logged and regularly audited for security and compliance purposes.
- Unauthorised access attempts or violations of access policies will be monitored and investigated as necessary.
- Regular access rights reviews and audits will be conducted to ensure adherence to the principle of least privilege.

4. Training and Awareness

- Users will be responsible for safeguarding their credentials and reporting any suspicious activities immediately to the ICT department.
- Users are responsible for ensuring their use of the Shire's ICT systems are in accordance with the Shire's Code of Conduct.

5. Review and Revision

- This policy will be reviewed bi-annually, or as necessary, to ensure its continued relevance and effectiveness.

6. Security Access Levels

- The restricted security groups in the File Server are in Appendix 1.
- Security access levels to SynergySoft Security Access levels in Appendix 2.
- Approval in writing from an Executive Manager is required for employees needing particular security access to the file server folders or SynergySoft groups.
- Once approved, the ICT department can provide access.

APPENDIX 1

Access Groups	
G_1 CEO Office_CEO	
G_1 CEO Officer_Human Resources	
G_1 CEO Office_Human Resources_HR_MANAGER	
G_1 CEO Office_Safety & Training	
G_2 Corporate Services_Finance	
G_2 Corporate Services_Finance_Financials	
G_2 Corporate Services_ICT	
G_2 Corporate Services_Payroll	
G_4 Community Services_Recreation_Management	
G_5 Engineering Services_Policies_SoN	
G_6 Shared Corporate Documents_Executives_HR	
G_Administrator Access	
G_Council Members	

APPENDIX 2

SynergySoft Security Access Levels			
Files	**Security Levels From**	**Security Levels To**	**Who Has Access**
General Correspondence	0; 10	1; 19	All Staff
Confidential Environmental Health	20	29	CEO, EMDS, MBH
Finance Only Including Rates	30	39	CEO, EMCS, Rates, FM, SFO, Mgmt Acct, ProCoord
Payroll Only	40	49	CEO, EMCS, FM, SFO, Mgmt Acct, Payroll
Human Resources (Personnel Files)	50	59	CEO, Exec Managers, HR Assistant, People & Culture Coordinator
HR (CEO)	60	69	CEO, People & Culture Coordinator
Complaints (Directed towards Staff only)	70	79	CEO, Exec Managers, People & Culture Coordinator
Sensitive Correspondence	999	999	CEO, Records, Gov Coord, Gov Officer, People & Culture Coordinator