1.0 PURPOSE

This policy defines how TSC Alliance (the organization) ensures that access controls are implemented and in compliance with IT security policies, standards, and procedures.

2.0 SCOPE

The policy applies to all of the organization's information systems that contain the organization's data, such as computers, servers, cloud and SaaS systems, mobile devices, and systems administered by third parties on the organization's behalf.

This policy defines "potentially sensitive electronic information" as data stored on the organization's information storage platforms that is not public in nature, where access should be restricted only to organization employees or a subset of organization employees.

All accounts that access the organization's information systems must adhere to this and other organizational policies governing technology use, including password rules and the use of multifactor authentication.

3.0 POLICY

3.1 Access Authorization (3.1.1, 3.1.2)

Role-based access is granted during the new user enrollment process. These roles are pre-approved by the Chief Financial Officer or an authorized delegate of the Chief Financial Officer and outlined in the new user procedures. Any access to potentially sensitive information outside of the user enrollment process or for guest, vendor or other non-employee accounts must be authorized by the Chief Financial Officer or an authorized delegate of the Chief Financial Officer.

3.2 Control of Data Flow (3.1.3)

The organization employs firewalls and other systems to restrict the flow of data only as needed by the business. The data flow controls are documented.

3.3 Separation of Duties (3.1.4)

System administration and regular system use should not be done using the same account. In many cases, information system administration and regular non-system administration work is being completed by different people using their own accounts. In cases where a single person is performing both information system administration and normal user activity, these actions must be completed using separate accounts. Routine, everyday user activity must be done using a standard user account. A separate account must be used for system administration where elevated privileges are required.

This separation of duties reduces the organization's exposure due to a compromised account. User accounts have more limited access to data and systems, so a compromised user account is less of a

liability. Accounts with administrative access are used less frequently and thus are less likely to be compromised by cyberattacks that target users.

3.4 Least Privileged Access (3.1.6, 3.1.7)

The organization uses a least privileged access methodology, allowing authorized access for users only to accomplish assigned tasks. Potentially sensitive electronic information is only made accessible to those with a legitimate business need.

Non-privileged user accounts cannot execute non-privileged functions. Privileged functions are audited.

3.5 Unsuccessful Logon Attempts (3.1.8)

Accounts must lock after a pre-defined number of failed logon attempts. Account lockout settings are controlled by Microsoft Office 365's smart lockout function.

3.6 Automatic Logoff or Locking (3.1.10, 3.1.11)

Accounts and systems must be configured to automatically lock after a pre-defined time period. Once locked, systems must require reauthentication to unlock. User sessions should terminate automatically after a pre-defined period of inactivity.

3.7 Remote Access Controls (3.1.12, 3.1.13, 3.1.14)

Remote access uses cryptographic mechanisms to protect the confidentiality of sessions.

Remote access is controlled and protected using firewalls and virtual private networks (VPNs) and remote access data transfer is encrypted. Remote access is centrally administered, monitored and managed. Remote access is only allowed through authorized mechanisms.

3.8 Remote Access to Privileged Actions (3.1.15)

Remote access for privileged functions is limited only to authorized individuals with IT management responsibilities and only for necessary IT management functions.

3.9 Wireless Network Controls (3.1.16, 3.1.17)

Wireless networks are approved by organization management. Users of wireless networks are given guidance on their proper use. Access to organization systems from wireless networks is limited to only what is necessary, and access is centrally controlled and monitored. Data traversing wireless networks is encrypted. Only authorized users may access wireless networks.

3.10 Access by Mobile Devices (3.1.18, 3.1.19)

Mobile devices include smart phones, laptops and tablets. Access to organization systems by mobile devices is allowed and is managed and controlled to allow only necessary access and only through access methods described above, such as VPNs.

The storage systems of mobile devices that access organization systems are encrypted.

3.11 Access to External Systems (3.1.20)

Access to externally hosted systems such as Microsoft Office 365 is controlled using the same methods described above control access to organization-owned resources. Users are instructed in the proper use of external systems and in the use of non-organization-owned computing resources.

3.12 Portable Storage Devices (3.1.21)

The use of portable storage devices is limited only to situations where electronic transfer of data via the organization's secure transmission mechanisms is not possible. All non-public data on portable storage devices must be encrypted.

3.13 Data on Publicly Accessible Systems

The organization's sensitive data must not be posted to or processed on publicly accessible systems.

4.0 RELEVANT NIST CONTROLS

Control	Control Description	Document Section
NIST 800-171 3.1	Access Control	Entire Document

5.0 REVISION HISTORY

Date	Name	Changes Made	Revision #
8/31/2021	Frank Schipani	Initial draft created	0.9
10/9/2023	Frank Schipani	Annual review	0.9
12/30/2023	Audit Committee	Approved Policies	