**ISMS Access Control Policy**

**Doc A9.1**

**Version: 1.0**

Publication Date: October, 2024

Current Status: Published

Author(s): C.D.Aluthge

Reviewed By: C.D.Aluthge

**Table of Contents**

1 Scope 3

2 Access Control Policy 3

2.1 General 3

2.2 Passwords 3

2.3 Auditing 4

3 Document Control and Approval 5

3.1 Distribution 5

3.2 Version Information 5

# Scope

This policy applies to the network placed at Satellite's facilities, which may be used by Wacky Widget employees or third parties who have signed relevant confidentiality and access agreements.

# Access Control Policy

Wacky Widget restricts access to information based on security concerns. Business demands must be accommodated within the parameters of this policy.

## General

A user account that is personally identified controls all data access. When a system does not allow access otherwise, shared and generic credentials are allowed.

The security requirements are set as follows:

•Make sure the information categorization levels and the related access control criteria are in sync.

•The concept of least privilege is used to give access.

•User access is controlled by formal permission processes and is reviewed on a regular basis.

•The standards of data protection and privacy legislation are satisfied.

•Client contractual obligations for data or service access are satisfied.

Service accounts may be utilized; however, the dangers posed by such accounts must be examined and understood before they are used. Access is restricted to the bare minimum necessary to satisfy the requirements.

Unauthorized access to the organization's networked systems is prevented.

It is not authorized to have an open wifi access point with access to business networks. The guest wireless network must be segregated to allow only public Internet access.

Access control methods for network services are maintained by the Service Desk.

## Passwords

Passwords are unique to each user and must be changed on a frequent basis to maintain privacy.

Passwords are classed as "Company Sensitive," which means they should not be shared with anyone else. Within teams, utilizing systems that only give a restricted number of credentials, exceptions can be made.

* When one user of a shared account no longer requires access, all shared credentials must be updated.

**In general:**

* Do not give your passwords to anyone else
* It is not a good idea to write down passwords. Only company-approved password managers may be used to store passwords necessary to execute Wacky Widget business tasks.
* PWSafe
* KeyPass

**Staff with standard privilege access to the Wacky Widget network, must follow best practice with regards to password complexity:**

* 10 characters is the minimum password length.
* 180 days is the maximum password age.
* 1 day is the minimum password age.
* Passwords must not be reused in the past.
* The Staff's name or dictionary passwords are not permitted in passwords.
* At least one upper case letter, one lower case letter, one number, and one special character are required in passwords.

**Staff who require elevated privilege or admin access to the Wacky Widget network, must maintain a separate account from their daily standard privilege account, and follow best practice with regards to password complexity:**

* 12 characters is the minimum password length.
* 90 days is the maximum password age.
* 1 day is the minimum password age.
* Passwords must not be reused in the past.
* The Staff's name or dictionary passwords are not permitted in passwords.
* At least one upper case letter, one lower case letter, one number, and one special character are required in passwords.

## Auditing

Security privilege changes should be auditable. For any modification, the following must be documented in logs.

* When changed
* By whom
* Who approved the changed.

All privileged or sensitive access rights should be reviewed at least once a year.

# Document Control and Approval

The Chief Information Security Officer is the document's owner and is responsible for ensuring that it is evaluated in accordance with the ISMS's review standards.

All members of staff have access to the most recent version of this document, which is also the published version.

Signature: Signature of Executive Manager Date: 01.11.2023

## Distribution

|  |  |
| --- | --- |
| **Name** | **Role** |
| *Intranet* | *Distribution to all staff* |