FACT SHEET

New Employee Onboarding Data Security Checklist

Have you recently welcomed new starters into your organisation? If so, it is critical to address information security from the start of their employment. Employee error or carelessness is a prime cause of data breaches and a thorough orientation can go a long way toward mitigating risk. Managers and leadership teams can help build and reinforce a company's total security culture by outlining strategies and ensuring employees recognise their roles in keeping data safe.

DID YOU KNOW?

Almost half (49%) of business leaders surveyed indicate that the lack of understanding of the threats and risks to the organisation is the biggest barrier to employees following information security policies.[1]

Here is a checklist of information security topics, both electronic and paper-based, to review during onboarding.

☐ **Information security regulations.**
Data breaches can result in fines and damage a company's reputation. Acquainting employees with the key aspects of relevant data security laws can provide valuable context to important data security discussions.

☐ **Incident reporting.**
Despite a business' best efforts, a data breach may still occur. Employees should know when and how to report these events and be assured they will not be penalised for speaking up. Make sure to inform your new starters of perceptions and expectations on incident reporting from the outset, so that new and current employees alike understand how to react if a data breach were to occur.

☐ **Printing procedures.**
Common mistakes, such as inadvertently leaving confidential documents out in the open around places like printers, increases the risk of data breaches. It is vital to reinforce the importance of quickly retrieving printed materials from the printer as this can reduce the likelihood of stolen information. If your business password protects its printers, don't forget to educate new employees on how to access and preserve the security of those passwords.

☐ **Electronic device policies.**
Personal mobile phones and tablets in the workplace are convenient but they can pose an increased risk for security incidents. When onboarding new employees, ensure they understand how to protect their devices at all times.

Source: 1. Shred-it Data Protection Report, 2021.

We protect what matters.

Shred-it®
A Stericycle® Solution

☐ **Keeping a clean desk.**
If your business has an official clean desk policy, you should explain exactly what that means for new employees. Typically, this requires employees to lock up all papers that display confidential information; remove non-essential documents from the top of the desk; and activate the computer's lock-screen before leaving for an extended time or at the end of the day.

Click here for a Clean Desk Policy.

☐ **Comprehensive document disposal.**
New employees must have a clear understanding of how to properly dispose of your business' documents. Informing new employees of your existing document disposal procedures can help mitigate risks and limit data protection complications. It may be best to introduce a Shred-it All Policy and advise them to dispose of all documents in a secure console to ensure secure destruction. This will take the guesswork out of what may be confidential or not. Not only does this help with the security of confidential documents, but given that all shredded paper is recycled, it is also best practice in terms of sustainability.

Click here for a Shred-it All Policy.

☐ **Password protocols.**
Passwords are an essential security precaution. New employees should be fully briefed on your organisation's password policy and know what it means to create strong passwords. A good password incorporates upper and lowercase letters, numbers and symbols, and must be updated regularly. If your business has a mandatory password update programme, make sure new employees are aware.

☐ **Email precautions.**
Cybersecurity incidents often happen because of employees clicking on emails they shouldn't. New employees should be trained on how to recognise suspicious emails, including malware, phishing schemes and ransomware, so they can learn to avoid harmful situations.

To learn more about best practices for information security visit shredit.co.uk or call 0800 197 1164.

We protect what matters.

Shred-it®
A Stericycle® Solution