As many users and companies have heard, the National Institute of Standards and Technology (NIST) introduced some pretty significant changes to password guidelines in 2017. There have been many articles supporting these changes and they have been hailed as overdue.

So, if these new guidelines are popular and already multiple years old, why haven’t more companies implemented them? Let’s take a look.

## Minimum Characters

Actually, this has not really changed. Instead the recommended length for passwords has increased; the revised recommended limit is up to 64 characters, and in some cases more. This is so users have the capability to use long passphrases and/or passwords comprised of several words. But the minimum password length is still 8.

The problem with 8 character passwords is the required complexity for shorter passwords. Creating an 8 character password with at least one upper and lower case letter, number, and special character that is easy for the user to remember is challenging for the average user, especially when these requirements apply to the multitude of passwords a user is required to maintain.

Users are/were writing them down, forgetting them and constantly having them reset, re-using them across multiple websites/applications, and/or changing only one character, digit, or symbol when forced to change them. Password crackers are/were being created to look for common substitutions for easy passwords - so this type of software is immediately looking for Password1, P@ssw0rd, P@ssword1, etc. Thus, even though these passwords meet the complexity rules, they are not considered secure passwords.

Regardless that the minimum remains 8 characters in the new NIST guidelines, these guidelines are targeted at using long passphrases rather than advocating less complex 8-10 character passwords.

The new NIST guidelines *could* eliminate the problem of people writing down their passwords, as they allow for passphrases such as “night pretty glass determines” or “healthluminatesmobilecouch” – up to 64 characters. Users can still add capitals, numbers, and symbols (such as the spaces) but they don’t have to.

But this change introduces two main problems. First, although users can pretty much remember 4 words strung together, if they are managing 30 different passwords to get into websites and applications, it remains difficult to remember which 4 words go with which application or website. Further, users don’t like to enter 20+ character passphrases at every login.

Password keepers can still be utilized, however, many online systems are beginning to reject passwords that are entered very quickly as they cannot verify that it is a human entering the password versus a program. Thus, humans are thwarted as well from using the Paste function when entering a password. Further, having browsers remember passwords is a generally insecure practice and therefore not an alternative to password keepers. The result is that users may be just as frustrated typing in longer passwords as with shorter more complex ones.

The second significant problem is that many applications are not set up to handle 64 character passwords and changing those systems over is not necessarily an easy or cost free endeavor.

## Password Dictionary

While the new password recommendations are for common word passphrases, NIST guidelines state that the words that make up a password or passphrase still must not contain:

1. A series of the same letter or number repeated (“AAAAAAAA” or “11111111”), or sequential letters or numbers (“ABCDEFGH” or “12345678”)
2. Your username, the system name, the company or website name, or combinations of these
3. Personal information about you (PII), such as birthdates, children or pet names, addresses, ages, etc.
4. Passwords in the “Prohibited Password Dictionary”

Again, there are two main problems introduced here. The first is that companies will need to create and maintain their own Prohibited Password Dictionary. There are some lists online that can be downloaded (that include common insecure passwords like Password1, P@ssw0rd, 12345678, etc.), but before they can be used they will need to be updated with:

* PII type information (usernames, birthdates, names including children’s names, etc.) for employees
* Company and company system/application related data
* The list of any company passwords that have been compromised in the past

so that users don’t include any of this type of information in their passwords/passphrases.

The second problem is how to maintain and enforce such requirements. Will the company have the resources to keep the list updated with the latest “bad” passwords? How will all the systems/applications consult the list and enforce compliance to it?

## Emoticons

NIST now recommends using emoticons and other non-standard character types, “when possible.” Again, this will be a challenge for many systems, old and new.

## 2FA and MFA [used here to mean more than 2]

Further, in lieu of password guidance based on data classification (public, private, sensitive, etc.) NIST has made a recommendation for Multi-Factor Authentication (MFA) “in all but the least sensitive applications.” MFA (as used here) is at least a step above Two-Factor Authentication (2FA), which is simply something you have (card, token, SMS code, etc.) + something you know (password, code, etc.).

The main problem here is that many companies aren’t even to the point of 2FA, much less implementing MFA. In addition, many companies with 2FA only implement such ‘higher’ authentication on critical or sensitive systems.

## Password Reset

One of the most popular changes is an easement of password changing requirements. NIST recommends that passwords be changed only if they are forgotten or compromised. But again, there are caveats, including the ones already listed above.

The NIST assumption here is that the passwords/passphrases being created are already long and strong (and not prohibited). Also that they are not being used to access multiple systems/websites. And, of course, that MFA is implemented.

Yet in just the past two years there has been a significant rise in the number of security breaches that have gone undetected for months. Indeed, the latest Real Estate scam, prevalent since 2018 and increasing, relies on the hacker gaining undetected access then sitting back, watching and waiting for the opportunity to redirect wired funds.

So the question of how companies will know exactly when a password/passphrase has been compromised is a very valid one.

## Conclusion

The NIST guidelines are designed to make authentication more secure, and when implemented all together with the proper user training, are generally accepted as doing so. In addition, these new guidelines are popular because they are also geared towards making authentication easier for users.

However, many users/companies are attempting to implement only the guidelines related to complexity and expirations. They are not requiring longer and stronger passwords or passphrases, they continue to have password reuse across multiple applications/websites, and behavior on the Internet and regarding suspicious emails has not suddenly gotten better in the process.

Many users can already choose to implement 2FA on multiple websites nowadays with their personal accounts. Still, banks and other similar websites had to actually mandate 2FA authentication due to low voluntary adoption. In short, users remain the weakest link.

The new NIST guideline changes all together are:

* Length—8-64 characters are recommended.
* Character types—Nonstandard characters, such as emoticons, are allowed when possible.
* Construction—Long passphrases are encouraged. They must not match entries in the prohibited password dictionary.
	+ Reset—Required only if the password is compromised or forgotten.
	+ Multifactor—Encouraged in all but the least sensitive applications.

The use of the words “recommended” and “encouraged” here does not mean these are optional. These are guidelines and it is only when they are all implemented together that they constitute good security practices.

Thus, companies that would like to implement the NIST guidelines first need to perform a risk assessment on any and all changes to password rules to determine if those changes will actually make them more secure. A plan that includes user training and awareness should be designed and implemented along with such changes.

But until such time as a company adopts NIST’s new guidelines, password requirements for compliance should remain as detailed below (and companies should consider to have them remain in effect in perpetuity for all 8-10 character passwords, regardless of the new NIST guidelines).

* Minimum of 8 characters (character length\*)
* At least one upper case letter, one lower case letter, one number, and one special character\*
* Change at minimum every 90 days\*
* Do not use PII, company info (including usernames), consecutive numbers/letters, or known bad passwords\*
* Cannot use last 4 passwords over again
* Lock out after 3-5 unsuccessful attempts (be able to specify duration of lock out)
* Force password change after reset by admin, including first login
* Minimum age of 30 days (before the user can change their password again)
* Passwords stored with non-reversable encryption
* Do not use the same password for multiple applications/websites
* Default passwords must be changed upon software/hardware first use

\*Updated NIST guideline exists

Note that if any system/application in scope for regulation compliance cannot enforce all these requirements, enforcement of the remaining requirements will need to be performed outside the system by compensating controls.

**Questions? Comments?**

**Contact Us today**:

**Author: Karen Chamberlain:** karen@hmscs.com

**Amy McNeeley:** Amy@hmscs.com

**Kathy Mortensen:** Kathy@hmscs.com

**Stuart Siegel:** Stuart@hmscs.com