



Passwords are the primary way in which the SES Group protects its computer systems and other infrastructure from unauthorised use. Constructing secure passwords and ensuring proper password management are essential. Poor password management and protection could allow unauthorised access to the SES Groups computer systems and could lead to the inappropriate disclosure and use of confidential or sensitive information. The purpose of this policy is to provide clear guidance and best practice for the creation of strong passwords.

Where Possible all computer systems and infrastructure must be protected by the use of strong passwords. All passwords must be unique and meet the following standard:

Passwords must be a minimum of 8 characters in length

Passwords should be changed at least every 90 days

Passwords must contain a combination of letters (both upper & lower case), numbers (0-9) and at least one special character eg: ", £, \$, %, ^, &, *, @, #, ?, !, €

Passwords must not be left blank

Passwords or part of a password must not contain:

Words with numbers appended

Words with simple obfuscation

Names of fictional characters

Common keyboard sequences

Names of people, places or organisations

A sequence of consecutive numbers or letters

Personal information related to a user

eg: bigup2000, password2012, paul2468

eg: p@ssw0rd, g0ldf1sh

eg: frodo, shrek

eg: qwerty

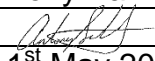
eg: spursgr8, LFC2005, ManUtd

eg: 12345678, abcdefgh, abcd1234

eg: users name, address, date of birth, ID number, telephone number

No password may be re-used by a user within a 12 month period.

Users must ensure all passwords are kept confidential at all times and are not shared with others including their co-workers or third parties.

Name:	Tony Ball
Signature:	
Date:	1 st May 2017

1	AS	TB - MD	01/05/17	N/A First Issue
Revision	Prepared by	Approved by	Issue Date	Description of Modifications Made