1.0 PURPOSE AND SCOPE

This policy describes how the organization protects its systems, buildings, and related supporting infrastructure against threats associated with the physical environment. This includes the physical office space, and any static and portable systems that may contain sensitive data. The organization's information systems are protected from threats such as flooding, burglary, civil unrest, and fires. Supporting systems include electrical power, cooling, and personnel responsible for maintaining systems.

2.0 POLICY

- Physical access to the organization's physical office is restricted to only authorized personnel. An electronic key card is required to gain access to the office space.
- Building access systems are maintained by building security personnel, including the maintenance of access logs and the maintenance of physical access devices such as locks and card readers.
- Office access is maintained by the organization and is secured by doors that lock automatically and can only be opened by numeric keypads
- Visitors to the office are escorted by an authorized employee.
- The organization's data-containing systems are hosted by Microsoft and protected by Microsoft's robust physical security controls.

3.0 RELEVANT NIST CONTROLS

Control	Control Description	Document Section
NIST 800-171 3.10	Physical Protection	Entire Document

4.0 REVISION HISTORY

Date	Name	Changes Made	Revision #
12/25/2022	Frank Schipani	Initial draft created	0.9
10/9/2023	Frank Schipani	Annual review	0.9
12/30/2023	Audit Committee	Approved Policies	