

CYBER SECURITY

Objective

This policy aims to establish and communicate the expectations for cyber security within Gilgandra Shire Council (Council), and to support the ongoing secure operation of the business in order to protect staff, customers and external partners.

Scope

This policy applies to all business units in all areas in which Council operates, and all employees and contractors. It more specifically applies to all data and information that Council processes, transmits or stores on its ICT infrastructure, systems or applications.

This policy applies to:


- Information, data and digital assets created and managed by Council, including outsourced information, data and digital assets
- Information and Communications Technology (ICT) systems managed, owned or shared by Gilgandra Shire Council and
- Operational Technology (OT) and Internet of Things (IoT) devices that handle Council data, Council held citizen data or provide government and/or Council services.

Policy

Confidential data

Confidential data is information for which unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the company, partners, affiliates, and customers. Common examples are:

- (a) Unpublished financial information
- (b) Personally Identifiable Information (PII)
 - (i) Account and/or Credit Card Numbers
 - (ii) Social Security Number (SSN)
 - (iii) Driver's License Number
 - (iv) Passport Number
 - (v) Tax File Number
 - (vi) Patient Identification Number
- (c) Data of customers/partners/vendors
- (d) Human resources records
- (e) Patents, formulas, or new technologies
- (f) Protected Health Information (PHI)
 - (i) Billing information from your doctor

- 
- (ii) Email to your doctor's office about a medication or prescription
 - (iii) Appointment scheduling note with your doctor's office.
 - (iv) MRI scans
 - (v) Blood test results
 - (vi) Phone records

Data security is the responsibility of all employees and contractors.

Protect Personal and Company Devices

All employees and contractors are required to protect personal devices used for work purposes and work devices safe in accordance with Council's *Cyber Security Policy Framework* (CSPF).

Manage Passwords Properly

Passwords are the first line of defence against numerous internet attacks GSC data, systems and infrastructure; hence password leaks are dangerous. All employees and contractors are required to keep all passwords secure and secret in accordance with Council's CSPF.

Transfer Data Securely

Transferring data introduces security risk. Therefore, all employees and contractors must take all reasonable steps to ensure data is transferred securely in accordance with Council's CSPF.

Additional Cyber Security Measures

To mitigate the possibility of security breaches, all employees must comply with Council's CSPF in relation to additional cyber security measures.

Remote Employees

Remote employees are also obligated to follow all aspects of this cyber security policy as well as Council's CSPF as they will also be using a company's/Council's systems, equipment, and confidential data.

Take Data Security Seriously

It is a requirement that all employees and contractors remain vigilant with cyber security and regard it seriously.

Relevant Legislation

State Records Act 1988 No.17

Associated Documents

- Cyber Security Policy Framework

- Australian Government ACSC – Essential Eight
- NSW Government Department of Customer Service – NSW Cyber Security Policy
- Standards Australia ISO/IEC 27001:2002

Responsible Officer:	Executive Leader Transformational Change		
Date Adopted:	19/09/23, 18/02/25	Resolution No:	178/23, 13/25
Version:	2	Review Date:	July (annually)