**Strong password guidelines**

**Guidelines for end users**

1. Minimum 8 characters
2. Include at least one upper case character
3. Include at least one lower case character
4. Include at least one numeric character
5. Include at least one special character
6. Expires after 30 days
7. Used for only one system or application
8. Not to be shared
9. To be cancelled as soon as user rights change or employee leaves the organisation
10. Automatically invoked on device log-off or application exit
11. Automatically invoked on screensaver activation
12. Not a simple string of characters (e.g. not 123456)
13. Not easily guessed (e.g. not user name, company name)
14. Does not contain complete words
15. A password should not be reused when setting a new password.

**Guidelines for system administrators**

1. Limit unsuccessful password logon attempts
2. Report unsuccessful password logon attempts
3. Enforce password rules
4. Check for the same password used across multiple systems