Information Security Framework

Customer Guidance Document

Version 1.0
February 2021

macquarie
CLOUD SERVICES

Confidentiality Statement

This document contains Macquarie Telecom Pty Limited (Macquarie Telecom) propriety and commercially sensitive information. The recipient may disclose the information contained herein to any officer, employee, contractor or agent who has specific need to access the information but only to the extent that such disclosure is necessary for evaluating the products and services as described in this document and subject to that person being obligated to maintain the confidentiality of the confidential and commercially sensitive information.

Table of Contents

1. Compliance Guidance

1.1 Purpose

Macquarie Telecom operate a comprehensive Information Security Management System (ISMS). This document is intended to provide high level guidance for the implementation of the information security programs within Macquarie Telecom.

This document can be shared with customers or prospects only under an executed confidentiality agreement. It contains sensitive information relating to compliance, governance, systems, processes, and reporting relating to key standards including ISO 27001:2013 and APRA CPS 234.

1.2 Information Security Governance

1.2.1 Policy Frameworks

1. Macquarie Telecom has established and maintains an Information Security Management System (ISMS) and Business Continuity Plan (BCP) that operates within the broader Security Policy Framework. The ISMS is regularly reviewed and tested according to the compliance schedule (at least annually) and addresses requisite procedures, compliance, and exceptions.
2. Security assessments and compliance are signed off by appropriate security staff within Macquarie Telecom Business Units, and the Macquarie Telecom Board Audit & Risk Sub-Committee.
3. Macquarie Telecom currently holds the following certifications against its policy frameworks in respect of our Cloud Services, Government Services, Data Centres, and Secure Internet Gateways:
    a. PCI DSS 3.2.1
    b. ISO 27001:2013
    c. ISO 9001:2015, ISO 14001:2015, ISO 45001:2018
    d. ACSC PROTECTED Federal Government Secure Internet Gateway
    e. Licensed Telecommunications Carrier

1.2.2 Board responsibilities

1. Macquarie Telecom has implemented Cyber Security and Information Security policies that are regularly reviewed by the Board as part of its governance function. The Board's Audit & Risk Sub-Committee is responsible for overseeing the implementation of these policies, with such implementation also supported by Executive Management and the CISO function. Further security roles and responsibilities have also been delegated for such implementation.

1.2.3 Risk Management

1. Macquarie Telecom identifies, evaluates, and treats cyber and information security risks that may impact its environment through a Security Threat Assessment and Compliance program. A Security Risk Register is maintained as well as a Corrective Action Register aligned to the ISO 31000 framework.
2. Security reporting including security risks and threat profile assessments are conducted and reviewed on monthly basis. The Board's Audit & Risk Sub-Committee regularly reviews the Cyber Security Policy and compliance annually or when material changes are made. Incidents that exceed pre-defined thresholds are reported immediately.

1.2.4 Reporting

1. Macquarie Telecom has established a comprehensive cyber and information security reporting processes which includes review by Executives and the Board.
2. Macquarie Telecom Board Audit & Risk Sub-Committee has a formal policy review process, including but not limited to regular review of the Cyber Security, Information Security, and Risk Management policies. These reviews occur annually or when material changes or major incidences may occur.
3. Security profiles, major incidents (where applicable), and compliance are reported monthly or more frequently if required.

1.2.5 Regulatory awareness

1. Macquarie Telecom has an internal regulatory compliance team with processes in place to identify and respond to regulatory requirements which may materially impact the Cyber Security Environment.

1.3 Assurance / Controls Testing

1.3.1 Independent assurance reports

1. Macquarie Telecom continue to re-certify annually our ISO 27001 framework which includes independent assessment and reporting by SAI Global.
2. A recent addition to our certification portfolio is AICPA SOC2 Type 2 (Service Organisation & Controls) which includes an unqualified independent assessment report.
3. If results from an independent audit or internal testing indicate any Non-Conformance, area of concern or opportunity for improvement, these are collected in a Corrective Actions Register and prioritised for remediation based on internal assessment.
4. A summary of assurance reports may be shared with Customers if requested to verify that Macquarie Telecom controls meet the requirements.

1.3.2 Assurance function

1. Macquarie Telecom has an internal assurance function supported by external vendors.

1.3.3 Control weaknesses

1. Macquarie Telecom has vulnerability management process in place that includes issue identification, management, and notification. These include external penetration testing of critical assets and automated systems that report on weaknesses to be assessed and prioritised for remediation.
2. Formal processes are in place to promptly remediate any identified weaknesses.
3. As a contractual requirement Macquarie Telecom will agree to inform any APRA regulated Customers within 30 days of identification of any control weaknesses that cannot be remediated and represent a material risk to the Customer's information assets.

