Version	Date	Author	Owner	Comments
V1.0	14 July 2020	Head of Risk, Information and Security Compliance	Head of Risk, Information and Security Compliance	Instruction created

Next review: July 2021

Security Instruction – The Use of Passwords

This information, although in the form of 'musts' and 'must nots', should be seen as positive guidance; its intention is to protect the company and the employee from security vulnerabilities, fraud, legal challenges and reputational/professional damage. The role of a password is to prevent unauthorised access to data. Passwords must be difficult for others to guess but, at the same time, be easy to remember. Additional technical instructions are issued to our ISS teams. Breaches of these instructions may lead to disciplinary action. Related instructions are:

- Acceptable Use of IT Systems
- Working Off-Site
- Acceptable Use of Email and Mailboxes
- Security Classifications
- Acceptable use of the Internet and Social Media
- Managing Information Security Incidents and Personal Data Breaches Guide
- Taking Equipment Overseas
- Records Management
- Clear Desk/Screen

Passwords must:

- Be at least 9 characters long
- Have at least one number
- Have at least one CAPITAL letter
- Have at least one symbol such as: !@#$%^&*(){}[]

For additional security, you may wish to use a 'passphrase' as these provide a good way to compose strong, lengthy passwords that are easier to remember, easier to type, and naturally complex; they are harder to crack than traditional passwords.

For example, if you enjoy watching Sherlock on TV, you could use MYD3ARWAT5ON or EXTERMIN8_EXTERMIN8 if you prefer Doctor Who.

Protecting Passwords:

You must:

- Password protect the email attachments containing OFFICIAL SENSITIVE PERSONAL information for the secure transmission only (e.g. for payroll purposes), ensuring the password meets the above stated complexity requirements and communicated to the recipient by another communication source, such as text or phone.

- Create a unique password every time you need to change it.

- Never write down your passwords: use the password manager.
- Never share your passwords with anyone.
- Never type your password when someone is looking over your shoulder.
- Never send your passwords to anybody in an email.
- Change passwords immediately if you know or suspect they have been compromised.
- Quit your Internet browser when you are finished using it.

Service accounts:

The use of service accounts should only be permitted where they are necessary for business or operational reasons. Service Accounts could be used by specific services on servers and in minimal cases, workstations. Passwords are stored in the encrypted Keepass/Keeper database. Passwords will get changed according to the password policies in the domains where the accounts live unless they're marked "do not expire" for any reason.

If you need further advice on this, or other instructions, you should contact any member of the Risk, Information and Security Compliance team on Ext. 7743, 7486, 7481 or 7526.