Unified UCSF Enterprise Password Standard

Esther Silver on November 20, 2017

Policy Type

Standard

This Unified UCSF Enterprise Password Standard was approved by the UCSF CIO on October 1, 2010, and is applicable to all Electronic Information Resources within UCSF, including the Medical Center. Questions about this standard can be sent to the Security & Policy Group, at security@ucsf.edu

<table>
<thead>
<tr>
<th>Category</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed logons allowed before lockout</td>
<td>5 failed attempts</td>
</tr>
<tr>
<td>Lockout duration</td>
<td>15 minutes</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>7</td>
</tr>
<tr>
<td>Maximum consecutive character repeats</td>
<td>2</td>
</tr>
<tr>
<td>Required characters</td>
<td>At least one in 3 of 4 character sets: Upper/lower case, numbers, symbols</td>
</tr>
</tbody>
</table>
Prohibited patterns

Easily guessed patterns: dates, phone numbers, proper names, minor variations on former password

This standard should be considered a minimum. Systems that are capable of exceeding these standards should if operationally feasible. Active Directory implements this standard as part of the Unified UCSF Enterprise Password Standard [1].

Privileged administrator accounts with access to sensitive Windows systems should use passphrases that are 15 or more characters in length and meet the other requirements within this standard. Passphrases should be reset at least every 90 days.

Important Reminders

- Pick as strong a password as possible and keep it safe. If at any time, you feel your password may have been compromised, change it.
- Certain regulations may require password aging for specific systems. For example, Payment Card Industry Data Security Standard (PCI-DSS) requires password changes every 90 days. PCI system owners are responsible for the implementation of password aging and should NOT rely on the minimum standard.

Exceptions

All systems must comply with the password standard if possible. There are some cases in which an exception may be granted, including:

- Technical limitations
- Regulatory reasons

Systems granted an exception may be required to have additional compensating information security controls in place, such as a stricter firewall, or greater access logging.

Exception Process

All exception requests should be directed to the UCSF IT Service Desk: online at http://help.ucsf.edu/ [2] or by phone (415) 514-4100.

UCSF Security & Policy (S&P) will investigate the request and render a decision. Requests will be reviewed by the Security and IT Policy Committee a periodic basis.

Exception Requests

Exception requests must contain the following information at a minimum:

- Name of the individual
- Affiliation/Title of the individual(s)
- Name of the system(s)
- Types of data the account(s) will have access to, particularly, any access to Restricted Information such as ePHI or PII
- Types of data on the system(s) where the exception(s) will be effective, particularly, any
access to Restricted Information such as ePHI or PII

- Reason for the request
- Duration, e.g., temporary (with start and end times) or permanent

**Granted Exceptions**

Exceptions granted will be tracked by S&P and will be reviewed every 12 months to ensure exceptions are still valid and required

**GET IT HELP.** Contact the Service Desk online, or phone 415.514.4100

   Site Login  Site Index

   Suggest an IT Improvement  © UC Regents

**Source URL:** [https://it.ucsf.edu/policies/unified-ucsf-enterprise-password-standard-0](https://it.ucsf.edu/policies/unified-ucsf-enterprise-password-standard-0)

**Links:**
[1] [https://it.ucsf.edu/policies/unified-ucsf-enterprise-password-standard-0](https://it.ucsf.edu/policies/unified-ucsf-enterprise-password-standard-0)