1.4 Human Resources / People & Culture

1.4.1 Awareness training

1. Macquarie Telecom provides cyber security awareness training to all employees and contractors upon commencement of employment. The training is refreshed annually.
2. Macquarie Telecom employees are made aware of, and must agree in writing to compliance with, the Macquarie Telecom IT Security Policy.
3. Macquarie Telecom Board and Executives have been provided with cyber security awareness training and are periodically briefed on updates as applicable.

1.4.2 Background checks

1. Macquarie Telecom's recruitment team performs a variety of pre-employment checks which may include reference checks, previous employment checks, Australian Right to Work checks, psychometric testing, police, and criminal checks depending on the specific role.

1.4.3 Staff roles and responsibilities

1. Macquarie Telecom employees have roles and responsibilities outlined within their position descriptions.
2. Macquarie Telecom's employment contracts contain clauses detailing disciplinary processes for breaches of employment contracts.

1.4.4 Professional skills and qualifications

1. Macquarie Telecom ensures that Customer data is protected by assessing relevant skills and qualifications of employees during the hiring process.
2. On the job training and mentoring is provided to employees where a gap in skills or qualifications is identified.
3. All employees receive periodic training that covers cyber security operations, risk management, or other IT related subjects as relevant to their role and responsibilities.

1.5 Response & Recovery

1.5.1 Incident Response and management

1. Macquarie Telecom has developed processes and deployed skilled staff for managing cyber and information security incidents under the major incident management process. The process includes playbooks of expected scenarios and is tested annually or when material changes are identified.
2. Security Incident Response and escalation is tiered depending on the event severity and includes communications of risks up to Executive Management and the Macquarie Telecom Board as appropriate.

1.5.2 Incident notification

1. Macquarie Telecom has formal processes in place that cover incident notification and communications, including Critical Issues Management Policy and Data Breach Response Plans.
2. Macquarie Telecom undertakes to advise Customers of any cyber security incidents that may materially affect the Customer's information assets and services.

1.5.3 Backups

1. All key systems and databases are regularly backed up. Backup restoration plans are tested periodically.
2. All key systems that can be accessed externally, have data that is encrypted at rest and in transit.
3. Macquarie Telecom owns and operates five datacentres, all located in Australia. Critical information is backed up and stored within our own datacentres.

1.5.4 Disaster Recovery Plan / Business Continuity Plan

1. Macquarie Telecom core data network services and cloud services are designed with high availability as a focus, with failover and redundancy built in to reduce the risks of outages and downtime to Customers.
2. Macquarie Telecom actively maintains a Business Continuity Plan across the business, the BCP is tested and results documented annually. Annual third-party audits and assessments are conducted of these artefacts.

1.6 Information Protection

1.6.1 Information Asset Classification

1. Macquarie Telecom does not implement information asset classification.
2. Physical assets that are assigned to a Customer are tagged and documented in an asset management system and is reviewed periodically.
3. Access to the asset management system is restricted to authorised staff. Access requirements are periodically reviewed.

1.6.2 Information security

1. Macquarie Telecom Customer data is readily identifiable. Such data includes information held in the:
   a. Billing system
   b. Sales Account tracking system
   c. Data Network and Voice network information, and Customer portals
   d. Emails relating to Customer services
   e. Cloud technical administrative systems and portals.

1.6.3 Information Sharing

1. Macquarie Telecom manages data and information sharing within its policies and procedures.
2. Macquarie Telecom does not share Customer data or information without receiving prior written permission from the Customer, save in circumstances where Macquarie Telecom is compelled to by governing regulations that requires the data to be shared with a government agency, regulatory authority, law enforcement agency, or other situations that are covered by the Macquarie Telecom Privacy Policy (macquarietelecom.com/privacy-policy/).

1.6.4 Data Locality

1. Customer data held by Macquarie Telecom is stored in Australia within Macquarie owned facilities.

1.6.5 Data Loss and Encryption

1. Macquarie Telecom uses an email-based Data Loss Prevention (DLP) system.
2. Data in transit across Macquarie Telecom's SDWAN network is encrypted using AES256 algorithms. Within the Macquarie Telecom core network, the traffic is decrypted and mapped securely across Macquarie Telecom's switch fabric.

1.7 Network & Operations Security

1.7.1 Vulnerability Management

1. Macquarie Telecom ensures that it is up to date with the latest cyber threats by running regular vulnerability assessments and management programs.
2. Managed security platforms get frequent threat and signature updates from security vendors.
3. Patch management is a key responsibility of the Macquarie Telecom internal system owner and adheres to vendor recommendations.
4. Threat intelligence is collected and monitored from several industry sources, including Microsoft ATP CERT along with other Government bodies.

