INFORMATION SECURITY AND PRIVACY STATEMENT

How Megaport Limited and all of its relevant business lines and subsidiaries manage and implement Information Security to earn and maintain the trust of our customers by keeping your data secure

1. Megaport's Services and Regulatory Context

Megaport Limited (ASX: MP1) and each of its related entities and subsidiaries ('Megaport', 'we', 'us' or 'our') is a global leading Network as a Service (NaaS) provider. Using Software Defined Networking (SDN), Megaport's platform enables customers to rapidly connect to services across the Megaport network. Services can be directly controlled by customers through Megaport's web-based portal or the open Application Programming Interface (API).

Megaport is a member of the following partner programmes: Alibaba Cloud Technology, AWS Technology, AWS Networking Competency, Cloudflare Network Interconnect, Google Cloud Interconnect, IBM Direct Link Cloud Exchange, Microsoft Azure Express Route, Nutanix Direct Connect, Oracle Cloud, Rackspace RackConnect, Salesforce Express Connect, and SAP PartnerEdge Open Ecosystem.

Megaport Limited is incorporated in Australia pursuant to the Corporations Act 2001 (Cth) and is listed on the Australian Securities Exchange (ASX), and is therefore required to comply with the **ASX Listing Rules**.

Megaport's services are governed by various laws and regulations specific to the telecommunications industry (**Telco Laws**), with Megaport holding a licence, being registered with and/or overseen by the relevant telecommunications regulatory body in each country in which it operates, as required.

Megaport also holds an **ISO 27001 certification,** as discussed in detail in paragraph 3.1 below.

2. Data Processing

2.1 Our Customers' Transmission Data

Megaport's services enable customers to provision data networking connections and transmit their data quickly and efficiently via Megaport's SDN. Customers control what data is transmitted, by what methods (i.e. protocol and encryption), and to what destination. Megaport provides the transport mechanism, reading data packet headers in order to route and forward packets appropriately. Megaport only retains certain metadata for billing and troubleshooting purposes, in accordance with relevant Telco Laws. For details, see clause 6(d) of our Global Services Agreement.

The infrastructure that facilitates the provision of our services resides in securely managed data centres operated by established providers who implement environmental, physical, and logical controls in compliance with Megaport standards (see details in paragraph 3.4 below).

In the event of service disruptions, outages and/or suspected security incidents, our internal policies dictate that our Security, Regulatory, and/or Privacy teams be involved to ensure that the appropriate investigation, remediation, and statutory notification actions are taken.

2.2 Personal Data

As we provide business-to-business services to corporate customers, the personal data Megaport collects from customers is limited to what is required for our own basic account administration purposes, like any other organisation would (e.g. customer representatives' contact details and interactions with customer support). Also, like any other organisation, we process some personal information as part of our marketing, sales, vendor administration and human resources processes. You can read more about how we process such personal data in Megaport's Privacy Policy.

Megaport has a dedicated Privacy Team and has adopted an internal Personal Data Protection Policy and related procedures designed to protect privacy, comply with various privacy laws, and accommodate the following:

- Privacy screenings on all new projects, processes, systems, products and services, and where required, comprehensive privacy impact assessments carried out by the relevant Department Head (or delegate) in conjunction with the Privacy Officer;
- Assessing the adequacy of the privacy and security measures of our vendors, suppliers and partners and ensuring that the appropriate contractual protections are incorporated in their contracts (including GDPR-required Data Processing Addenda and EU cross-border standard contractual clauses);
- Ensuring the Privacy Team's involvement in security incident investigations where personal data is impacted; and
- Keeping records of our personal data processes, disclosures, breaches, and requests for access and information.

3. Information Security Policy

Megaport, its Board of Directors, Executive Team, and staff are committed to safeguarding the Megaport IT Assets. In commitment to this objective the Megaport board has approved an Information Security Policy and authorised the Information Security Risk Committee (**ISRC**) to establish, operate, and maintain an Information Security Management System (**ISMS**), employing a risk management process aligned to IEC/ISO 27001:2013 standard.

The ISMS and associated policy, processes, procedures, and standards govern all aspects of IT Asset use at Megaport and endeavours to minimise the risks associated with the use of those IT Assets through:

- Formal governance and oversight of risk management.
- Risk assessment (e.g. identify, assess, treat, monitor) according to the Megaport ISMS Risk Management Framework.
- Continual review and improvement.
- Ensuring compliance with all applicable legal, regulatory, and commercial requirements.
- Application of risk treatment in the form of policy, process, procedures, standards and controls.

The objective of the ISMS and Information Security Policy for Megaport is to minimise risks to Megaport's IT Assets as expressed in the loss or degradation of security characteristics:

- Confidentiality – by which it is available only to authorised persons or systems.
- Integrity – by which it is changed only by authorised persons or systems in a permitted way.
- Availability – by which it can be accessed by authorised persons when needed.

