1Password

9 principles for a better company password policy

Research by Acronis shows that 80 percent of businesses don't have a password policy. Yet every company relies on passwords. Some employees have different logins for every device, app and website. Others access everything through a Single Sign-On (SSO) service. If any password is weak – even one – it could allow an attacker to slip past your company's defenses. That's why it's critical that your business has the right password policy in place.

80% *of businesses don't have a password policy*

Ask yourself two questions when crafting these rules: Are they strong enough to thwart potential hackers? And will employees actually follow them? Because if they're too weak, your company will still be exposed. And if they're too complicated, many employees will shrug their shoulders and continue to use weak passwords, or re-use the same password for all of their corporate devices and accounts.

If you're struggling to find that balance, or not sure where to begin, this guide will help.

Every password needs to be different

As a general rule, passwords should never be reused. If an employee uses the same set of characters to log into everything, they're putting your business at risk. Imagine they signed up for a new social network at home. Then, six months later, that service was breached and every user's password was leaked onto the internet. Criminals could theoretically discover the affected employee's password and use it to log into their work accounts.

According to Acronis, this 'password stuffing' strategy was the second most common type of cyberattack in 2020. Unique passwords will protect your employees but it can be tough to enforce them, especially if your company doesn't use SSO or an identity and access management solution (IAM). If you adopt a password manager, however, everyone can generate strong, unique passwords for every account and then autofill them across all of their work devices.

Ban common passwords

The most common passwords include "123456," "qwerty" and "password." They're easy to memorize but also simple for a hacker to guess. Research shows that many employees also use the company name or the service they're logging into as inspiration for their passwords, which are equally predictable for cybercriminals.

Top most common passwords of the year 2020

Password	Time to crack it
123456	Less than a second
123456789	Less than a second
picture1	3 hours
password	Less than a second
12345678	Less than a second
111111	Less than a second
123123	Less than a second
12345	Less than a second

You can eliminate common passwords by creating a ban list. As the National Institute of Standards and Technology (NIST) explains in its Digital Identity Guidelines, it could include dictionary words, passwords that have shown up in old data breaches, and anything that uses repetitive or sequential characters, such as "aaaaa" and "123abcd." You might be able to enforce your ban list via an SSO service, password manager, or mobile device management (MDM) solution. If not, you should let everyone know that you've created a list and where they can find it.

Most passwords should be fairly long

Longer passwords are always better. Why? Because each character makes it harder and harder for a hacker to crack with a brute force attack. Microsoft recommends a minimum length of eight characters — a number that many people don't adhere to, according to research by Safety.com. If you choose a higher number, Microsoft warns, there's a chance some of your employees will default to something predictable like "passwordpassword," or write their password down in an unsafe place.

67.3%

of survey respondents said their average password was equal to or less than eight characters long.

19.3%

of respondents said their average password was fifteen characters or more.

But that's where an enterprise password manager comes in. The best will suggest a long and unique password every time your employees sign up for something new. The password manager will then remember that piece of information and autofill it any time they need to log in. If your team has a password manager, it's just as easy to use a 50-character password as it is to use a five character one. As such, we see no reason why you shouldn't use a higher minimum password length of 15 or 20 characters.

Numbers and symbols should be optional

It's true that numbers and special symbols add to a password's complexity. But they're not essential. Employees can achieve a similar or greater level of complexity by extending the length of their passwords instead. Yes, you could enforce both a minimum length and the use of numbers and symbols. But consider these two password policies and how your team would react to them:

1) All passwords must be 15 characters long
2) All characters must be 12 characters long and contain at least one number and symbol

The second password policy sounds more complicated. And if an employee thinks a rule is inconvenient, they'll be more likely to rebel and use a weak password instead. Don't take the risk and keep your policy as simple as possible, while maintaining a high level of security for your business.

