Password Standard Policy

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 180 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	eg: bigup2000, password2012, paul2468
Words with simple obfuscation	eg: p@ssw0rd, g0ldf1sh
Names of fictional characters	eg: frodo, shrek
Common keyboard sequences	eg: qwerty
Names of people, places or organisations	eg: spursrgr8, LFC2005, ManUtd
A sequence of consecutive numbers or letters	eg: 12345678, abcdefgh, abcd1234
Personal information related to a user birth, ID number,	eg: users name, address, date of telephone number

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

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

Name:	Tony Ball
Signature:	
Date:	10/10/2024