1Password

SECURITY 101

A CHECKLIST OF BEST PRACTICES FOR YOUR BUSINESS

Getting the basics right when it comes to security could not only save you time and money, but also the reputation of your business.

This checklist is a great starting point for laying solid foundations for security success and reducing the risk of cybercrime to your business. You can also use it as a point of reference when reviewing the policies and procedures you already have in place.

But, of course, every business is different. Any best practices should be tailored to fit the unique needs of your business.

Guiding principles

Before we jump into the actions you can take, let's quickly cover the guiding principles of a solid security strategy. These will act as your guiding light every step of the way – from developing your security policies to designing your training programs.

Create a culture of security

*According to a recent survey, **91%** of workers understand the risk of password reuse, but **66%** admitted to doing it anyway.*

Security relies on everyone across your business – only people can bring together all of the elements of a security infrastructure and make it work. To make that happen, security awareness alone isn't enough. Security needs to become embedded in your company culture.

That's the essence of a "culture of security."

By nurturing a security-first mindset, you can protect the business and its customers and increase overall productivity by letting employees work the way they need to – while staying secure in the process.

Culture vs awareness

Awareness	Culture
The knowledge of threats and the defenses and protections in place.	Individuals understand security and the role they play in it, along with the associated attitudes towards security and how that impacts their actions.

> *Security culture is what happens with security when people are left to their own devices. Do they make the right choices when faced with whether to click on a link? Do they know the steps that must be performed to ensure that a new product or offering is secure prior to ship?*
>
> **Chris Romeo**
> CEO of Security Journey

A strong security culture is supported by tools and processes that promote success, like support from the security team, open communication, technical controls, and productivity software.

For more in depth guidance on creating a culture of security, download our guide **The guide to creating a culture of security.**

Limit access to limit risk

The principle of least privilege is a security practice that restricts users to the minimum levels of access necessary to perform their work. To make this work, you need to shift your mindset from what might be inconvenient for employees to what is convenient for attackers, and security vulnerabilities in general.

Why? Because we're all human. Even with a deeply embedded culture of security, people are still caught out or make mistakes. These things are inevitable. In fact, attackers rely on it.

When you limit access to secrets, you reduce the risk of them being leaked or maliciously obtained. You also limit the damage they can cause.

Essentially: You can't abuse, misuse, or lose something you don't have.

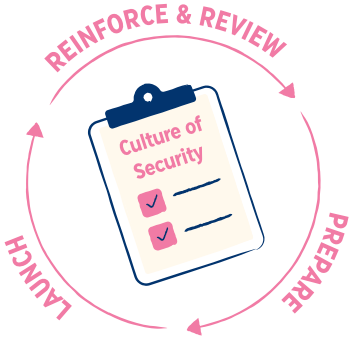
Make the secure thing the easiest thing to do

As you build your security strategy, focus on reducing risk, not eliminating it. Any security policy only works if your employees buy-in, and your organization molds better security habits from top to bottom. Complete adoption is crucial, and the only way to achieve that is by making the secure thing the easiest thing to do.

Security teams play a key role here. By being mindful of how they can support employees, making themselves accessible, providing the right tools, and setting standards with technical controls, they can empower employees to work securely – and keep the business safe as a result.

Best practices checklist

Business security is a holistic, ongoing effort that requires preparation, implementation, and reinforcement.



Use this checklist to start building the foundations for a culture of security:

Prepare

Documentation

- [ ] Write and document policies. **Consider including:**
  - [ ] Password policy.
  - [ ] Email policy.
  - [ ] Internet usage policy.
  - [ ] BYOD (bring your own device) policy.
  - [ ] Remote working policy.
  - [ ] Incident remediation policy.

> *Documenting protocols and expectations is essential for security. Consider what you're trying to protect and the biggest risks to that asset.*
>
> **Harlie Hardage**
> Senior Security Specialist, 1Password

For further guidance and a more comprehensive list, visit the SANS Institute.

- [ ] If you already have defined policies, revisit them to make sure they're still up-to-date, relevant, and reasonable.
- [ ] Make sure employees know who is responsible for security within your business and how to contact them if there's a problem.
- [ ] Define what access your users need, so that they can only access the information, systems, and tools they need to perform their role.

Tips for writing your security policies

Remember other obligations you must meet (regulatory requirements, certifications, and customer expectations) when writing these policies.