3.1 ISO 27001 Certification

Megaport manages an Information Security Management System (ISMS) compliant with the ISO/IEC 27001:2013 standard. Certification was received on 9 December 2020 and the ISO/IEC 27001 certificate and Statement of Applicability are available upon request. Megaport's ISO/IEC 27001 certification is subject to an internal audit and an external surveillance audit annually.

ISO Scope Statement

Provision of Megaport's Software Defined Network (SDN) Services, including Switch port, Virtual Cross Connect (VXC), Megaport Cloud Router (MCR), Megaport Virtual Edge (MVE), and Internet Exchange (IX) and its supporting infrastructure, in accordance with the ISO/IEC 27001 Statement of Applicability (SoA) version 1.0.

ISO Scope Description

All Megaport operations are governed by the ISMS. The scope of ISO audit and certification is focused on the business processes, technology, and people involved in delivering customer SDN services.

This scope reflects Megaport's operating methods and information technology and Business Continuity Strategy that discards the traditional castle-and-moat operating model in lieu of a more adaptive, virtual organisation model. This approach leverages cloud service-based technologies that are capable of conducting operations almost anywhere, globally.

The scope boundary includes:

- Administrator endpoint;
- Application and server infrastructure residing in cloud service environments;
- Virtual (e.g. AWS) and physical (e.g. DC, carrier) network segments and media; and
- Physical network infrastructure deployed in DCO partner premises.

It explicitly excludes physical locations in which Megaport staff or technology operate, including:

- The physical environment where administrators perform their duties and the network connection in which they use;
- Physical data centre sites, rooms, or racks;
- Network segments beyond the Megaport customer-facing switchport (i.e. cross connect into customer premise equipment).

Business Processes

The following processes are included in the ISMS scope:

- Design, procure, or deploy network media, infrastructure, or point-of-presence locations;
- Configure, activate, change, terminate, or support customer services or issues;
- Monitor, maintain, or report on customers' services or network and associated infrastructure (i.e. health, performance, and capacity monitoring and remediation);
- Design, develop, maintain, or enhance customer consumed services, interfaces, and orchestration components; and
- Design, develop, maintain, or enhance monitoring, management, maintenance, productivity solutions and tools.

People

Megaport staff, and when appropriate contractors, are directly responsible for the above business processes, including:

- Information Security Risk Committee
- Product Team
- Engineering Department
- Operations Department
- Global Procurement Team

Locations

Megaport presence reaches over 716 enabled data-centre locations globally involving more than 100 data centre operators (DCO). Given this extensive reach, reliance on DCO management of physical security controls, and Megaport's more adaptive, virtual approach to Information Security, no data centre locations have been included in Megaport's ISO compliance scope. All physical locations, with the exception of the Brisbane head office, are excluded from audit and certification.

Megaport and customers rely on data centre operators to ensure that physical security controls are implemented and effective in the relevant data centre(s). For specific questions related to physical security controls, consult the data centre operator in which your infrastructure is located.

While not explicitly in scope for certification, the ISMS and associated risk management processes account for the operation of IT infrastructure in these controlled environments and treatment ensures that any risk associated with any related threats is minimised. This includes controls relating to explicit hardening standards, configuration change practices, and monitoring for unauthorised or suspicious activity.

The inclusion of the Megaport Brisbane head office address is a requirement of JAS-ANZ certification; however, no production equipment or network connections are operated from this or any Megaport office location. Standard building security controls are employed but many physical security controls of Annex 11 are excluded as they are the responsibility of the building lessor.

ISO Statement of Applicability (v1.0) Exclusions

Megaport's ISO Statement of Applicability (v1.0) can be provided upon request. It applies all ISO 27002 controls with exception of those noted and justified below:

ISO 27002 Control	Applicable	Justification
8.3.1 Management of removable media	No	Use of removable storage media is prohibited in the production environment thus related procedures are not required.
8.3.2 Disposal of media	No	
8.3.3 Physical media transfer	No	
11.1.1 Physical security perimeter	Yes	Only applicable to the Brisbane head office location. No production equipment resides in the head office location.
11.1.2 Physical entry controls	Yes	
11.1.3 Securing offices, rooms, and facilities	No	No physical data centres are within ISMS scope and this control does not apply to Brisbane head office.
11.1.4 Protecting against external and environmental threats	No	
11.1.5 Working in secure areas	No	
11.1.6 Delivery and loading areas	No	

11.2.1 Equipment siting and protection	No	
11.2.2 Supporting utilities	No	
11.2.3 Cabling security	No	
11.2.4 Equipment maintenance	No	
11.2.5 Removal of assets	No	
14.2.4 Restrictions on changes to software packages	No	Neither open source or COTS is not modified by Megaport developers.
14.2.7 Outsourced development	No	Software Development work is not outsourced.
18.1.5 Regulation of cryptographic controls	No	There are no specific agreements nor jurisdictions in which Megaport operates that regulate the use of cryptographic material used by Megaport.

