OBERON COUNCIL

POLICY 2140

CYBER SECURITY POLICY

1. 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 Oberon 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

2. Purpose

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

3. Cyber Security Guidelines

Oberon Council has developed Cyber Security Guidelines to assist staff in the day-to-day awareness of cyber security and to help ensure that the organisation is actively preventing cyber security risks. The initial guidelines can be found as Annex A.

4. Accountability, Roles and Responsibilities

Cyber security is the responsibility of all in the organisation to ensure a collective approach to minimise risk. The Executive Management Team and managers are responsible for the ongoing training, mitigation and reporting of cyber related incidents.

Oberon Council through the Audit Risk and Improvement Committee (ARIC) will review the cyber security risks annually and the organisations process to reduce or eliminate the risks. The review will include the organisations cyber security guidelines, the organizations response to cyber attack and the organisations 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

Approving Authority	Oberon Council
Contact	Director of Corporate Services
Approval	Ordinary Meeting – 18th October 2022: Item 13.04
Revision Date	October 2023
Issue Date to Staff	14 November 2022

Annex A - Oberon Council – Cyber Security Guidelines

User Systems

- **Password and Account Access Controls**
    - Oberon Council staff will use strong passphrases that meet best appropriate practices. As at September 2022 the requirement is a minimum of eight characters using three of following four, upper case letter, lower case letter, number, symbol.
    - 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 Oberon Council staff member
    - Multi-factor authentication will be in force for all users[1] accessing the system outside of designated Oberon Council networks
    - The Microsoft 365 environment is geo-blocked to prevent access from outside of Australia.

- **External Scams**
    - Oberon 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 using an independently acquired alternate contact method
    - Requests for changes related to the transfer of funds must be authorised by an appropriate Oberon 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 Oberon Council management will follow procedures of both onboarding and offboarding of organisation staff
    - When onboarding key information including user credentials, license requirements, level of system access and hardware requirements will be controlled in accordance with privacy and security protocols.
    - When offboarding an Oberon 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
    - Oberon 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**
    - Record logs shall be kept when Oberon Council data is used or moved in the Office 365 environment. The logs can be reviewed by management and an access granted in accordance with the job role.

[1] For technical reasons certain accounts such as the account associated with backups will not have MFA but will use more complex passphrases.

  - If internal organisational 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)
  - Where appropriate a retention period will be attached to records

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 organisation staff and confirm that only trusted applications are in use
  - IT Staff will keep a software register listing the supported software. Requests for software to be added to the support list will be subject to approval by the IT Steering Committee

- **Remote Work**
  - Access to Oberon Council infrastructure will be completed using Virtual Private Networks with internal security controls enforced[2]
  - Organisational staff must not access secure information or systems from publicly accessible devices
  - Organisational staff must not access secure information or systems from public Wi-Fi networks such as those founds to hotels, airports and cafes. They should hotspot to a mobile phone instead

Mobile Devices

- **Device Management**

[2] Only IT staff need to directly access on-premises infrastructure. Non-ITstaff can access all applications using cloud based resources

  - Mobile devices provided by Oberon Council or used for organizational purposes will have management applications installed
  - Management applications will provide the ability to provide secure connection to Oberon Council networks and remotely wipe devices in the instance of loss or return upon staff offboarding

- **Organisational Data**
  - Oberon Council data will only be accessed via mobile devices that have management applications installed

Business Continuity & Disaster Recovery

- **Core Infrastructure Replication**
  - Oberon Council core infrastructure will be replicated to an Australian based data centre

- **Replication Security**
  - Any replication of Oberon Council infrastructure must adhere to Australian security standards (including ISO 27001 and NSW Mandatory 25)
  - Any replication of Oberon Council infrastructure must adhere to Australian data sovereignty laws
  - Any replication of Oberon Council infrastructure must be kept secure and only accessed by approved staff and third-party contractors

- **Data Loss Plans**
  - In the instance where Oberon 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 Oberon 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 Oberon 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 Oberon 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 Oberon 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**
  - Oberon Council infrastructure stored at any of its locations and sites will only be accessed by authorised staff or third-party contractors

Local Network Security

- **Ad Hoc Device Connection**
  - Approval must be provided by either Oberon 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 Oberon Council infrastructure
  - These settings are to be replicated across all Oberon Council locations and sites

- **Network Filtering & Security**
  - Firewall hardware is to be implemented at all Oberon Council sites and locations to secure and filter incoming and outgoing network traffic.
  - Application white and blacklisting to be configured to prevent the installation of malicious software
  - Network reports are to be provided to Oberon 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
  - Oberon Council will comply with the Essential Eight standard for computer security with a longer term plan to meet the Mandatory 25 as outlined by Cyber Security NSW.

- **Security Reporting**
  - Annual reporting to be provided showing where Oberon Council is currently meeting security compliance requirements and where additional works are required
  - In the instance where additional works are required Oberon Council will investigate and implement appropriate solutions

Documentation of Procedures

Key operational document registry in relation to the mitigation of Cyber Security will be created for staff and accessed via the Oberon Council Intranet or IT knowledge base. This registry will be updated regularly as per operational requirements.