1.7.2 Security Hardening

1. Macquarie Telecom ensures that all platforms, devices, and applications are hardened in line with vendor recommendations.
2. Periodic security and vulnerability reviews are conducted against key systems to ensure that hardening practices are applied according to policy and procedures.

1.7.3 Change Control

1. Macquarie Telecom runs formal change management process for all changes that may materially impact a Customer's service. Changes are reviewed and are subject to code reviews and vulnerability scans when required.
2. Customer network changes are reviewed and agreed to with a nominated representative from the Customer.
3. Internal system or network changes are subject to the Macquarie Telecom change management process. If a change has the potential to impact a Customer's service, the Customer will be notified in advance through the nominated personnel.

1.7.4 Security Operations

1. Macquarie Telecom has formal processes and controls in place to detect and respond to cyber-attacks with adequate staff skilled in cyber-attack detection and response.
2. Macquarie Telecom runs multiple centralised SIEMs that incorporate interfaces from all relevant platforms. Logging from key systems has been implemented.
3. The SOC function is performed by a team of Macquarie Telecom IT security staff within business day coverage and a 24×7 call out function. Macquarie Telecom has also invested in SOC tools that detect suspicious user behaviour and triggers security responses automatically.

1.7.5 Network Security

1. Macquarie Telecom has extensive cyber security protection controls at a network level to protect Macquarie's and Customer's information assets. They include but not limited to:
   a. Network segmentation with traffic flow controls
   b. Network security zones
   c. Firewalls
   d. Web application firewalls
   e. Database firewalls
   f. Network intrusion detection systems
   g. Network intrusion prevention systems
   h. Internet proxy with adequate protective controls
   i. Mail security with adequate protective controls.

1.7.6 Endpoint and Server security

1. Macquarie Telecom uses malware protection on endpoints to protect Customer's information assets.

2. Server infrastructure uses malware protection where appropriate and all key logs are stored and fed into multiple SEIMs for rapid threat detection and alerting.
3. Macquarie Telecom is actively migrating to a zero-trust model for all employee endpoints.

1.7.7 I Infrastructure security

1. Macquarie Telecom has strong access controls and policies implemented to ensure a model of least-privilege.
2. Key systems provide access authentication and traffic logging that is managed centrally.
3. Macquarie Telecom has implemented Role Based Access Control (RBAC) to ensure all privileged users are managed and audited regularly.
4. All supplier default credentials are disabled or reset prior to use.

1.8 Access Controls

1.8.1 Identity and Access Management

1. Macquarie Telecom's SDWAN solution and underlying core equipment provides access authentication and traffic loggings
2. Customer syslogs and NetFlow can be enabled from our Management Platform Orchestrator.
3. Access to core network equipment by Macquarie Telecom staff is securely managed.
4. Macquarie Telecom has implemented role-based access control to ensure all privileged users are managed and audited regularly
5. Remote Access requires Multi-Factor Authentication
6. All supplier default passwords have been reset

1.8.2 Multi-Factor Authentication

1. Macquarie Telecom uses Multi-Factor Authentication (MFA) and Single Sign-On to access privileged or sensitive systems wherever possible. This includes remote access to portals.

1.8.3 Password Security

1. Macquarie Telecom has a password policy in place that follows industry best practices to ensure appropriate password complexity. These policies are implemented via various technical controls based on the system.

1.8.4 Role-Based Access Control

1. Role-Based Access Control (RBAC) are implemented for all systems and includes segregation of duties. Key security roles and responsibilities are reviewed in line with our security policy. More frequent assessments are conducted on critical systems and roles.

1.9 Software Development & Acquisition

1.9.1 Web Application Security

1. Macquarie Web applications are adequately protected against cyber-attacks through various controls, these include:
    a. Layer 7 Web Application Firewalls
    b. Intrusion Detection Systems
    c. Intrusion Prevention Systems
    d. Version control implemented as recommended by the systems or software suppliers
    e. Automated vulnerability scans.
2. Customer data that is located within a web application is securely stored behind Macquarie Telecom firewall architecture.

1.9.2 Secure Coding

1. Macquarie Telecom ensures that vulnerabilities in developed code are minimised and rectified through various controls that include:
    a. Penetration testing is performed on web-facing systems annually
    b. Macquarie has implemented DevSecOps for code development.
    c. Mandatory OWASP training for employees as part of the development team onboarding
    d. Quarterly hackathons to refresh training
    e. Static code analysis tools to detect security issues performed monthly

f. Peer review of code prior to being committed to production
g. Automated tests to cover common security issues.

