SGS ECL Password Best Practice Info

Context

The SGS ECL 'ECL Cyber' team are a team of industrial/ICS/OT security professionals – mainly ICS/OT security consultants and engineers. Often, we are asked to consult and advise on a variety of ICS/OT security practices including password management. This document represents a repository of password best-practice snippets and links to support both IT and OT practitioners in making good risk-based decisions on password policy and philosophy

Best Practices – Complexity and Expiry NOT recommended

Microsoft

Password expiration requirements do more harm than good, because these requirements make users select predictable passwords… Password complexity requirements reduce key space and cause users to act in predictable ways, doing more harm than good…
https://docs.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide

SANS

Password expiration is a dying concept. Essentially, it's when an organization requires their workforce to change their passwords every 60, 90 or XX number of days. And while there are several reasons behind the password expiration policy, most at this point seem obsolete…
https://www.sans.org/blog/time-for-password-expiration-to-die/

Stop inflicting painful complexity requirements, instead long live the passphrase…
https://www.sans.org/blog/nist-has-spoken-death-to-complexity-long-live-the-passphrase/

NIST

5.1.1.2 … Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically) …
5.1.1.1 … *No other complexity requirements for memorized secrets SHOULD be imposed…*
https://pages.nist.gov/800-63-3/sp800-63b.html

NCSC UK

Regular password expiry is a common requirement in many security policies. However, in the Password Guidance published in 2015, we explicitly advised against it…
https://www.ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry
https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words

Google

Password expiration is turned off by default because research has shown little positive impact on security.
https://support.google.com/a/answer/139399?hl=en#zippy=%2Chow-password-expiration-works

Contact

SGS ECL welcome the opportunity for robust debate and discourse on this subject. Email cyber@ecl.co.nz if you have any comments. See https://eclcyber.co.nz for more info on SGS ECL.