**ISMS Access Control Policy**

**Doc A9.1**

**Version: 1.0**

Publication Date: January 2019

Current Status: Published

Author(s): Michael Woolard

Reviewed By: Michael Woolard

**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

The network within scope of this policy is that installed at the organization’s premises which may be accessed by employees of Wacky Widget or by 3rd parties who have signed appropriate confidentiality and access agreements.

# Access Control Policy

Wacky Widget controls access to information on the basis of security requirements. Business needs must work within the confines of this policy.

## General

All access to data is controlled by a user account which is uniquely identifiable. Shared and generic credentials are only permitted when a system does not allow access otherwise.

The security requirements are set as follows:

* Ensure there is consistency between the information classification levels and relevant access control requirements
* Access is granted using the principle of least privilege
* User access is subject to formal authorization procedures and to periodic review
* Data protection and privacy legislation requirements are met.
* Client contractual commitments regarding access to data or services are met

Service accounts may be used; however, risks that are brought about by such accounts must be risk assessed and understood prior. Access is limited to least privilege required to meet need.

The organization protects its networked systems from unauthorized access.

Open wireless access point with access to company networks is not permitted. Guest wireless network must be segmented to provide access to public Internet only.

Service Desk maintains access control procedures by which network services may be accessed.

## Passwords

Passwords are unique to each user and must be changed regularly to ensure confidentiality.

Passwords are classified as Company Sensitive, and must not be shared with anyone else. Exceptions can be made within teams using systems that only provide a limited set of credentials.

* All shared credentials must be changed when 1 user of a shared account no longer requires access

**In general:**

* Do not give your passwords to anyone else
* Passwords are not to be written down. Passwords required to perform Wacky Widget business functions may only be stored in company approved password managers
  + PWSafe
  + KeyPass

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

* Minimum password length: 10 characters
* Maximum password age: 180 days
* Minimum password age: 1 days
* History: Must not re-use passwords
* Passwords must not contain the Staff’s name or dictionary passwords.
* Passwords must contain at least 1 upper case letter, 1 lower case letter, 1 number and 1 special character.

**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:**

* Minimum password length: 12 characters
* Maximum password age: 90 days
* Minimum password age: 1 days
* History: Must not re-use passwords
* Passwords must not contain the Staff’s name or dictionary passwords.
* Passwords must contain at least 1 upper case letter, 1 lower case letter, 1 number and 1 special character.

## Auditing

Changes to security privileges should be auditable. The following must be recorded in logs for any change

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

A periodic review of all privileged or sensitive access permissions should be carried our annually.

# Document Control and Approval

The Chief Information Security Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff and is the published version.

Signature: Executive Manager Signature Date: 01.01.2019

## Distribution

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

## Version Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author(s)** | **Details** |
| 0.1 | 11/28/18 | M.Woolard | First draft |
| 0.2 | 12/07/18 | M.Woolard | Second draft |
| 1.0 | 01/01/19 | M.Woolard | First published |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 