# Security & Data Privacy Policy

The following physical security controls apply to Customer Equipment and Customer Content residing in a Data Center in connection with the provision of Services to Customer.

**1. Physical Security - Data Centers**.

**1.1. Dedicated Resources**. Servers and devices dedicated to Customer's use will be located in a controlled access Data Center (or portion thereof) either operated by or dedicated to use by LighEdge or its Affiliates.

**1.2. Monitoring Access/ Activities**. The Data Center will be monitored by CCTV camera surveillance with video retention as per organization policy. Video Surveillance shall cover at least all building perimeter entrances and exits. LightEdge limits access to the Data Center to authorized individuals. Access is granted through electronic access badge, biometric data or other approved security authentication method. Access to the Data Center will be electronically logged with retention as per organization policy. The Data Center has single Customer entry point into the facility.

**1.3. Operation Areas**. Building operations areas (i.e. AHU/HVAC rooms, UPS/Battery rooms, Electrical rooms) are secured and only accessed by LightEdge personnel and approved contractors with a business need.

**1.4. Fire Protection**. The Data Center has an appropriate fire alarm, fire suppression and emergency notification systems for the facility and specific interior areas. Such systems meet the requirements set for by the National Fire Protection Association (NFPA).

**1.5. Sanitization**. Following the expiration or termination of the Agreement, LightEdge will wipe data from those hard drives and storage devices dedicated to Customer use in accordance with NIST media sanitization standards prior to re-use.

**2. Security Controls Audits & Reporting**. LightEdge retains qualified third-party auditors to validate and certify the control of environment for the Services in accordance with industry standards. The following compliance reports or certifications are available to the Customer through the Service Portal: HIPAA; HITRUST; LightEdge's latest Payment Card Industry (PCI) compliance report; Statement on Standards for Attestation Engagements (SSAE) No. 18 audit report; SOC 1, 2, and 3 Type II; reports relating to its ISO/IEC 20000 & 27001 certification; and NIST 800-53. The Customer will treat such audit reports as LightEdge's Confidential Information under the Agreement.

**3. Administrative Controls**.

**3.1. Background checks**. To the extent permitted by law, LightEdge will perform pre-employment background checks of its employees who perform the Services and is committed to supervision and continued training.

**3.2. LightEdge Access**. LightEdge will restrict the use of administrative access codes for Customer's account to its employees and other agents who need the access codes for the purpose of providing the Services.

**3.3. Customer Access**. As the primary system administrator, Customer is responsible for the management of their account, including creation, change management, and termination, and enforcement of related remote working and password controls. Customer remains the primary system/account administrator and is responsible for the integrity, security, maintenance and appropriate protection of Customer Content by: (i) selecting and purchasing appropriate security Services; (ii) implementing appropriate encryption and logical access controls; and (iii) maintaining appropriate application security controls.

**3.4. Encryption**. Encryption of data stored within the Customer Content may be employed at the discretion of Customer, by electing to purchase or use capabilities provided by LightEdge or otherwise obtained by Customer from third parties.

**4. Addendums**. Customer and LightEdge will comply with applicable laws in relation to their collection and processing of any personal data (including sensitive data) in the provision and use of the Services:

**4.1. DPA**: If and to the extent the provision of Services by LightEdge to Customer involves the processing (or similar term under the applicable law) of personally identifiable information (or similar term under the applicable law), then the Data Processing Addendum available at: https://go.lightedge.com/dpa shall be incorporated into and made part of the Agreement.

**4.2. CCPA**: If and to the extent the California Consumer Privacy Act of 2018 (CCPA) (Cal. Civ. Code §§ 1798.100 to 1798.199; Cal. Code Regs. tit. 11, §§ 999.300 to 999.337) applies to the processing of Personal Information (as defined in the CCPA), then the CCPA Addendum available at: https://go.lightedge.com/ccpa-addendum shall be incorporated into and made part of the Agreement.

**4.3. BAA**: If Customer is subject to the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), as a Covered Entity or Business Associate (as defined in HIPAA) and use the Services in a manner that causes LightEdge to create, receive, maintain, or transmit Protected Health Information on its behalf, then the Business Associate Agreement available at: https://go.lightedge.com/baa shall be incorporated into and made part of the Agreement.