Password Policy

Document Owner: Data Protection Officer

Approved by: Chief Information Officer

Date Approved: 24th January 2023

Next Review Date: January 2025

Version: 1

Security Classification: Internal use only.

Version	Revision Date	Revised by	Section Revised
1	01.23	Judi Wood	Policy created

Purpose

This policy supports the IT regulations to ensure that passwords used to access computer resources are selected and updated in line with best proactive security standards.

The IM Group Ltd.’s IT regulations state that Users must take all necessary steps to protect and maintain the security of any equipment, software, data, storage area and/or passwords allocated for their use. This policy dictates the minimum that a user must do to conform to this requirement when selecting and updating a password.

Password policies are used to mitigate possible attacks against IM Group Ltd.’s IT infrastructure and the data held upon it. Use of long, complex passwords help to mitigate attacks that attempt to guess passwords, and regular password changes to mitigate long term exploitation of any disclosed or discovered passwords.

Password Selection

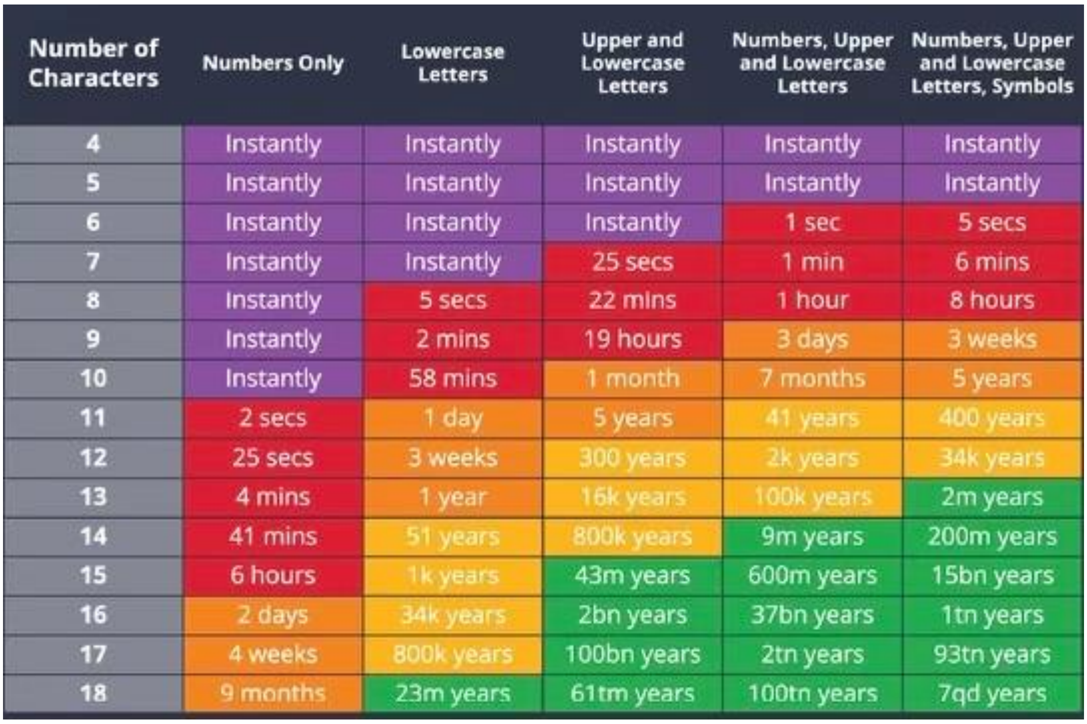
To protect IM Groups systems and data, users must select a password that is secure and difficult to guess.
In accordance with security best practice the following rules are mandatory:

- All passwords should have a minimum of twelve characters.
- Each password must contain a combination of at least three out of four-character sets:
    - Uppercase characters (A through to Z)
    - Lowercase characters (a through to z)
    - Numerical digits (0 through to 9)
    - Non-alphabetical characters (e.g.! $ # % @ +)
    - Previous passwords used must not be re-used.

In addition, while not actively enforced by the password creation process:

- Accounts created for use on external online resources must not use the same password for IM Group Ltd.’s authentication.
- Passwords must not be something that can easily by guessed (avoid using your name, children or a pet’s name, car registration number, football team, etc). Hackers have compiled very extensive lists of words and combinations in use and add to that list by the hour. These lists are then used to probe access to your account alongside activities to identify possible phrases you may use such as known dates, names, places etc. Hence, the recommendation to use a 12+ combination of letters, numbers, and special characters in a non-pattern-based format.
- You may choose to combine random words with numbers and characters (i.e.. CornSt8plerFleece!)

The chart below demonstrates how long it takes a potential hacker to find your password to enter your accounts.



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	61tm years	100tn years	7qd years

See Appendix A for a complete list of enforced password settings.

Changing a Password

Passwords must be changed regularly to mitigate the long term exploitation of any disclosed or discovered passwords. It is recommended those passwords are changed every 60 days.

Password Use

Passwords are the mechanism used to protect the security of IM Groups systems and must be protected.

- Passwords must be kept secret.
- Passwords must not be written in a form that others could identify.
- Passwords must not be stored electronically in a non-encrypted format.
- Passwords must never be shared with others.
- Care should be taken to prevent anyone from watching you type your password.

Appendix A - Enforced password settings and rationale

	Setting	**Rationale**
Minimum password length	12 characters	In line with recommended minimum password sizes, to reduce the risk of dictionary attacks.
Minimum password age	0 days	To allow immediate changing of password following help desk reset.
Maximum password age	60 days	To ensure passwords are changed each year, while avoiding potential impact on staff.
Password history	24 passwords	To prevent the same password from being re-used (Note this is the maximum possible value).
Password Complexity	Enabled	To enforce stronger passwords (three of uppercase, lowercase, numbers, symbols).
Change password at first use	No	Disabled to simplify logon process for staff working from home.
Account lockout	15 minutes automatic Account Lockout after 3 bad passwords	To prevent dictionary attacks without impacting on staff