Business Continuity Management

Definitions

"Business Continuity Management" or "BCM" means the holistic management of the process of identifying the organization's business critical functions, evaluating risks and their impacts, and developing plans that enable organizational resiliency in the midst of Incidents.

"Disaster Recovery" or "DR" means the process, policies and procedures that are related to preparing for recovery or continuation of technology infrastructure which are vital to an organization when impacted by an Incident. DR focuses on the IT or technology systems that support business functions, as opposed to Business Continuity, which involves planning for keeping all aspects of the business (e.g. operations, facilities, personnel, equipment, infrastructure, applications, etc.) functioning in the midst of an Incident.

"Incident" is a situation that is, or could lead to, a disruption, loss, emergency or crisis. An Incident could materially impair or halt operations of the Supplier.

Business Continuity Management Standard

CenturyLink requires its suppliers (each a "Supplier") to comply with, at a minimum, the Business Continuity Management standards listed in Subsections a-k below ("BCM Standard") to ensure Suppliers are able to continue to support CenturyLink when CenturyLink or the Supplier experiences an Incident. Supplier shall comply with this BCM Standard and must maintain a Business Continuity Management plan ("BCM Plan") that outlines the Supplier's processes for ensuring continuity of Supplier's business in the event of an actual or threatened Incident during the period of time Supplier is providing products or services to CenturyLink. Supplier's BCM Plan may include a Disaster Recovery plan and an Incident management plan. Upon CenturyLink's request, Supplier must provide CenturyLink with a copy of its BCM Plan or meet with a CenturyLink BCM representative at a convenient time to review Supplier's BCM Plan and any exercise or test results.

a) Supplier must conduct a business impact analysis and risk assessment to sequence its recovery and mitigate the impacts of potential threats and hazards.
b) Supplier must implement strategies to protect and fortify environments, facilities, networks, systems/applications and Supplier's people.
c) Supplier must back up its data and systems/applications to an alternate location that is in a different geographic location dispersed from the primary location and routinely test the backups to confirm viability.
d) Supplier's BCM Plan must include defined roles and responsibilities, activation triggers, a communication plan, recovery solutions and a sequence for recovering all of Supplier's functions, facilities, networks, environments and systems/applications that are utilized to provide products and services to CenturyLink.
e) Supplier must review and update its BCM Plan whenever there are operational changes, but not less than once each calendar year.
f) Supplier must test/exercise its BCM Plan at least once each calendar year and share those results with CenturyLink during audit assessments.
g) Supplier must maintain and exercise its Incident management structure to ensure timely recovery from Incidents and provide prompt notifications to CenturyLink when the provisioning of the products and services could be interrupted.
h) Supplier must manage the resiliency of its third-party vendors and subcontractors to ensure they can continue to support Supplier when Supplier or its third-party vendors and subcontractors experience operational disruptions.
i) Supplier must immediately notify CenturyLink when any actual or anticipated Incident could cause a disruption in the delivery of its products or services to CenturyLink. Notifications should be sent to Supplier's CenturyLink point of contact.
j) Supplier will take the appropriate steps to immediately address any such Incident and will provide CenturyLink with a report stating the reason for the outage/disruption and indicate the measures being taken to prevent a reoccurrence.
k) Supplier must not make or permit any statements to be made concerning any Incident that expressly mention CenturyLink to any third-party without the written authorization of CenturyLink.