

Business Continuity Statement

Barracuda Networks, Inc. (“Barracuda”) maintains an up-to-date Business Continuity Plan (“BCP”) that includes a crisis management plan (including how to handle security incidents), a comprehensive crisis communications plan, and a disaster recovery plan in case Barracuda’s IT resources become compromised and how those IT resources will recover. The BCP is included in the documentation that we make available to the independent third party auditors to obtain various certifications and attestations. Consistent with security industry best practices, Barracuda does not provide its BCP documentation to customers or partners. Instead, we created this Business Continuity Statement to provide customers and partners with information on how Barracuda plans to restore business functionality after a major disruption of operations.

Continuity Focus

Barracuda’s focus is to continually strengthen our resiliency to provide our global business partners and customers with consistent and reliable services. With these processes, our partners and customers can count on us during a critical event to continue providing services with minimal disruptions. Barracuda understands that security and data protection services must work exceptionally well. Our customers need connectivity and must have their systems stay secure. Barracuda has implemented controls to resume our operations in the event of a catastrophic event affecting Barracuda with the target of minimal downtime and maximum efficiency to minimize impact on our customers. Each of our functional areas is ready to meet the challenges of disruption by having evaluated, mitigated, and planned their specific responses to a variety of possible scenarios.

Crisis Management Team

A Crisis Management Team (“CMT”) will be quickly convened when necessary and is led by the Chief Legal Officer and the Chief Information Security Officer. Members of the CMT generally include the heads of IT, Security, Human Resources, Finance, Legal, Marketing, Sales, Engineering, and Technical Support working in conjunction with applicable local site leadership. The CMT is responsible for collecting, evaluating, disseminating, and monitoring incident information and addressing issues requiring resolution. The CMT also tracks the current and potential implications of the incident and the status of resources assigned to the incident. The CMT will conduct meetings as required while the catastrophic situation is ongoing to discuss the issues, statuses, actions, and communications. This includes discussing, determining, and coordinating the recovery of functions and facilities, personnel,

local and remote data processing, voice and data communications, and functionality of the organization and its products. Barracuda will also assess whether it must report the incident to applicable regulatory authorities and will do so in compliance with applicable law. The CMT will distribute crucial information to Barracuda's employees and other stakeholders and provide key support and assistance in responding to and recovering from the critical event.

Personal Safety

Barracuda maintains emergency contact information for its employees. Barracuda employees have designated their emergency contacts and can electronically update their contacts as needed.

Vital Data and Records

Barracuda's data and records are critical to its business. As such, we have data backup and retention capabilities to minimize data loss. Barracuda utilizes tools and software to frequently backup the company's business information, including the SaaS applications upon which it relies, for data recovery purposes. The departments that comprise Barracuda's business operations each have department-specific business continuity plans for their operations so that each function can recover from a crisis in an organized way.

Remote Work

If a major event causes an inability to access facilities for a short or extended period, Barracuda has the technological capability for its employees to go remote and to continue to provide necessary services to customers. Additionally, Barracuda's indispensable business applications are remotely accessible. Barracuda has implemented the necessary infrastructure in its network to have the capability of handling the volume of traffic if most Barracuda employees work remotely. Barracuda can implement remote work at any facility swiftly and for extended periods of time, if needed.

Communication and Collaboration Tools

If there is a major disruption of operations, communication channels may be impacted or degraded. At Barracuda, we have established highly resilient, multiple alternative communication channels that help us coordinate when the normal channels are not available. These communication channels enable us to continue to coordinate internally and with our partners and vendors to keep providing our customers with the support they need.

Barracuda Multi-Mode Communications

Barracuda recognizes that its products are used by customers in crucial environments. As such, we have implemented a global model relating to the deployment and use of our products. Our worldwide organization has a geo-diverse workforce that is readily available for our customers even if there is a disruptive event in a single region. Barracuda technical support uses a follow-the-sun model with support technicians in every region of the world. Through use of cloud-based calling, the company technical support resources can be available and route customer calls to an alternate location as needed to ensure seamless support.

Supply Chain

Barracuda's manufacturing and supply chain produces its hardware products. Barracuda maintains a reserve inventory, which we may access if there is an issue with our supply chain. Barracuda maintains components and pre-built hardware inventory that we may readily ship out to our customers promptly even during any disruption of our operations. Manufacturing operations currently exist in the US and the UK.