LIGHTEDGE SOLUTIONS DATA CENTER PHYSICAL ACCESS POLICY

The following data center physical access policy ("Access Policy") regulates access to and activities within any of the LightEdge Solutions Data Center (each, a "Data Center"). LightEdge reserves the right to update or amend the Access Policy, as necessary. Any update or amendment of the Access Policy shall be provided to Customer via the Service Portal.

1. LightEdge's and Customer's Responsibilities.

LightEdge is responsible for ensuring that all resources under its control remain physically secure. LightEdge maintains this Access Policy to provide a framework for Customers to follow for physical security and access to LightEdge Data Center and to instruct Customers on the procedures and policies that LightEdge staff and employees follow.

2. Data Center Access List.

Customer's Authorized Contact shall provide LightEdge with a list ("Access List") of individuals to be granted access to the Data Center ("Authorized Personnel"). Customer will be required to review and update the Access List on a bi-annual basis. Customer is responsible for maintaining and updating its access list. Each Authorized Personnel is required to approve the Access Policy (Exhibit I).

3. Restrictions.

Access into the Data Center requires adherence to the following protocols and restrictions on dangerous materials:

- No smoking or chewing tobacco is allowed.
- No combustible materials may be brought into the data center, including lighters, hand-warmers, mace, tear gas, aerosol cans, or compressed air.
- No eating or drinking is allowed in the data center.
- No drugs or alcohol are permitted in the data center.
- No weapons or firearms are allowed in the data center.
- No external fire suppression devices are allowed.
- Only hardware that will fit in approved racks are allowed in the data center spaces.
- All work-related materials must be cleaned up before leaving.
- All work-related trash or garbage must be disposed of properly.
- No illegal activity of any kind is permitted.
- No cardboard boxes, paper of combustible material may be stored in the data center areas.

4. Access Keycards and Identification.

LightEdge will issue identification badges and access keycards to Authorized Personnel. At no time shall any transfer of identification badges or access keycards occur between an Authorized Personnel and/ or any other employee, agent or third party without pre-approved, written permission from LightEdge. If at any time LightEdge becomes aware that an access badge or access keycard has been transferred in violation of this policy, immediate revocation of access to the Data Center may occur.

5. Physical Access Procedures.

5.1. Physical Access Procedures: Authorized Personnel.

Access to the Data Center is gained through the main lobby entrance. All Authorized Personnel must identify themselves before LightEdge grants them access into the facility. Once access is granted, Authorized Personnel will activate their badge and LightEdge will scan and record a digital image of their biometric data (which may include face, including facial geometry, or may include palm and/or one or more fingerprints) each time Authorized Personnel enter our data center. These images will be solely used for security purposes, in order to ensure that only authorized individuals gain access to our facility. You hereby indicate that you understand and agree to our scanning and recordation of the designated biometric data for security purpose. All badges are activated for an eight (8) hour period.

5.2. Physical Access and Procedures: Visitors.

Customers may grant temporary access to employees, vendors or agents not identified on the Access List ("Visitors") via the Service Portal. All Visitors shall enter the Data Center through the Data Center Vestibule and must sign into the "visitor registration terminal". All Visitors are escorted at all times within the secured area of the Data Center.

Authorized Personnel may allow Visitors to gain access to the Data Center, subject to the Authorized Personnel access level, provided that:

1. A Data Center employee or staff member must accompany Visitors at all times while within the Data Center.
2. All Visitors must sign in and sign out when entering or exiting the Data Center. Visitors must wear the identification badge at all times.
3. Any exceptions to any of the above policies must have been approved in writing by LightEdge.

5.3. Emergency Access by Visitors.

Emergency access by Visitors to the Data Center may be requested by Customer. In this case, LightEdge shall obtain oral confirmation by Authorized Contact via phone. Access to the Data Center under this condition shall be noted as an "emergency access" in the Data Center security logs. Any inappropriate use of "emergency access" may result in access being immediately denied and the Visitor being ejected from the Data Center and/or Customer's "emergency access" privileges revoked.

5.4. Visitor Policy

Each Visitor is required to electronically agree to the Visitor Access Policy before accessing the Data Center (Exhibit II).

6. Disclosure of Security, Access, or other Policies Governing the Security of the Data Center.

All persons entering the Data Center, whether Authorized Personnel or Visitors agree to hold all information related to the security, operation, policies or procedures relating to the Data Center in the strictest of confidence and to take the same degree of care to protect such information as they do with their own proprietary information. No less than reasonable care shall be maintained by Authorized Personnel or Visitors.

