

OVERVIEW

EQUINIX BUSINESS CONTINUITY PROGRAM

At Equinix, we take all precautions possible to detect and respond to incidents before they develop into unplanned interruptions. Our Business Continuity Program is one component of our overall operational strategy and process. Additional components include the robust design and construction of our International Business Exchange™ (IBX®) data center locations, our Standard Operating Procedures (SOPs), and expert staff trained to respond to a variety of events. In addition, Equinix employs third-party experts to provide support as needed.

The Equinix Business Continuity Program follows an industry best practice model for governance, documentation and exercises. The program is sponsored by the Chief Operating Officer, and is governed by the Business Continuity Program Executive Steering Committee, consisting of Equinix executives and subject matter experts who meet at least once per calendar quarter. The Executive Steering Committee maintains visibility into the inner workings of the Business Continuity Program, receives regular updates/reports regarding program progress and testing results, and provides program direction and support. In addition, the Business Continuity Program is a regular subject of discussion with our Governance Committee, a subset of the Board of Directors.

Emergency Response

Life safety is an absolute priority. Appropriate plans are in place for each IBX location to ensure that physical threats are addressed as quickly as possible, and customers, staff and other on-site personnel are protected from unsafe conditions. Equinix is responsible for handling emergency response for office sites solely occupied by the Company. This responsibility is assumed by the landlord's building management where Equinix occupies space in a multi-tenant office building. All IBX data centers follow SOPs (e.g., engineering, emergency, security, site operations, etc.) which detail the immediate responses to be taken by employees when an incident occurs. These procedures are designed to prevent or minimize physical injury and to ensure the integrity of the facilities and property.

Evacuation tests are conducted annually to ensure staff compliance and familiarity with documented procedures. Equinix facilities comply with all country, local and municipality codes, regulations and requirements, including occupational safety and health standards.

Crisis Management

Equinix has a strong crisis management capability in place with representation from senior leaders across the organization globally. The program includes regional crisis management teams and plans with oversight from a global/executive team with its own tailored plan. Each plan documents the procedures for identifying, assessing and escalating the severity of events, and contains position

descriptions along with operational checklists for team members. Communication processes and protocols ensure that customers receive clear and timely updates in addition to the standard Incident Communications process. Crisis management exercises for each team are conducted at least twice per year to ensure that we stress-test our processes and procedures.

Business Recovery – Key Locations

Business recovery plans have been developed for key locations, including headquarters offices. A business impact analysis is used in the planning stage to gather data, identify business process recovery priorities and document systems, applications and maximum allowable downtime. Plan owners and plan builders assist the Business Continuity Program Office in developing and maintaining plans that contain the detailed information necessary to execute department business process recovery strategies. They include a description of the strategy the business function will employ, as well as the resources and procedures to recover business processes within their recovery time objectives (as documented in the business impact analysis). Business recovery plans take into account the critical number of staff required to perform key business functions and are tested annually. Business recovery plans take into account the critical number of staff required to perform key business functions and a detailed Threat and Risk Assessment. These plans are reviewed and tested annually.

Business Recovery – IBX Data Centers

IBX data centers are designed to ensure the highest levels of availability. This includes infrastructure systems, such as physical security, fire detection and suppression, uninterruptible power systems, emergency generators and structural reinforcement of the building. IBX data center operational capability is supported by experienced staff who have completed training and follow well-defined processes and procedures, and engage in good housekeeping practices. IBX data centers are monitored 24 hours a day, 365 days a year to ensure we can respond immediately to incidents affecting IBX data center operations. The Equinix site selection process is directed by regional real estate teams with a cross-functional membership including legal, design, engineering, construction and operations.



OVERVIEW

EQUINIX BUSINESS CONTINUITY PROGRAM



We assess physical and environmental risks including seismic, flood, airplane flight path, proximity to active rail and roads, proximity to hazardous waste, fuel tanks, asbestos, etc. In addition, we review active business uses of adjacent properties. IBX data center employees are trained to respond and secure the IBX data center and its contents and address incidents to support ongoing business operations. Equinix maintains comprehensive internal SOPs, health and safety procedures, and business continuity-related processes and documentation to ensure rapid response to IBX data center emergencies. These procedures include:

- Evacuation procedures.
- Incident management and reporting procedures.
- Emergency communications procedures, involving all levels of company management.
- Post-incident review, root cause analysis and resolution tracking.
- Procedures for handling all applicable threats for the IBX data center location.

A threat and risk assessment is performed for each operational IBX data center and is reviewed annually for material changes that directly or indirectly impact the services provided. The threat and risk assessment identifies threats and risks to a facility within the following categories:

- **Natural hazards** – earthquake, flood, hurricane/typhoon, tsunami, severe heat/cold.
- **Man-made** – bomb threat, proximity to airports/railroads/freeways.
- **Site infrastructure** – electrical failure, generator failure, fuel shortage, HVAC outage.
- **Health threats** – injuries, communicable diseases, pandemic.
- **Economic/political threats** – civil unrest, labor disputes.
- **Application outage** – locally hosted applications.

Each risk is evaluated for likelihood and impact to people, property and business and assigned an inherent risk score. Existing management and mitigation measures are considered when developing a residual risk score. The residual risk score is used to evaluate additional mitigation measures in order to achieve incremental potential improvement.

IBX data center business recovery plans are developed based on the results of the business impact analysis, which identifies the business processes executed within an IBX data center, the impacts of an interruption and the maximum time in which a given process would need to be restored (assuming a worst-case scenario).

The results of the business impact analysis are reviewed and validated by management and used as the baseline for developing IBX data center business recovery plans. These plans include site information, descriptions of each business process, recovery priorities, resource requirements, manual workarounds if a system or application is unavailable, vital records, key vendors, etc. Training on these plans is conducted annually.

Equinix conducts a variety of tests to ensure continuity of critical business processes. Testing at Equinix IBX data centers includes, but is not limited to, physical security; scheduled preventative maintenance tests on critical infrastructure to ensure proper fail-over to back-up systems; dynamic monitoring of critical infrastructure for proper performance; scenario-based tests for staff; and evacuation drills. All tests are followed up with a post-test analysis and extensive reviews, which are communicated to management.

Disaster Recovery – Systems & Applications

IT disaster recovery has been designed to address the recovery of Equinix's technology assets. Backup/failover capabilities of Equinix's internal processes exist between our own data centers. All critical systems rely on backup data as part of the disaster recovery plan. Backup frequency varies by application but is no less than daily for all applications. The type of backup differs based on application, database, program, system and network data. Backup data is stored at the disaster recovery site. The disaster recovery plan comprises multiple "Run Books" that address the detailed technical steps necessary to relocate (if necessary) and restore Equinix systems and applications that have been disrupted. The time frames for recovering systems and applications are driven by the business process recovery time objectives articulated in the business impact analysis, from both the headquarters and IBX data center perspectives. Disaster recovery is integral to business operations; as new applications are brought online, new Run Books are developed and tested. Up and downstream RTOs and RPOs are captured and tested for critical processes, vendors and systems.

Communication

Most importantly, if the unexpected does happen, Equinix keeps its customers informed of the occurrence of the incidents as well as the impact and steps taken to resolve them. We always provide notifications to customers for customer-impacting incidents. Timely notifications are provided throughout the incident life cycle and include details on the nature of the incident and steps taken to resolution. Escalation procedures and time frames are defined and are part of our operating procedures checklist. Customers may opt in to our automatic email alerts to receive notification of any incident that may impact service availability in an IBX data center.

For more information on our Business Continuity Program, please contact your Customer Success Manager.