ICRMP Password Policy Guidance

Scope:

Based on the updated recommendations in the Digital Identity Guidelines report that the National Institute of Standards (NIST) released in June of 2017, ICRMP would like to change its password policy to adhere to the updated recommendations.

The NIST Report can be found at this URL: https://pages.nist.gov/800-63-3/sp800-63b.html Section 5 and Appendix A of the report are the source of the updated recommendations.

The New Password Policy we recommend follows the updated recommendations from the Digital Identity Guidelines from the NIST:

1. Passwords must be at least 10 characters long
2. Password character complexity is **NOT** required
3. Passwords do **NOT** expire
4. Password must not contain characters that repeat more than twice or keyboard patterns (qwerty, 1234, asdf)
5. Passwords must be screened against a list of commonly used passwords, user names and dictionary words. Any password that matches any of these categories will be rejected and a new password must be chosen.
6. After 3 failed logon attempts, Accounts are locked out for 60 minutes
7. Accounts are immediately disabled when no longer in use (Temporary Vendor accounts, Staff Member departure, etc)

Analysis:

The updated password policy the NIST recommends will put ICRMP and our members in a better security position overall. This excerpt from section A.5 of the NIST Digital Identity Guidelines report sums it up well:

"Length and complexity requirements beyond those recommended here significantly increase the difficulty of memorized secrets and increase user frustration. As a result, users often work around these restrictions in a way that is counterproductive. Furthermore, other mitigations such as blacklists, secure hashed storage, and rate limiting are more effective at preventing modern brute-force attacks. Therefore, no additional complexity requirements are imposed."