FACTSHEET

New Employee Onboarding Data Security Checklist

When welcoming new employees, it is critical to address information security from the start. 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 administrators can help build and reinforce a company's total security culture by outlining strategies and ensuring staff recognize their roles in keeping data safe.

DID YOU KNOW?

Nearly half (47%) of C-suite leaders and 31% of small business owners say that human error or accidental loss by an employee was the main cause of data breaches in their organizations.[1]

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

- **Information security regulations.** Different business sectors, including finance, healthcare and legal, are heavily regulated. Violations can result in fines and damage a company's reputation. Acquainting employees with the key aspects of relevant data security laws, such as the Gramm-Leach-Bliley Act (GLB Act), the Health Insurance Portability and Accountable Act, and the Sarbanes-Oxley Act (SOX) can provide valuable context to important data security discussions.
- **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 important to reinforce the importance of quickly retrieving printed materials from the printer as this will reduce the likelihood of stolen information. Posting reminders by printers and/or on computer desktops can further emphasize this point. If your company password-protects its printers, don't forget to educate new hires on how to access and preserve the security of those passwords.

NEW EMPLOYEE ONBOARDING DATA SECURITY CHECKLIST

- **Keeping a clean desk.** If your company has an official clean desk policy, you should explain exactly what that means for staff. 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.

- **Comprehensive document disposal.** New employees should have a clear understanding of how to properly dispose of documents. A *Shred-it-All* Policy advises organizations to dispose of all documents in a secure console to ensure secure destruction. This policy is recommended because it takes the guesswork out of information disposal and establishes secure document destruction as the norm. 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.

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

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

- **Electronic device policies.** Organizations sometimes encourage employees to use their own cell phones and tablets in the work environment. While convenient, it can pose an increased risk for security incidents. New employees should understand how to protect their devices at all times. In addition, staff should know the proper way to ensure complete destruction if equipment needs to be retired.

- **Incident reporting.** Despite an organization's best efforts, a data breach may still occur. Staff should know when and how to report these events and be assured they will not be penalized for speaking up.

Source: 2019 Data Protection Report, USA, Shred-it

To learn more about best practices for information security when onboarding and training new employees, visit **Shredit.com** or call **800-697-4733**.

Shred-it®