Workstation Policy

BritePool

January 2020

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.8

Table 2: Document history

Date	Comment
Jan 2 2020	Initial document

1 Purpose and Scope

a. This policy defines best practices to reduce the risk of data loss/exposure through workstations.

b. This policy applies to all employees and contractors. Workstation is defined as the collection of all company-owned and personal devices containing company, client, partner, or user data.

2 Policy

a. Workstation devices must meet the following criteria:

   i. Operating system must be no more than one generation older than current

   ii. Device must be encrypted at rest

   iii. Device must be locked when not in use or when employee leaves the workstation

   iv. Device must be used for authorized business purposes only

   v. Loss or destruction of devices should be reported immediately

   vi. Laptops and desktop devices should run the latest version of antivirus software that has been approved by IT

b. *Desktop & laptop devices*

   i. Employees will be issued a desktop, laptop, or both by the company, based on their job duties. Contractors will provide their own laptops.

   ii. Desktops and laptops must operate on macOS or Windows.

c. *Mobile devices*

   i. Mobile devices must be operated as defined in the Removable Media Policy, Cloud Storage, and Bring Your Own Device Policy.

   ii. Mobile devices must operate on iOS or Android.

   iii. Company data may only be accessed on mobile devices with Slack and Gmail.

d. *Removable media*

   i. Removable media must be operated as defined in the Removable Media Policy, Cloud Storage, and Bring Your Own Device Policy.

   ii. Removable media is permitted on approved devices as long as it does not conflict with other policies.