NIST seem to be moving in the right and common sense direction regarding password policy.  Their research has proven that the massive password requirement overheads such as **periodic password changes** and **forced password complexity**, in fact make systems less secure.

Aviva should be globally re-aligning ourselves to these new guidelines.  In-fact, this follows our koru value of Kill Complexity.  The NIST Digital Identity Guidelines are currently in draft and is expected to be made final by September 2017.

---------------------------------------------------------------

*“****No more periodic password changes****. This is a huge change of policy as it removes a significant burden from both users and IT departments. It’s been clear for a long time that periodic changes do not improve password security but only make it worse, and now NIST research has finally provided the proof.*

***No more imposed password complexity*** *(like requiring a combination of letters, numbers, and special characters). This means users now can be less “creative” and avoid passwords like “Password1$”, which only provide a false sense of security.*

***Mandatory validation of newly created passwords against a list of commonly-used, expected, or compromised passwords****. Users will be prevented from setting passwords like “password”, “12345678”, etc. which hackers can easily guess.”*

*Read more:* [*https://venturebeat.com/2017/04/18/new-password-guidelines-say-everything-we-thought-about-passwords-is-wrong/*](https://venturebeat.com/2017/04/18/new-password-guidelines-say-everything-we-thought-about-passwords-is-wrong/)

---------------------------------------------------------------

***DRAFT NIST Special Publication 800-63B - Digital Identity Guidelines - Authentication and Lifecycle Management -*** [*https://pages.nist.gov/800-63-3/sp800-63b.html*](https://pages.nist.gov/800-63-3/sp800-63b.html)

[*https://pages.nist.gov/800-63-3/*](https://pages.nist.gov/800-63-3/)

[*https://www.nist.gov/itl/tig/special-publication-800-63-3*](https://www.nist.gov/itl/tig/special-publication-800-63-3)

Verifiers SHOULD NOT impose other composition rules (e.g., mixtures of different character types) on memorized secrets. Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically) and SHOULD only require a change if the subscriber requests a change or there is evidence of compromise of the authenticator.

## Appendix A: Strength of Memorized Secrets

This appendix is informative.

### A.1. Introduction

Despite widespread frustration with the use of passwords from both a usability and security standpoint, they remain a very widely used form of authentication. Humans, however, have only a limited ability to memorize complex, arbitrary secrets, so they often choose passwords that can be easily guessed. To address the resultant security concerns, online services have introduced rules in an effort to increase the complexity of these memorized secrets. The most notable form of these is composition rules, which require the user to choose passwords constructed using a mix of character types, such as at least one digit, uppercase letter, and symbol. However, analyses of breached password databases reveals that the benefit of such rules is not nearly as significant as initially thought, although the impact on usability and memorability is severe.

Complexity of user-chosen passwords has often been characterized using the information theory concept of entropy [[Shannon]](https://pages.nist.gov/800-63-3/sp800-63b.html#shannon). While entropy can be readily calculated for data having deterministic distribution functions, estimating the entropy for user-chosen passwords is difficult and past efforts to do so have not been particularly accurate. For this reason, a different and somewhat simpler approach, based primarily on password length, is presented herein.

Many attacks associated with the use of passwords are not affected by password complexity and length. Keystroke logging, phishing, and social engineering attacks are equally effective on lengthy, complex passwords as simple ones. These attacks are outside the scope of this Appendix.

### A.2. Length

Password length has been found to be the primary factor in characterizing password strength. Passwords that are too short yield to brute force attacks as well as to dictionary attacks using words and commonly chosen passwords.

The minimum password length that should be required depends to a large extent on the threat model being addressed. Online attacks where the attacker attempts to log in by guessing the password can be mitigated by throttling the rate of login attempts permitted. In order to prevent an attacker (or a persistent claimant with poor typing skills) from easily inflicting a denial-of-service attack on the subscriber by making many incorrect guesses, passwords need to be complex enough that throttling does not occur after a modest number of erroneous attempts, but does occur before there is a significant chance of a successful guess.

Offline attacks are sometimes possible when one or more hashed passwords is obtained by the attacker through a database breach. The ability of the attacker to determine one or more users’ passwords depends on the way in which the password is stored. Commonly, passwords are salted with a random value and hashed, preferably using a computationally expensive algorithm. Even with such measures, the current ability of attackers to compute many billions of hashes per second with no throttling requires passwords intended to resist such attacks to be orders of magnitude more complex than those that are expected to resist only online attacks.

Users should be encouraged to make their passwords as lengthy as they want, within reason. Since the size of a hashed password is independent of its length, there is no reason not to permit the use of lengthy passwords (or pass phrases) if the user wishes. Extremely long passwords (perhaps megabytes in length) could conceivably require excessive processing time to hash, so it is reasonable to have some limit.

### A.3. Complexity

As noted above, composition rules are commonly used in an attempt to increase the difficulty of guessing user-chosen passwords. Research has shown, however, that users respond in very predictable ways to the requirements imposed by composition rules. For example, a user that might have chosen “password” as their password would be relatively likely to choose “Password1” if required to include an uppercase letter and a number, or “Password1!” if a symbol is also required.

Users also express frustration when attempts to create complex passwords are rejected by online services. Many services reject passwords with spaces and various special characters. In some cases the special characters that are not accepted might be an effort to avoid attacks like SQL injection that depend on those characters. But a properly hashed password would not be sent intact to a database in any case, so such precautions are unnecessary. Users should also be able to include space characters to allow the use of phrases. Spaces themselves, however, add little to the complexity of passwords and may introduce usability issues (e.g., the undetected use of two spaces rather than one), so it may be beneficial to remove spaces in typed passwords prior to verification.

Users’ password choices are very predictable, so attackers are likely to guess passwords that have been successful in the past. These include dictionary words and passwords from previous breaches, such as the “Password1!” example above. For this reason, it is recommended that passwords chosen by users be compared against a “black list” of unacceptable passwords. This list should include passwords from previous breach corpuses, dictionary words, and specific words (such as the name of the service itself) that users are likely to choose. Since user choice of passwords will also be governed by a minimum length requirement, this dictionary need only include entries meeting that requirement.

### A.4. Randomly-chosen Secrets

Another factor that determines the strength of memorized secrets is the process by which they are generated. Secrets that are randomly chosen (in most cases by the verifier or CSP) and are uniformly distributed will be more difficult to guess or brute-force attack than user-chosen secrets meeting the same length and complexity requirements. Accordingly, at LOA2, SP 800-63-2 permitted the use of randomly generated PINs with 6 or more digits while requiring user-chosen memorized secrets to be a minimum of 8 characters long.

As discussed above, the threat model being addressed with memorized secret length requirements includes rate-limited online attacks, but not offline attacks. With this limitation, 6 digit randomly-generated PINs are still considered adequate for memorized secrets.

### A.5. Summary

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 throttling are more effective at preventing modern brute-force attacks. Therefore, no additional complexity requirements are imposed.