Password rules – information for organisations

Why are we changing?

* We have listened to user feedback about the challenges of password management in ESR.
* We have aligned with guidelines set out by the National Cyber Security Centre- <https://www.ncsc.gov.uk/>

What are we doing?

* We have simplified our policy whilst retaining recommended rules.
* There is no expiry period enforced by default for passwords on new accounts.
* There is no repeat/sequential character rule.
* There are 3 rules for password requirements:
* Minimum password length of 12 characters.
* The password may not be the same as any of the previous 4 passwords.
* Commonly used passwords, such as password1, are not allowed.
* Developing simple guidance to help employees better manage their ESR password.

What can you do?

* Consider your use of expiry periods on employee user accounts, if you are still using them.
* Review local policies for ESR users alongside your other IT system access requirements.
* Ensure all your employees understand their responsibilities with managing their user account.
* Where large numbers of accounts require an update to remove the expiry period log an SR and we will work with you to help where possible.