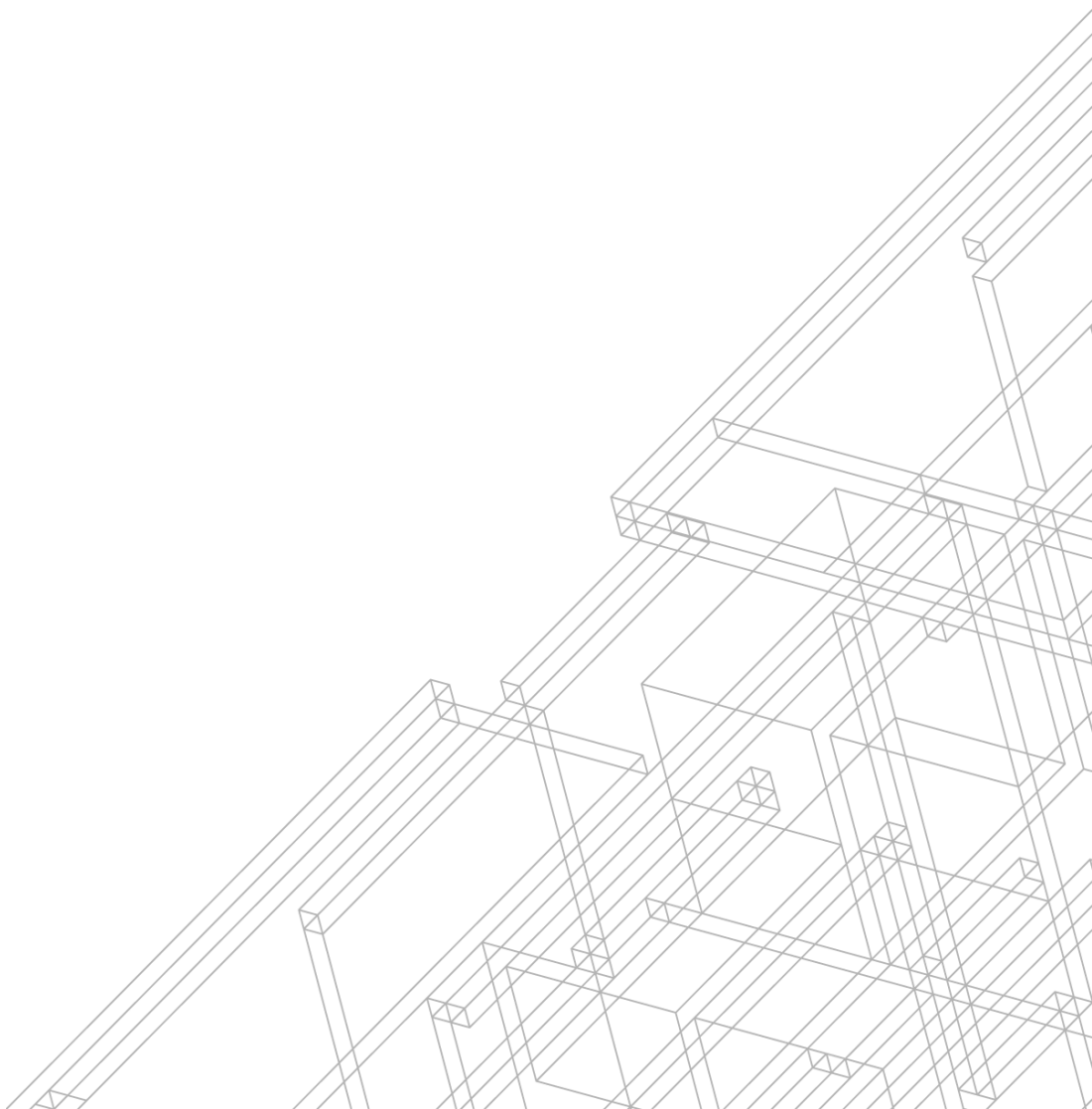
Megaport

Megaport Information Security

Business Continuity Strategy



1 BUSINESS CONTINUITY PLAN

Business Continuity (BC) is the process of ensuring that critical business processes are supported and persist during periods of disruption, duress or after sudden adverse changes in operating conditions (e.g., macro-events, large-scale technology failure). Business continuity planning consists of preparation and testing of processes and procedures that provide that support and assurance that operations continue at an accepted level.

Megaport Software-Defined-Networking (SDN) services are continuously monitored and maintained to ensure reliability and performance of services. Megaport network operations perform 24/7 incident and problem management for expedient resolution and disaster recovery.

1.1 BUSINESS CONTINUITY STRATEGY

The Business Continuity strategy at Megaport has two fundamental operating principles:

1. SDN services are designed with continuous availability principles.
2. Corporate resources, capabilities, functions, and IT Assets are geographically diverse.

The nature of our business operations, as well as this distributed strategy, insulates Megaport from risks associated with traditional business operations including macro-events and technology failure.

SDN operational processes and supporting infrastructure are designed according to the following principles:

1. Operate network infrastructure within hardened physical premises of reliable data-centre operators.
2. Our network is designed with industry-accepted principles for redundancy, such as diverse egress and path.
3. Our technology stack is designed with resiliency, high availability, and recovery at all layers, and is managed through continuous integration and deployment (CI/CD) to mitigate the risk from making large changes.
4. Continually monitor and maintain sufficient availability and capacity.
5. Leverage virtual infrastructure practices and automate components of administration, maintenance and recovery.
6. Configuration deployment mechanisms support automation, scaling, and remote management.

Corporate back-office processes and supporting infrastructure will be designed to:

1. Enable mobile staff to safely operate from any internet connection.
2. Minimize reliance on systems or resources residing in Megaport managed facilities.
3. Facilitate reliable communications, information exchange and collaboration systems.

Each department within Megaport has developed specific Business Continuity Procedures (BCP) for all critical services and processes in order to support the business beyond business-as-usual break/fix conditions. These BCP are tested and validated annually.

1.2 INFORMATION SECURITY REQUIREMENTS

Information Security requirements of IT assets are not forfeited or suspended during BC events. Each BCP complies with all Information Security Program policies and standards, including:

1. Alternative processes, procedures and technologies are required to adhere to Information Security Policy requirements of original processes or technology.
2. Comparable controls are assured during an event and will not invoke design or use of assets that introduces further risk to Megaport or expose assets in a manner that compromises the security of information and technology assets.