INFORMATION SECURITY AND PRIVACY STATEMENT

How Megaport manages and implements Information Security to earn the trust of our users by keeping your data secure

Megaport Services

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 their mobile device, computer, or the open Application Programming Interface (API).

Megaport is an Alibaba Cloud Technology Partner, AWS Technology Partner, AWS Networking Competency Partner, Google Cloud Interconnect Partner, IBM Direct Link Cloud Exchange provider, Microsoft Azure Express Route Partner, Nutanix Direct Connect Partner, Oracle Cloud Partner, Salesforce Express Connect Partner, and a member of the SAP PartnerEdge open ecosystem.

Compliance

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

Megaport's services are also 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.

ISO 27001 Certification

Megaport is currently undertaking a project, with the assistance of external management consultants, aimed at achieving compliance with the ISO 27001 standard in 2020. This project has five key phases and is currently progressing through Phase 3.

- Phase 1: Information Gathering, Scope and ISMS Definition.
- Phase 2: Information Security Risk Assessment.
- Phase 3: Risk Treatment (Security Roadmap).
- Phase 4: Internal Audit and Management Reviews.
- Phase 5: On-site Certification Audit.

Data Processing

Transmission Data:

- Megaport's services enable customers to provision data networking connections and transmit raw 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 merely 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: https://www.megaport.com/legal/global-services- agreement/.

- The infrastructure that facilitates the provision of our services resides in securely managed data centers operated by established providers who implement environmental, physical, and logical controls in compliance with Megaport standards

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, and vendor administration processes. You can read more about how we process such personal data in Megaport's Privacy Policy: https://www.megaport.com/legal/privacy-policy/.
- Megaport has a dedicated Privacy Team and has adopted an internal Personal Data Protection Policy and related procedures designed to protect privacy and comply with various privacy laws, including to accommodate the following:
    - privacy screenings on all new projects/processes and privacy impact assessments where required
    - assessing the privacy and security measures of our vendors and ensuring that the appropriate contractual protections are incorporated in their contracts
    - ensuring the Privacy Team's involvement in security incident investigations where personal data is impacted
    - keeping records of our personal data processes, disclosures, breaches, and requests for access/information

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 (**Committee**) to establish, operate and maintain an Information Security Management System (**ISMS**) employing a risk management process aligned to 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 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 the minimisation of 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 an allowed way.
- Availability – by which it can be accessed by authorised persons when it is needed.

Information Security Roles & Responsibilities

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

The Committee will sponsor and actively support the ISMS and compliance with relevant statutory, contractual and regulatory requirements (e.gt 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.
- Review and assign 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 communicate the importance of effective information security management and of conforming to the information security management system requirements.

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.

Information Security Controls

- **Data Processing Facilities:** Production infrastructure facilitating Megaport services resides in securely managed data centers 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 please consult the data center operator in which your infrastructure is located.
- **Network Security:** Production network infrastructure is only installed and operated from authorised data center providers and, to the greatest extent possible, isolated from the public Internet. Our network is protected using network security devices such as firewalls and intrusion detection systems (IDS).
- **Endpoint Security:** Megaport user endpoints are fully configuration managed and employ next-generation anti-malware agents to protect and detect malicious activity.
- **Server Security**: Megaport production servers are deployed and secured in Amazon Web Services (AWS) public cloud, managed and maintained according to DevOps security principles and controlled through a strict continuous integration/continuous delivery (CI/CD) pipeline. As part

of this process, we maintain change control procedures and regularly apply software patches to our infrastructure. AWS does not have access rights to our applications or data.

- **Application Security**: Megaport customer web portal and API are protected via a web application firewall (WAF), DDoS prevention service and penetration tested annually. Customer communications with our web portal and API are secured by Transport Layer Security (TLS).
- **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**: Megaport staff are trained on hire with regard to Information Security Policy and responsibilities are updated regularly regarding appropriate behaviour to combat external threats.

Customer Responsibilities

Information security is a shared responsibility between Megaport and our customers. By using Megaport's SDN, the customer should evaluate and employ additional controls, as deemed appropriate, including but not limited to:

- Securely managing its authentication credentials for Megaport 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 the those intended

Vincent English
Vincent English (Aug 5, 2020 13:30 GMT+10)

Vincent English
Chief Executive Officer
Megaport

27 July 2020