Administration 6 – ACCESS MANAGEMENT POLICY

1. Policy Statement

1.1. Protecting access to IT systems and applications is critical to maintain the integrity of the Shire of Christmas Island's (SOCI) technology and data and prevent unauthorised access to such resources.

1.2. Access to SOCI's systems must be restricted to only authorized users or processes, based on the principle of strict need to know and least privilege.

2. Background

2.1. Access controls are necessary to ensure only authorized users can obtain access to SOCI's information and systems.

2.2 Access controls manage the admittance of users to system and network resources by granting users access only to the specific resources they require to complete their job related duties.

The preparation of a financial report in conformity with Australian Accounting Standards requires management to make judgements, estimates and assumptions that effect the application of policies and reported amounts of assets and liabilities, income and expenses.

The estimates and associated assumptions are based on historical experience and various other factors that are believed to be reasonable under the circumstances; the results of which form the basis of making the judgements about carrying values of assets and liabilities that are not readily apparent from other sources. Actual results may differ from these estimates.

3. Policy Objective

3.1. The objective of this policy is to ensure SOCI has adequate controls to restrict access to systems and data.

4. Scope

4.1. This policy applies to:

4.1.1. All SOCI workplaces.

4.1.2. All employees, consultants, contractors, agents and authorized users accessing SOCI systems and applications.

5. Definitions

5.1. "Access Control" is the process that limits and controls access to resources of a computer system.

5.2. "Users" are employees, consultants, contractors, agents and authorized users accessing SOCI's systems and applications.

5.3. “Privileged Accounts” are system or application accounts that have advanced permissions (as compared to regular Nominative User Account permissions) on such systems or applications.

Examples of Privileged Accounts include Administrator and Super User accounts.

5.4. “Access Privileges” are systems permissions associated with an account, including permissions to access or change data, to process transactions, create or change settings, etc.

5.6. “Administrator Account” is a user account with privileges that have advanced permissions on an IT system that are necessary for the administration of this system.

For example, an administrator account can create new users, change account permissions, modify security settings such as password settings, modify system logs, etc.

5.7 “Super User Account” are accounts where the nominative user has Access Privileges required to complete their job tasks – usually to process transactions or approve changes.

For example, a Super User Account on Synergy can enter and remove expenses to a GL.

5.8. “Nominative User Accounts” are user accounts that are named after a person.

For example chris@shire.gov.cx is a NUA on SOCI’s Outlook platform.

chris.su is a NUA on the Synergy platform.

An NUA on Synergy can raise purchase orders that are to be approved by the appropriate Director or Line Manager with appropriate authority.

6. Guiding Principles – General Requirements

6.1. SOCI will provide access privileges to Institution technology (including networks, systems, applications, computers and mobile devices) based on the following principles:

6.1.1. Need to know – users or resources will be granted access to systems that are necessary to fulfill their roles and responsibilities.

6.1.2. Least privilege – users or resources will be provided with the minimum privileges necessary to fulfill their roles and responsibilities.

6.2. Requests for users’ accounts and access privileges must be formally documented and appropriately approved.

6.3. Requests for temporary accounts for non-SOCI staff must be formally documented and approved by Director of Finance and the CEO. These will be very rare and typically only for external-auditors to log into Synergy to assist with audit matters.

6.4. Where possible, these temporary account to automatically expire at a pre-set date.

When temporary access is required, such access will be removed immediately after the user has completed the task for which the access was granted.

6.6. Access rights will be disabled or removed when IT receives notification that a user is terminated or ceases to have a legitimate reason to access SOCI systems.

6.7. Existing user accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges.

Examples of accounts with excessive privileges include:

6.7.1. A temporary account assigned to external contractors or vendors.

6.7.2. An active account with access rights for which the user's role and responsibilities do not require access. For example, users that do not have authority or responsibility to approve expenses should not have access with approval permissions within a financial system.

6.7.3. System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not the Administrator.

6.7.4. Any unknown active accounts.

7. Exceptions to the Policy

7.1. Exceptions to the guiding principles in this policy must be documented and formally approved by the IT Director.

Policy exceptions must describe:

14.1.1. The nature of the exception

14.1.2. A reasonable explanation for why the policy exception is required

14.1.3. Any risks created by the policy exception

14.1.4. Evidence of approval by the IT Director

8. Inquiries

8.1. Inquiries regarding this policy can be directed to the Director of Governance, Planning and Policy.

9. Systems Mapping

9.1 The IT Officer shall keep an updated Systems Map of users and label whom is an Administrator, Super User or Nominative User for MEX, Outlook, Synergy, etc.

10. IT Officer and Director of IT Responsibility

10.1 Broadly, there will be one Administrator to the network being the IT Officer. The IT Officer will have full Administrator access to all SOCI IT systems including MEX, Synergy, Outlook, Server 2000 and so on.

10.1.1 The IT Officer is responsible for ensuring the 'Emergency Temporary Access' provisions in AD 9 – Change Documentation Management are upheld.

10.2 The Director of Finance and IT will be a Super-User and also grant necessary Access Privileges to staff across the various platforms to enable them to perform their job duties.

For example in the case of issuing an email address on the Shire's domain, staff will typically receive a Nominated User Account with the ability to create, send and delete emails from their own account.

They will be able to set the passwords to their own accounts only. Staff will have no power to create new email addresses, lock accounts or change permissions to other NUAs.

The NUAs are for staff to access the platform to perform work functions solely for their job scope. They will not be granted permissions to be able to alter the network systems.

The Director of Finance will ensure "Privileged Accounts" with sufficient Access Privileges are assigned to staff as needed for the job roles (for example, the senior finance officers will have permissions to add or remove General Ledger entries to process finances. This position however will not have Administrator level privileges such as onboarding or removing accounts from any platform).

Supporting Documents

1. IT Officer logbook
2. Sign off by new account recipients with IT Officer and HR

Document Control Box

Version	Approved, Amended, Rescinded	Date	Officer	Resolution number	Key changes/ notes	Next Review date	File Ref No.
1	Approved	21/3/2023	Chris Su	15/23			