**Backup Policy**

**Nexelus**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Purpose**

To protect the confidentiality, integrity, and availability of data, both for Nexelus and Nexelus’s customers, complete backups are performed **<BACKUP FREQUENCY>** to assure that data remains available when it’s needed and in the case of a disaster.

**Policy**

Nexelus policy requires that:

* Data should be classified at time of creation or acquisition according to the Data Classification Policy
* An up-to-date inventory and data flow map of all critical data are maintained.
* All business data should be stored or replicated into a company controlled repository, including data on end-user computing systems.
* Data must be backed up according to its level defined in Data Classification Policy.
* Data retention period must be defined and comply with any and all applicable regulatory and contractual requirements. More specifically,
  + Data and records belonging to Nexelus customers must be retained per Nexelus product terms and conditions and/or specific contractual agreements.
  + By default, all security documentation and audit trails are kept for a minimum of seven years, unless otherwise specified by Nexelus’s Data Classification Policy, specific regulations, or contractual agreement.

**Backup and Recovery**

***Customer Data***

Nexelus stores customer data in a secure production account in **<YOUR CLOUD PROVIDER>**, using a combination of **<DATABASE TYPES>** databases. By default, **<CLOUD STORAGE>** provides durable infrastructure to store important data and is designed for durability of 99.999999999% of objects.

Nexelus performs automatic backups of all customer and system data to protect against catastrophic loss due to unforeseen events that impact the entire system. An automated process will back up all data to a separate region in the same country (e.g. US East to US West). By default, data will be backed up **<FREQUENCY>**. The backups are encrypted in the same way as live production data. Backups are monitored and alerted by **<MONITORING SYSTEM>**. Backup failures trigger an incident by alerting the Security Officer.

***Source Code***

Nexelus stores its source code in git repositories hosted by **<VERSION CONTROL>**. Source code repositories are backed up to Nexelus’s **<CLOUD PROVIDER>** account on a **<FREQUENCY>** basis. In the event that **<VERSION CONTROL>** suffers a catastrophic loss of data, source code will be restored from the backups in **<CLOUD PROVIDER>**.