Demand passphrases

There will always be some passwords that your staff need to memorize. The password for their company laptop, for instance, or the one required to unlock their password manager. In these instances, the type of password we normally recommend – one that's composed of random characters – won't be realistic, because it's simply too difficult to remember. If you try to enforce it, many people will either write their password down, which isn't very safe, or revert to something weaker.

Instead, you should recommend passphrases. These are created by combining a handful of real but unrelated words. A passphrase could be “ball-orange-moon-car,” for instance. As long as each word is random, the complete passphrase will be difficult for an attacker to crack. We recommend setting four or five words as a minimum passphrase length. You can set a higher word count, but that will make the phrases more difficult to remember and potentially put off employees.

Baroness-Crab-Snorkle-Cheesy

Pigsy.Drool.Pancake.Handbag

Forsaken-Toggery-Grandma-Lettuce

Cupcake.Shark.Perfume.Bulldoze

Skunk-Tippet-Hillock-Horn

Forget about expiration dates

Many companies force their employees to change their passwords on a 30- or 60-day basis. But you don’t need to make this part of your policy, because a strong password is a strong password. It’s like hiring a world-class boxer to guard a nightclub, only to fire them and hire a different but equally capable boxer the following month. The account is still protected but the level of security hasn’t changed, and in the process you’ve added a small inconvenience for employees.

Microsoft and the UK’s National Cyber Security Center both advise against setting a rule like this. Research by the University of North Carolina has shown that people usually comply by switching, adding or deleting a single character. They’re the easiest changes to make, after all. But as Microsoft explains, an attacker can easily predict the new password based on the previous one. Instead, make it a rule that a password only needs to be changed if it shows up in a data breach.

Employees forced to change passwords will take the easy way out

Password	Revisions
123456	!23456
123456789	987654321
picture1	p!cture$1
password	p@$$w0rd
qwerty	123456
111111	000000

Adopt multi-factor authentication

Team members should use two-factor authentication (2FA) wherever possible. It's an extra layer of security that protects accounts from would-be attackers who have managed to find or deduce an employee's password. Here's how it works: employees can ask for a 2FA code to be sent any time they sign into an account – it could be via email, a dedicated authentication app, or text message (though we don't recommend using SMS as it's vulnerable to interception). They'll be asked to submit this code to prove their identity when signing in.

An attacker is unlikely to have access to both the account password and the place where the employee retrieves their 2FA codes. Many password managers and SSO providers will let you check whether staff are using 2FA. It's a good idea to enforce this level of protection for accounts that can access business-critical information. You could also extend the rule to all apps and services that offer 2FA. Nobody likes disruptions, so make sure your employees have the tools and training required to submit 2FA codes as conveniently as possible.

Ensure your policy is a success with 1Password

Many people are resistant to change. They might have used the same password for years and never knowingly been hacked. The easiest way to convert them is with 1Password. Long and unique passwords? 1Password can create these in a flash and remember them on your employees' behalf. Authentication codes? 1Password can generate and autofill these too. Watchtower will also tell employees when a password has been leaked and needs to be updated.

Writing a password policy is one challenge; enforcing it is another. With 1Password Business, you can create custom policies that enforce good security habits. You can require that everyone use a standalone 2FA app when they unlock 1Password, for instance. 1Password Business and Teams can also generate breach reports that show whether any company email address has been affected by a known data breach. You can then follow up with affected employees and explain why their updated password should follow your policy.

Be patient and transparent with your staff

You should expect some push-back when you implement a new password policy. (Yes, even if you introduce a password manager like 1Password.) And, as technology changes, there's a chance that you'll need to update your policy in the future. Talk to your employees so they understand why your company's rules are changing. Answer their questions and provide training if they've never used a password manager before. If you're patient and transparent, you can get your whole team onside and ensure everyone is working to keep your business secure.

Visit 1Password.com/business to sign up for a 14-day free trial, or contact the 1Password Sales team to find out how to get started. Follow 1Password on Twitter and LinkedIn, and keep an eye on the 1Password blog for product and company updates.