Password policy

1. Introduction

1.1 Scope

This policy sets out Buzz Saw's requirements for the use of strong passwords, the protection of those passwords, and the regular changing of those passwords.

This policy applies to all staff, including employees, contractors and interns, etc. working under the Access Control Policy.

1.2 Revision History

Revision	Date	Record of Changes	Approved By
0.0	01/01/2020	Initial Issue	JE/WS

1.3 Control of hardcopy versions

The digital version of this document is the most recent version. It is the responsibility of the individual to ensure that any printed version is the most recent version. The printed version of this manual is uncontrolled, and cannot be relied upon, except when formally issued by the ISMS Manager and provided with a document reference number and revision in the fields below:

Document Ref.	Rev.	Uncontrolled Copy	X	Controlled Copy

1.4 References

Standard	Title	Description
SO 27000:2014	Information security management systems	Overview and vocabulary
5O 27001:2013	Information security management systems	Requirements
ISO 27002:2013	Information technology-security techniques	Code of practice for information security controls

1.5 Terms and Definitions

- “staff”includes all of those who work under our control, including employees, contractors, interns etc.
- “we”and”our”refer to <Short Name>

1.6 Responsibilities

The ISMS Manager is responsible for all aspects of the implementation and management of this procedure unless noted otherwise.

Managers and supervisors are responsible for the implementation of this policy, within the scope of their responsibilities, and must ensure that all personnel under their control understand and undertake their responsibilities accordingly.

2. Password Policy

2.1 General

To ensure the continuing security and integrity of all Buzz Saw's system/access login accounts the following procedures and practices must be followed:

- All users must ensure that their password is not divulged or shared with anyone else.
- All users must not write down and store their passwords within the office.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- At initial setup systems may automatically generate temporary passwords, and these should be changed at the earliest opportunity.
- All ICT devices which may require local logon privileges for configuration and maintenance must have the built-in default admin (or equivalent) account password promptly changed in line with the guidelines of this policy wherever possible

  All ICT systems should:

  – Support individual user authentication

  – Prevent the storing of passwords in clear text or in any easily reversible form

  – Provide for management of specific roles and functions within a system enabling

  delegation of tasks to individuals

  – Not contain or utilize embedded (hard-coded)passwords

2.2 All passwords must meet the following requirements:

- nore-use of last 10 passwords.

- maximum password age 42 days.
- minimum password age 2 days.
- minimum password length is 8 characters.
- account lockout threshold 5 invalid logon attempts.
- reset account lockout counter after 30 minutes.
- users are prompted to change password at logon 7 days prior to the existing one expiring.
- passwords must contain at least three of the following five elements:
  - numeric-(0-9)
  - uppercase-(A-Z
  - lowercase-(a-z)
  - special characters (?,!,@,#,%,etc…)

2.3 Responsibilities of those creating passwords

2.3.1 Do not use passwords which have any of the following characteristics:

- contains less than 8 characters
- is a word found in a dictionary of any language
- is a common usage word such as:
  - names of family, pets, friends, co-workers, fantasy characters, etc.
  - computer terms and names, commands, sites, companies, hardware, software.
  - birthdays and other personal information such as addresses and phone numbers.
  - word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

  - any of the above spelled backwards.
  - any of the above preceded or followed by a digit (e.g.,secret1,1secret)

- are the same as password used for non-business purposes
- are the same as passwords used for other business systems

2.3.2 Do not do any of the following:

- use passwords which contain parts of your account name, or your full name, that exceed two consecutive characters.
- share business passwords with anyone, including administrative assistants or secretaries.
- reveal a password over the phone to anyone
- write passwords down and store them anywhere in your office
- reveal a password in an email message
- reveal a password to your line manager
- talk about a password in front of others
- hint at the format of a password (e.g., “my family name”)
- reveal a password on questionnaires or security forms
- share a password with family members
- reveal a password to co-workers while on holiday
- reveal a password to someone who demands it – refer them to this document
- use the “Remember Password” feature of applications (e.g., Internet Explorer, SAP etc…)
- store passwords in a file on any computer system (including mobile devices or similar) without encryption
- leave a password unchanged for more than the recommended period

2.3.3 If you suspect a password has been compromised

If an account or password is suspected to have been compromised, report the incident as soon as possible to **<**IT Services> and Immediately change any/all passwords which may have been compromised.

3. Breaches of Policy

Buzz Saw will take all necessary measures to remedy any breach of this policy including the use of our disciplinary or contractual processes where appropriate.

4. Records

Records retained in support of this procedure are listed in the ISMS Controlled Records Register and controlled according to the Control of Management System Records Procedure.