# Datacenter Policy

BritePool

January 2020

## Contents



Table 1: Control satisfaction

| Standard | Controls Satisfied |
|---|---|
| TSC | CC6.4 |

Table 2: Document history

| Date | Comment |
|---|---|
| Jan 2 2020 | Initial document |

# 1 Purpose and Scope

a. The purpose of this policy is to define security procedures within the organization's data centers and secure equipment areas.

b. This policy applies to any cloud hosted providers and facilities within the organization that are labeled as either a data center or a secure equipment area. Such facilities are explicitly called out within this document.

c. This policy applies to all management, employees and suppliers that conduct business operations within cloud host or data centers and secure equipment areas.

# 2 Background

a. This policy defines the policies and rules governing data centers and secure equipment areas from both a physical and logical security perspective. The document lists all data centers and secure equipment areas in use by the organization, prescribes how access is controlled and enforced, and establishes procedures for any visitor or third party access. This policy also defines prohibited activities and requirements for periodic safety and security checks.

# 3 Policy

a. The following locations are classified by the organization as secure areas and are governed by this policy:

    i. At this time all data centers are hosted by cloud provider(s) (Amazon) with strict data center and secure area access policies. The company currently maintains no physical data centers under its control.

b. Each data center and secure area must have a manager assigned. The manager's name must be documented in the organization's records. In the case of any on-prem data centers, the manager's name must also be posted in and near the secure area.

c. Each secure area must be clearly marked. Access to the secure area must be controlled by at least a locked door. A visitor access log must be clearly marked and easily accessible just inside the door.

d. Persons who are not employed by the organization are considered to be visitors. Visitors accessing secure areas shall:

    i. Obtain access to secure areas in accordance with reference a.

   ii. Only enter and remain in secure areas when escorted by a designated employee. The employee must stay with the visitor during their entire stay inside the secure area.

   iii. Log the precise time of entry and exit in the visitor access log.

e. The following activities are prohibited inside secure areas:

   i. Photography, or video or audio recordings of any kind.

   ii. Connection of any electrical device to a power supply, unless specifically authorized by the responsible person.

   iii. Unauthorized usage of or tampering with any installed equipment.

   iv. Connection of any device to the network, unless specifically authorized by the responsible person.

   v. Storage or archival of large amounts of paper materials.

   vi. Storage of flammable materials or equipment.

   vii. Use of portable heating devices.

   viii. Smoking, eating, or drinking.

f. Secure areas must be checked for compliance with security and safety requirements on at least a quarterly basis.