3.2 Information Security Roles and Responsibilities

The ISRC is composed of the Executive Team, plus representatives from the Information Security, Privacy and Compliance departments. The primary role of the ISRC is to govern the ISMS and ensure that it aligns to Megaport's Information Security strategy and achieves Megaport's Information Security objectives.

The ISRC will sponsor and actively support the ISMS and compliance with relevant statutory, contractual and regulatory requirements (e.g. ISO 27001:2013, SOC, PCI-DSS) by:

- Ensuring that the Information Security Policy and associated policy framework is established, ratified, and communicated.
- Governing the risk management processes of the ISMS.
- Reviewing and assigning roles and responsibilities for the management of information security, as required to meet the objectives of the ISMS.
- Promoting the continual improvement of the ISMS through periodic review and process refinement.
- Continuously communicating the importance of effective information security management and of conforming to the Information Security Management System requirements.

3.3 Risk Management Framework

The methodology adopted by Megaport and used in completing the initial and all on-going Information Security Risk Assessments for the risk management process is aligned to the following standards:

- ISO/IEC 27005:2011 Information Security Risk Management
- ISO/IEC 31000:2009 Risk Management
- ISO/IEC 27001:2013 Information Security Management

3.4 Information Security Controls

Facilities: Production infrastructure facilitating Megaport services resides in securely managed data centres operated by established providers that implement appropriate environmental, physical, and redundancy controls as prescribed by regulations and customary business practices within their region of operation. For specific questions related to physical security controls, consult the data centre operator in which your infrastructure is located.

Network Security: Production network infrastructure is only installed and operated from authorised data centre providers. Perimeter security is managed by stateful, protocol aware filtering mechanisms (e.g. AWS Security Groups) or hardened Access Control Lists (ACL). Perimeter-facing infrastructure is hardened against CIS Benchmarks where available and vendor best-practices. Network resources are protected using network security devices such as firewalls and Intrusion Detection Systems (IDS).

Endpoint Security: Megaport user endpoints are fully configuration managed with hardening standards applied and employ next-generation anti-malware agents to protect against and detect malicious activity.

Server Security: Megaport production servers are deployed and secured in cloud service provider environments - primarily Amazon Web Services (AWS) public cloud and to a limited extent Google Cloud Platform (GCP). Megaport operates IT Assets within these environments in acknowledgement and consideration of the applicable shared responsibilities models for AWS and GCP.

Server instances are managed and maintained according to DevOps security principles and best practices. Control is carefully managed via a strict continuous integration/continuous delivery (CI/CD) pipeline and most instances are ephemeral. As part of this process, we maintain change control procedures and regularly apply software patches to our infrastructure. Critical data is routinely backed up and recovery testing conducted periodically.

Application Security: Megaport customer web portal and API are protected via a web application firewall (WAF), DDoS prevention service and regularly penetration tested. Customer communications with our web portal and API are secured by Transport Layer Security (TLS) and up-to-date ciphers.

Identity and Access: Megaport users are provisioned with only required access privileges and removed upon role or employment change. Critical systems are authenticated with multiple factors and password strength policy requirements.

Monitoring and Response: Megaport monitors its systems and has extensive audit logs to detect security incidents, and has a defined Incident Response Framework including policies, processes, and procedures to respond to incidents.

Security Awareness Training: All staff receive training on joining Megaport, and annually thereafter, with regards to the Information Security Management System (ISMS) and associated risk management processes, Information Security Policy, Personal Data Protection & Privacy Policies, and the procedures and individual responsibilities regarding each. Information Security and Privacy awareness updates are provided when appropriate to bring awareness to and combat external threats.

3.5 Customer Responsibilities

Information security is a shared responsibility between Megaport and our customers. As Megaport offers telecommunication services, customers should be aware that, while the services themselves are isolated and segmented, they are deployed over a shared underlying network technology.

By using Megaport's SDN, customers should evaluate and employ additional controls, as deemed appropriate including but not limited to:

- Securely managing its authentication credentials for Megaport's web portal and API.
- Enabling connections only to trusted external parties.
- Ensuring that network packet filtering mechanisms, such as firewalls, are applied as necessary and ensure only explicitly permitted and traffic is exchanged.
- Apply transport or application-layer encryption to transmitted data.

- Ensuring sufficient physical port and service diversity is provisioned to satisfy a customer's redundancy requirements, as well as compliance with any recommendations from Megaport partners.
- Preventing RFC-1918 compliant address space prefix advertisement to external peers and ensuring prefixes are accurate, registered, owned by the customer, and restricted to those intended.

Vincent English
Vincent English (Mar 12, 2021 15:13 GMT+10)

Vincent English – CEO Megaport

12 March 2021