1.10 Physical & Environmental Controls

1.10.1 Data Centre Physical Access

1. Macquarie Telecom data centres are certified against several international standards including ISO 27001/2 which covers physical and environmental controls:
   a. Physical access
   b. Security guards / manned reception
   c. Designed to sustain natural disasters
   d. Backup power generators and redundant power feeds
   e. Redundant network connections
   f. Redundant cooling systems
   g. Fire detection and suppression systems
   h. Humidity and dust level alarms
   i. HR processes to address the immediate removal or employees or contractors access upon resignation or termination.

1.11 Supplier Management

1.11.1 Supply Contracts

1. Macquarie Telecom has formal contracts or agreements with all key suppliers. These contracts may not specifically cover cyber security language unless the supplier is directly supporting Macquarie Telecom cyber security services.

1.11.2 Third party supplier risk management

1. Third party supplier risks are incorporated into the overall Macquarie Telecom Board governance reporting structure, including but not limited to risk management and cyber security risk reporting.
2. Suppliers are managed as part of the Supplier Assurance process. If Macquarie Telecom discovers or is notified of a security incident involving a third party supplier, then it is reported to the relevant business level subject to the existing incident severity matrix.

1.11.3 Third party management

1. Macquarie Telecom has implemented supplier management policies and compliance oversight of contract deliverables and SLAs. This is typically managed by the functional owner of that contract or service. For key suppliers, including Telecom Access and security suppliers, they are actively managed with SLA reporting and frequent reviews.

1.11.4 Third party contracts

1. Macquarie Telecom has formal contracts or agreements with all key suppliers which are reviewed regularly. These contracts may not specifically cover cyber security language unless the supplier is directly supporting Macquarie Telecom Group cyber security services.
2. Macquarie Telecom Third party supplier contracts do incorporate compliance with the Australian Privacy Act, and all other applicable Telecom Industry legislative and regulatory requirements.

1.12 Data Ownership & Sovereignty

1.12.1 Data Ownership

1. Macquarie Telecom is fully compliant with the Australian Privacy Act to ensure the privacy of Customer data. (macquarietelecom.com/privacy-policy/).

1.12.2 Data Protection and Privacy

1. Macquarie Telecom applies RBAC processes to ensure only relevant staff or authorised third party vendor staff have access to Customer information as required. These controls and staff are reviewed periodically.

2. 2. Macquarie Telecom only stores pertinent information relating to the delivery of Customer services including the following:

   a. Customer Billing information
   b. Customer technical network configuration
   c. Sales and Account information
   d. Emails relating to Customer services

   This data is identified and distinguishable to each Customer.

   For Cloud services, the Customer may purchase other services such as Application Hosting and Data Storage.

   If at the end of a Services agreement with Macquarie Telecom, and the Customer requests Macquarie Telecom to delete Customer data, Macquarie will delete all data excepting where we have regulatory obligations to store information.

3. For access to Customer information in Cloud or Telecom services, Macquarie Telecom provides Customer portals including Macquarie Inview & MacView (such as Billing, Usage, Configurations, etc.) Data is segregated by application-level security based upon access tokens. This is tested using manual and automated processes and verified by third party penetration testing. SDWAN Orchestrator is multi-tenanted by design and allows Customers access to their own data partition. The security designs within the software prohibits Customers seeing other Customer data. The Orchestrator is hosted on Macquarie Telecom infrastructure within our Data Centres. Access is via Macquarie Telecom single sign-on with multi-factor authentication

1.12.3 Jurisdiction / Sovereignty

1. All data is stored in Australian Data Centres that are owned and managed by Macquarie Telecom.

Sydney
Level 15
2 Market Street
Sydney NSW 2000
T 02 8221 7777

Melbourne
Level 1
441 St Kilda Road
Melbourne VIC 3004
T 03 9206 6800

Brisbane
Level 15
127 Creek Street
Brisbane QLD 4000
T 07 3874 2300

Perth
Level 10
251 Adelaide Terrace
Perth WA 6000
T 08 9229 0000

Canberra
Level 7
54 Marcus Clarke Street
Canberra ACT 6277
T 02 6257 6277

Macquarie hub+
T 1800 789 999

Intellicentre 1
Level 16
477 Pitt Street
Sydney NSW 2000
T 1800 789 999

Intellicentre 2
17 – 23 Talavera Road
Macquarie Park NSW 2113
T 02 8221 7256

Intellicentre 4
Fairbairn ACT 2609
T 1800 789 999