Office Security Policy

Sour Lemon Digital, LLC

May 2023

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.4

Table 2: Document history

Date	Comment
Nov 1, 2022	Initial document

1 Purpose and Scope

a. The policy aims to ensure the confidentiality, integrity, and availability of sensitive information, protect against unauthorized access or disclosure, and maintain a secure work environment for team members. All members of Sour Lemon Digital, LLC and hired contractors are expected to adhere to this policy.

2 Policy

a. *Physical Security*

   i. Home Office Security:

      1. Team members are responsible for maintaining a secure and private home office environment.
      2. Home office access must be restricted to authorized individuals only.
      3. Locking personal workstations or laptops when unattended is mandatory.
      4. eam members should report any theft or loss of equipment immediately to the appropriate authorities and notify the company.

b. *Equipment Security*

   i. The following policies are applied to all company provided equipment:

      1. Company-provided equipment must not be shared with unauthorized individuals.
      2. Team members must ensure the physical security of their company-provided laptops, mobile devices, or any other equipment.
      3. Unauthorized disassembly or modification of company-provided equipment is strictly prohibited.
      4. Lost or stolen access cards/keys/fabs shall be reported immediately

c. *Malware Protection*

   i. The following policies are applied to all company provided equipment:

      1. Team members must keep their software, including operating systems, antivirus, and security patches, up to date.
      2. Only company-approved software and tools should be installed on company-provided equipment.

3. Suspicious emails, attachments, or websites should be reported to the IT department without clicking or downloading any suspicious content.

a. *Secure Network Connections*

   i. Team members must use secure and encrypted network connections (e.g., VPN) when accessing company resources or systems.

   ii. Wi-Fi networks must be secured with strong passwords and encryption.

   iii. Public or untrusted networks should be avoided when accessing company systems or sensitive information.

b. *Enforcement*

   i. Employees, contractors, or third parties found in violation of this policy (whether intentional or accidental) may be subject to disciplinary action, including:

      1. reprimand
      2. loss of access to premises
      3. termination