You can always add to them later, but you should use this as an opportunity to assess your business goals and how security is needed to mitigate risks. Your policies should align with these aspirations.

Training

- [ ] Create training content. **Consider covering:**
  - [ ] Safe password practices.
  - [ ] Phishing and social engineering.
  - [ ] Shadow IT.
- [ ] Develop new onboarding resources.

Education and a well-designed training program is key to building a culture of security. Create content that caters to multiple learning styles, and use mindfulness techniques to support rule-based training. Along with education, open conversations about what people want to learn, and how you can support them.

Provide the right tools

- [ ] Invest in productivity tools that make the secure thing the easiest thing to do.

> *By offering productivity tools that support security policies, not only do the tools make security-minded decisions simple, they increase productivity and show the security team genuinely wants to help people - and the program - thrive.*
>
> *If individuals believe you care about their success, and it's effortless to contribute to security, most people will opt in.*
>
> **Harlie Hardage**
> Senior Security Specialist, 1Password

- [ ] Introduce a password manager or identity access management so that employees can only access the information, systems, and tools they need to perform their role.
- [ ] Choose the right password manager.

Creating unique, complex passwords for every account is tedious without the right platform – pushing people to fall into coping strategies like using short passwords, easy to guess passwords, and reused passwords.

You'll need a password manager that integrates easily with existing tools, secures employees without getting in the way, is easy to manage, and creates strong passwords with just a click.

Choose the right password manager

> *Not only does 1Password make it easy for employees to follow good password practices, it helps reinforce your access control policies. If you forget to remove access to a portal, 1Password acts as a second line of defense when offboarding employees.*
>
> *1Password also makes it easy to grant access to credentials when a new employees joins your organization.*
>
> **Harlie Hardage**
> Senior Security Specialist, 1Password

- [ ] Enable two factor authentication for all accounts, where it's available.
- [ ] Make sure you have access controls in place.

> *We believe our teams are responsible and security-minded, and part of that is trust, but the other part is knowing we're giving them the right tools for the job.*
>
> **Joao Fernandes**
> IT Systems Engineer, Intercom

Technical controls

Determine the technical controls required for your business and appropriately mitigate the highest risks for your business.

- ☐ **If you have an intranet:** include protections like firewalls, network device hardening, and implementing proper network segmentation.
- ☐ **For endpoint management:** antivirus software, disk encryption, and ensuring devices are staying updated are essential.
- ☐ **Consider device management programs:** Depending on the size and complexity of your organization's device inventory, you might also need to consider device management programs.
- ☐ **Back up data:** Make sure that essential data is backed up, are recent, and can be restored.
- ☐ Install the latest software on devices and enable automatic updates.

The technical requirements needed will vary based on an organization's infrastructure and the assets you are trying to protect, so carefully assess your needs to develop a cybersecurity program that fits your organization.

Launch

- [ ] Hold an all hands kick off event so that everyone knows about your new security strategy.
- [ ] Roll out your chosen password manager.
    - [ ] Make it available to employees so that they can create and use strong passwords.
    - [ ] Give employees only access to the information, systems, and tools they need to perform their role.
- [ ] Incorporate your new training resources into your onboarding program, so that employees are empowered to work securely from day one.
- [ ] Have monthly team meetings with interactive activities to reinforce learnings.
- [ ] Build company compliance into reviews.
    - [ ] Review compliance to rules and policies.
    - [ ] Assess employee attitudes towards security, social norms, and day-to-day behaviors.
- [ ] Course correct slow adopters.
    - [ ] Use insights from tools and surveys to identify slow adopters.
    - [ ] Create resources to help them course correct.

Reinforce

- [ ] Regularly review and audit employee access.
  - [ ] Revoke access that is no longer needed.
- [ ] Introduce gamification awards for active security contributors.
- [ ] Periodic training with interactive activities to reinforce learnings and best practices.

> *Regular training sessions help to build a culture of security within your business. If you only hold remedial training, and wait until something bad happens, it can create negative connotations about security for employees.*
>
> *When security training is regular, slow adopters won't feel called out either – it becomes the norm.*
>
> **Harlie Hardage**
> Senior Security Specialist, 1Password

- [ ] Monitor. Tweak. Repeat.
  - [ ] Schedule regular time slots throughout the year to review policies, training documentation, onboarding resources, tooling and make improvements.