ESH GROUP
PASSWORD POLICY

Policy Author:	Paul Carmody, Head of IT
Date:	May 2018
Policy Review Date:	2019
Policy Owner:	Mark Sowerby, Group Chief Financial Officer

1 Policy Statement

Passwords are an important part of computer security and the front line protection for our IT systems and data.

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords and their frequency of change in line with best practice.

2 Scope

This policy applies to all workers who either have, or are responsible for, an account that requires a password to access any IT system that processes data for or on behalf of the Esh Group or who are required to password protect documents of a sensitive nature to share with external parties.

2 Policy

2.1.1 All passwords should be memorable yet remain difficult for unauthorised people to guess. Choose passwords that are at least 8 characters in length and avoid basic combinations such as “password”, “password1” and “P455w0rd” which are strictly prohibited.

2.1.2 Group IT recommend using three random words as your password but avoiding simple combinations such as “onetwothree” or words that are closely related to you personally, such as the names of family members or pets.

2.1.3 Workers must choose unique passwords for their company accounts and not use a password that they are already using for a personal or social media account.

2.1.4 If the security of a password is in doubt, for example, if it appears that an unauthorised person has logged in to the account — the password must be changed immediately.

2.1.5 Default passwords, such as those created for new workers when they start or those provided with any new system when they’re initially set up, must be changed as soon as possible.

2.1.6 Workers must never share their passwords with anyone else, including co-workers, managers, administrative assistants, family or friends. The exception would be IT staff members to aid in resolving an IT issue on your behalf. If you do provide your password to IT, you are strongly advised to change it following the support call.

2.1.7 Group IT support will never ask you for your password via email. Should you receive a request from IT for your password in this manner, please inform the Head of IT.

2.1.8 Workers are prohibited from sharing their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.

2.1.9 Workers must refrain from writing passwords down and keeping them at their workstations.

2.1.10 IT Services recommend using a Password Manager if you manage many passwords in your role, however workers must not use password managers or other tools to help store and remember passwords without seeking advice from Esh Group IT first.

2.1.11 If protecting documents with a password, do not send the document and the password in the same email. If possible, call the recipient and provide the password over the phone or deliver it separately by other means, such as a text message.

3 Policy Compliance

3.1 Compliance Measurement

3.1.1 IT Services and Group Internal Controls team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

3.2 Exceptions

3.2.1 Any exception to the policy must be endorsed by the appropriate Business Director and approved by the Head of IT in advance.

3.3 Non-Compliance

3.3.1 An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.