Policy Register
Cyber Security

Organization: **Balranald Shire Council**

Policy Adopted: **17.05.2022**
Minute Number: **2022/96**
File Ref: **D22.65215**

Document Control

Issue	Prepared / Revised By & Date	Action / Amendment Details	Approved By & Date
1	2022		Council 17.05.2022

Overview

Strong cyber security is an important component of the NSW Beyond Digital Strategy, enabling the effective use of emerging technologies and ensuring confidence in the services provided by Balranald Shire Council

Cyber security covers all measures used to protect systems and information processed stored or communicated on these systems (from compromise of confidentiality, integrity, and availability)
Cyber security is becoming more important as cyber risks continue to evolve

Purpose

The policy outlines the mandatory requirements to which Balranald Shire Council must adhere, to ensure cyber security risks to their information and systems are appropriately managed

Cyber Security Guideline

Balranald Shire Council has developed a Cyber Security Guideline to assist staff in the day-to-day awareness of cyber security and to help to ensure that the organization is actively preventing cyber security risks

Internal Audit

Balranald Shire Council ARIC committee shall review the cyber security risks annually and the organizations process to reduce or eliminate the risks
The ARIC will review the organizations cyber security guidelines, the organizations response to cyber attack and the organizations security controls
The ARIC will supply a statement annually for the External Audit process advising that they have undertaken a review as above and the recommendations that are being implemented

Cyber Security Guidelines

User Systems

- **Password Controls**
  - Balranald Shire Council staff will use strong passphrases that meet best appropriate practices using letters, numbers, and symbols
  - Passphrases will not be replicated across multiple platforms unless it has been enrolled into a Single Sign On environment
  - If a password has been suspected of being compromised, then a reset of the credentials will be initiated with new information provided to the appropriate Balranald Shire Council staff member
- **External Scams**
  - Balranald Shire Council staff need to be aware of scams, how to identify them and the most common vectors of attack
  - If privileged information is requested the identity of the person making the request must be identified to confirm their authority
  - Requests for changes related to the transfer of funds must be authorised by an appropriate Balranald Shire Council manager
  - Personally identifiable information must never be provided via telecommunication or email
  - Additional training is to be provided to staff to assist in recognizing scams with ongoing testing to be completed annually
- **Staffing Changes**
  - When applicable Balranald Shire Council management will follow procedures of both onboarding and offboarding of organization staff
  - When onboarding key information including user credentials, license requirements, level of system access and hardware requirements will be provided to a third party for configuration
  - When offboarding a Balranald Shire Council staff member correct procedures will be followed including removal of licensing, lock out of system credentials and forwarding of communication to the appropriate user
  - Balranald Shire Council will have periodic reviews of staff access and licensing to confirm that the most appropriate settings are in place

Information & Data Protection

- **Data Monitoring**
  - Records shall be kept when Balranald Shire Council data is used or moved both from the primary ERP (Content Manager) and external storage facility (SharePoint / OneDrive)
  - If internal organizational data has been exposed incorrectly to an external third party these records will be used as evidence of the exposure
- **Data Security**
  - Facilities and applications used for data storage shall have the ability for auditing and to prevent access from staff and third parties not authorised for the files in question
- **Data Storage & Classification**
  - Records of where information is stored will be kept separately from the data storage facilities
  - Information will be classified into categories to allow for appropriate filing (such as Confidential, Sensitive, Internal Use Only)

Cyber Security Tools

- **Endpoint Applications**
  - Anti-Virus applications will be installed on all user and server environments to protect against external intrusion and remove malicious programs where required
  - Anti-Virus applications are to be automatically patched on a regular basis to provide the latest protections available
- **Supported Operating Systems**
  - Device operating systems will be kept up to date and only versions currently supported by the software vendor with regards to maintenance and security updates

