Risk Treatment Plan – UCSB 2023-001
Password/Passphrase Management
Authentication Management

**Purpose:** UC’s Electronic Information Security Policy IS-3, Section III, Subsection 6.1.2, sets guidelines for optimized sets of security controls using a Risk Treatment Plan (RTP).

This Risk Treatment Plan is for password/passphrase and authentication management, as discussed in the UC Account and Authentication Management Standard Sections 4 and 5. This plan addresses and modifies the requirements set out in section 4.1, dealing with password strength, section 4.3, dealing with password changes, section 4.5, dealing with session timeout, and section 5.3, dealing with account and reset lockout. This treatment plan seeks to balance threats to authentication systems from password attacks with user behavior and compliance while helping to manage support costs.

**Conditions for use of this risk treatment plan**

- Accounts and Passwords/passphrases used as part of the campus Single Sign On (SSO) system
- Accounts and Passwords/passphrases used as part of any managed authentication infrastructure designed to regulate access to multiple people e.g. Active Directory, RACF.
- Accounts and Passwords/passphrases used as part of an individual device such as a PC or server, including privileged accounts.

**Minimum required controls**

- In general, the password/passphrase strength requirements in section 4.1 apply with the three exceptions to increase the strength of passwords/passphrases against brute force and dictionary attacks.
- Password/passphrase length must be 12 characters or more in all use cases that support that character length.
- Passwords/passphrases from 12 to 15 characters must use at least 3 out of the 4 character classes described.
- Passwords/passphrases from 16 to 19 characters must use at least 2 out of the 4 character classes described.
- Password/passphrase changes increase support burdens and provide minimal improved security when passwords/passphrases are not used across multiple services. Consistent with NIST recommendations, mandatory user password/passphrase changes are not required when users are instructed not to reuse passwords/passphrases at other locations at the point where the password/passphrase is set or changed.
- Endpoints shall be configured to lock/reset an account after 10 failed login attempts.
- Endpoints containing or accessing data classified at Protection Level P3 or P4 should be configured with a session timeout of no more than 15 minutes of inactivity.
Recommended Controls

- In all cases, where possible, users should be advised not to reuse passwords/passphrases at multiple sites at the point when a password is set or changed.
- Where possible, users should be advised to select longer passwords/passphrases over shorter ones.
- Automated password/passphrase strength checking and enforcement should be applied when technically possible (i.e., when supported by the technology). Password/passphrase strength requirements apply even when they cannot be technically enforced, for example, in IoT applications.
- The reuse of previously retired passwords/passphrases is discouraged.
- Constructing a new password/passphrase by varying a single character, such as adding or changing a number to the end of a password/passphrase, is discouraged.

Approved by: draft, CISO, UCSB 2023-001
Date: September 29, 2023