SECURITY POLICY

Roshal Space Consultants Ltd is hereinafter referred to as "the company".

1. OVERVIEW

Consistent standards for network access and authentication are critical to the company's information security and are often required by regulations or third-party agreements. Any user accessing the company's computer systems has the ability to affect the security of all users of the network. An appropriate Network Access and Authentication Policy reduces risk of a security incident by requiring consistent application of authentication and access standards across the network.

2. PURPOSE

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to the corporate network are authenticated in an appropriate manner, in compliance with company standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

3. SCOPE

The scope of this policy includes all users who have access to company-owned or company-provided computers or require access to the corporate network and/or systems. This policy applies not only to employees, but also to guests, contractors, and anyone requiring access to the corporate network. Public access to the company's externally reachable systems, such as its corporate website or public web applications, are specifically excluded from this policy.

4. POLICY

4.1 Account Setup

During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

- Positive ID is required
- Users will be granted least amount of network access required to perform their job function.
- Users will be granted access only if they accept the Security Policy.
- Access to the network will be granted in accordance with the Security Policy.

4.2 Account Use

Network accounts must be implemented in a standard fashion and utilised consistently across the organisation. The following policies apply to account use:

- Accounts must be created using a standard format (i.e., first name-last name, or First initial-last name etc).
- Accounts must be password protected (refer to 4.9 Password Strength for more detailed information).
- Accounts must be for individuals only. Account sharing and group accounts are not permitted.
- User accounts must not be given administrator or 'root' access unless this is necessary to perform his or her job function.
- Guest access is not allowed under any circumstance. Only employees will be allowed network access.

- Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of the Senior Management team.

4.3 Account Termination

When managing network and user accounts, it is important to stay in communication with the Senior Management team so that when an employee no longer works at the company, that employee's account can be disabled, blocked and archived. A process is in place to notify the Senior Management team in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.)

4.4 Authentication

User's machines must be configured to request authentication against the domain at start up. If the domain is not available or authentication for some reason cannot occur, then authentication should occur on the local machine.

4.5 Use of Passwords

When accessing the network locally, username and password is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document, and passwords must conform to 4.9 Password Strength.

4.6 Multi-factor / 2 step authentication

Multi-factor authentication is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism. On certain software's/systems/accounts that can turn MFA on, this will be enabled using a personal telephone number, email address or authenticator app securely downloaded.

4.7 Remote Network Access

Remote access to the network is requested by a Senior Manager and the IT team/consultancy will action this remote access to the network.

4.8 Login credentials

Screensaver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason, screensaver passwords are encouraged.

4.9 Password Strength

All passwords are to be treated as sensitive and confidential information. Any system that handles valuable information must be protected with a password-based access control system. Each user must have a strong, private password to access any service. Never use the same password for more than one account. Create a password using the *Three Radom Words* formula with a number and character and a mix of upper and lower case for example (note purple glass) N0tePurpleGl4ss$.

4.10 Minimum Configuration for Access

Any system connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, users should update their antivirus software, as well as other critical software, to the latest versions before accessing the network.

4.11 Encryption

Industry best practices state that username and password combinations must never be sent as plain text. If this information were intercepted, it could result in a serious security incident. Therefore, authentication credentials must be verbal or encrypted during transmission across any network, whether the transmission occurs internal to the company network or across a public network such as the Internet.

4.12 Failed Logons

Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the company must lock a user's account after a number of unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the Senior Management team/Consultant. Roshal enforce that users will be locked out after 5 failed attempts: this will stop the user from accessing their device for 15 mins. .In order to protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

4.13 Non-Business Hours

While some security can be gained by removing account access capabilities during non-business hours, the company does not mandate time-of-day lockouts. This may be either to encourage working remotely, or because the company's business requires all-hours access.

4.14 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

4.15 AI Usage and Security Policy

As part of our commitment to maintaining a secure a responsible IT environment, the use of Artificial Intelligence (AI) technologies within the company is governed by the following guidelines:

1. **Authorised AI Tools**: Employees must only use AI tools and platforms that have been approved by the IT department/Senior management. Unauthorised use of third-party or unvetted AI tools is prohibited to ensure security, compliance, and data privacy.

2. **Data Privacy and Confidentiality**: AI applications that process sensitive or confidential data must adhere to company privacy policies and data protection regulations (e.g., GDPR). AI models should not be trained on or exposed to any proprietary or personal data without proper authorisation. Employees must be aware of the dangers of exposing personal information.

3. **Access Control**: Access to AI systems must be restricted based on role and need. Only authorised personnel with relevant training should have access to AI systems that handle sensitive information relating to the company.

4. **Security Measures**: AI tools should be regularly updated and maintained to address known vulnerabilities. All AI systems should be subject to the same security standards and protocols as other critical IT systems, including encryption and multi-factor authentication.

5. **Ethical Use**: AI systems must be used in accordance with ethical guidelines that prevent misuse, bias, and discrimination. Any AI-driven decision-making processes should be transparent, auditable, and aligned with the company's values.

6. **Incident Reporting**: Any suspicious activity or security incidents related to AI systems must be reported immediately to the Senior Management. This includes potential breaches, unauthorised access, or misuse of AI tools.

By adhering to these guidelines, we ensure the safe and responsible use of AI technologies within our organisation, protecting both our data and our reputation.

5.0 ENFORCEMENT

This policy will be enforced by the Senior Management Team of Roshal Space Consultants ltd. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination/consideration of termination of employment. This limits the risk of the user destroying or copying any data. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 DEFINITIONS

- *Antivirus Software:* An application used to protect a computer from viruses, typically through real time defences and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.
- *Authentication:* A security method used to verify the identity of a user and authorise access to a system or network
- *Encryption:* The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.
- *Password:* A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

Signed:

Craig Parsons
Managing Director
Roshal Space Consultants Ltd

Date: 16th June 2026