    - Device operating systems are to be automatically patched on a regular basis to provide the latest protections available
- **Supported Business Applications**
    - Business applications will be kept updated either through third party vendors or through regular automated patching
    - A Standard Operating Environment will be configured to streamline what applications are in use by organization staff and confirm that only trusted applications are in use
- **Remote Work**
    - Access to Balranald Shire Council infrastructure will be completed using Virtual Private Networks with internal security controls enforced
    - Organizational staff must not access secure information or systems from publicly accessible devices

Mobile Devices

- **Device Management**
    - Mobile devices provided by Balranald Shire Council or used for organizational purposes will have management applications installed
    - Management applications will provide the ability to provide secure connection to Balranald Shire Council networks and remotely wipe devices in the instance of loss or return upon staff offboarding
- **Organizational Data**
    - Balranald Shire Council data will only be accessed via mobile devices that have management applications installed

Business Continuity & Disaster Recovery

- **Core Infrastructure Replication**
    - Balranald Shire Council core infrastructure will be replicated to an Australian based data centre
- **Replication Security**
    - Any replication of Balranald Shire Council infrastructure must adhere to Australian security standards (including ISO 27001 and NSW Mandatory 25)
    - Any replication of Balranald Shire Council infrastructure must adhere to Australian data sovereignty laws
    - Any replication of Balranald Shire Council infrastructure must be kept secure and only accessed by approved staff and third-party contractors
- **Data Loss Plans**
    - In the instance where Balranald Shire Council has been notified of data breach or loss staff will initially follow the appropriate internal procedure or policy
    - Third parties and law enforcement will be informed immediately as is appropriate for the recovery of data or investigation of the source of a data breach
- **Time To Recovery**
    - In the instance where Balranald Shire Council is required to recover from a system fault or breach third party contractors will restore access to core infrastructure within a reasonable period
- **Offsite Replications**
    - A secondary replication of Balranald Shire Council infrastructure shall be kept for additional security and will adhere to the same security as listed above

Core Infrastructure Changes

- **Testing & Approvals**
    - Where core infrastructure or application updates are required Balranald Shire Council will work with third party contractors for the configuration of a suitable testing environment before moving the update to production
    - If additional infrastructure is required for testing purposes this will be configured as an ad hoc server in the organizations cloud environments
- **Implementation Procedures**
    - Once testing has been completed and approval provided by all third parties and Balranald Shire Council the changes are to be implemented within the organizations core infrastructure
    - Third party contractors will make themselves available for additional testing or issue rectification as required

Physical Site Access

- **Core Infrastructure Access**
  - Balranald Shire Council infrastructure stored at any of its locations and sites will only be accessed by authorised staff or third-party contractors (as per Appendix A)

Local Network Security

- **Ad Hoc Device Connection**
  - Approval must be provided by either Balranald Shire Council management or approved third parties before an ad hoc device can be physically connected to the local network
- **Local Wireless Network**
  - A separate wireless network is configured for the connection of public or ad hoc devices
  - Increased security rules are to be applied to this wireless network to prevent access to critical Balranald Shire Council infrastructure
  - These settings are to be replicated across all Balranald Shire Council locations and sites
- **Network Filtering & Security**
  - Firewall hardware is to be implemented at all Balranald Shire Council sites and locations to secure and filter incoming and outgoing network traffic
  - Application white and black listing to be configured to prevent the installation of malicious software
  - Network reports are to be provided to Balranald Shire Council stakeholders by third party contractors as requested

Payment Card Practices

- **Trusted Hardware & Applications**
- **Client Information**

Ongoing Compliance & Reporting

- **Security Compliance**
  - Ongoing security compliance checks to be completed by authorised third party contractors to confirm that best appropriate practice is being followed
- **Security Reporting**
  - Annual reporting to be provided showing where Balranald Shire Council is currently meeting security compliance requirements and where additional works are required
  - In the instance where additional works are required Balranald Shire Council will investigate and implement appropriate solutions

Appendix A: Authorised ICT Contacts

Policy Register - Cyber Security

Name	Position