Customer and Authorized Personnel agree not to disclose any information pertaining to the security of the Data Center to a third party for a purpose other than use of the Services.

7. Data Center Access Levels.

For our customers' convenience, LightEdge maintains several levels of access to the Data Center.

Access levels include:

7.1. Unrestricted Access to All Contracted Space(s)

Access to all area of Data Center is limited to LightEdge Data Center operations staff.

7.2. Restricted Access to Specific Contracted Space(s)

Customers in this category will have access to the area of the Data Center containing their equipment provided they have purchased at least one full rack worth of space. Customers will have access to common area (restrooms, break room).

7.3. Escorted Access to Contracted Space(s)

Customers purchasing shared collocation services will only have unrestricted access to common areas. Access to Data Center areas will require an escort by a LightEdge Staff Member at all times.

7.4. Workstation Recovery Space

Customers purchasing workstation recovery services will only have unrestricted access to common areas and the workstation recovery room. Access to Data Center areas will require an escort by a LightEdge staff member at all times.

The level of access shall be determined and maintained by LightEdge and Customer according to the terms and conditions of the agreement between LightEdge and Customer.

8. Data Center System and Network Security.

Customer, Authorized Personnel and/ or Visitors shall not allow unauthorized access to the Data Center; unauthorized use of any of LightEdge's product or services; unauthorized use of any equipment, hardware, connections or other materials that Customer does not have permission to use; disruption or interference with the connectivity and access or otherwise impeding other customers' use of the LightEdge Data Center, products.

9. Consequences of Violation.

If LightEdge becomes aware of an alleged violation of any of the terms of the Access Policy, LightEdge shall initiate an investigation. During the investigation, LightEdge may restrict Customer's access to the Data Center or other LightEdge products and services to prevent further possible unauthorized activity.
Failure to adhere to the Access Policy may result in the expulsion of Authorized Personnel and/ or Visitors from the Data Center and could result in the termination for cause of the agreement between Customer and LightEdge. Appropriate response to violations of these rules shall be solely within the discretion of LightEdge.

Exhibit I
Acknowledgement

Failure to knowingly comply with the Access Policy is ground for immediate removal from the Data Center.

I have been given a copy of the LightEdge Access Policy and acknowledge their receipt. I have had an opportunity to review and ask questions about these procedures and policies. I agree to follow these procedures and policies to the best of my abilities.

Company: _____

Name (print): _____

Signature: _____

Date: _____

Exhibit II
LightEdge Solutions Visitor Policy

All visitors to LightEdge Solutions offices and data centers are subject to the LightEdge Solutions Visitor Policy. By signing the signature pad or visitor log, you agree to abide by this policy.

Visitor Access
Visitors are considered anyone who is not an employee, authorized client, or authorized vendor. Visitors do not have authorization to visit any areas beyond the main lobby without an authorized escort. Visitors are subject to the following:
• Providing a government issued ID
• Signing the signature pad or visitor log, and therefore agreeing to this policy
• Wearing a LightEdge Solutions visitor badge in plain sight while on LightEdge Solutions property
• Turning in the LightEdge Solutions visitor badge upon departure from the facility

Recording Devices
LightEdge Solutions prohibits the use of electronic recording devices in secure areas. Examples of prohibited devices includes the following:
• Cameras, including cell phone cameras
• Tape recorders
• MP3/Digital recorders

Removable Media
LightEdge Solutions prohibits the connection of removable media to any network, system, or asset. Removable media includes, but is not limited to the following:
• Flash memory devices (USB thumb drives)
• CD/DVD media
• Hard disks
• Laptops and Tablets
Restrictions

LightEdge Solutions prohibits the following activities:
• No smoking (including vaporizers) or chewing tobacco is allowed inside the building, smoking is restricted to designated areas outside the building
• No food or drinks are allowed in the data center
• No drugs or alcohol are permitted in the data center
• No weapons, explosives, or firearms are allowed
• No illegal activity of any kind is permitted
• Access controlled and fire rated data center doors must not be propped open
• No trash or debris may be left on the data center floor at ANY time

LightEdge Solutions requires its visitors to:
• Report any leaks, spills, or any other abnormal condition to LightEdge staff immediately
• Report all accidents or injuries to LightEdge staff immediately

Privacy and Confidential Information
LightEdge Solutions is a managed service provider and may store personal information and/or confidential information. LightEdge Solutions prohibits visitors from obtaining, copying, or disclosing personal information and confidential information. As a visitor, you agree to protect any personal information and confidential information and may be required to agree to a LightEdge Solutions Non-Disclosure Agreement (NDA).