Data Confidentiality Employee Handbook

Many of our customers acknowledge that the best way to secure data is to educate employees themselves. Most data breaches happen due to human factors. Yet, few organizations manage to educate their employees effectively. We wanted to help system administrators by providing a simple, portable template for employees. That's why we created the Data Confidentiality Handbook template so you don't have to start from scratch. We asked system administrators that use AeroFS what documents they provide to their employees. This guide builds on these documents and conversations.

First Things First

Before you get started on your data confidentiality initiatives, here are some action items to keep in mind:

- Find out what applications your employees are using for file sharing and collaboration
- Determine what types of information is being shared internally and externally
- Train your team on best practices for secure collaboration
- Create a Data Confidentiality Handbook and share it with your employees
- Encourage employees to be active participants in keeping company information confidential

Print and distribute the next two pages to your employees.

It's your handbook.

ABOUT AEROFS

AeroFS delivers highly secure, enterprise-class file sharing and synchronization solutions that enable enterprises to better control and secure their data and increase collaboration among users. Like Dropbox and other online file-sharing offerings, AeroFS allows users to simply drag and drop files into a folder to sync and share them with colleagues and external partners. Unlike those offerings, however, AeroFS is deployed on the enterprise's own infrastructure, and so enterprise data always stays under company and IT control. Files are shared directly between users' devices, and enterprise data never resides on AeroFS servers. The company is funded by blue-chip investors, including Avalon Ventures, Andreessen Horowitz, Y Combinator, NHN Investment, and others.

Learn more at aerofs.com.

Why Our Data Must Be Kept Confidential

A company where data is not kept confidential may suffer in many ways.

Loss in revenues

- The company may lose contracts because existing customers lose confidence in the company's ability to keep their data private.
- The company may lose future contracts because new customers do not trust the • company with their data.
- The company may lose contracts because competition knows about their plans and secrets.
- The company may be the victim of frauders who know how to attack their systems

Increase in costs

- The company may have to compensate customers and employees if personal information was leaked.
- The company may have to pay government fines if they are legally required to keep data confidential.
- The company may have to pay for expensive security stop gap measures.
- The company may have to pay additional costs if partners find information they can leverage in negotiations.

Why You Are Responsible For Data Confidentiality

The company trusts you with the company's data because we want you to have a positive impact. In return, you are responsible to keep this data confidential. On top of the risks for the company, you personally can face legal and financial risks if you disclose the data.

LEGAL RISKS

Whether it is intentional or not, leaking confidential data may result in heavy fines and jail time.

FINANCIAL RISKS

In addition to legal costs, you may have to compensate for damages to the company.

On November 24, 2014, confidential data from Sony Pictures Entertainment was leaked on the Internet. The company set aside $15 million to deal with ongoing damages from the hack.

On November 5, 2014, Lyft sued a former employee after he allegedly downloaded documents to his personal Dropbox account.

Top Three Things To Do To Keep Data Confidential

Separate your personal and professional data

When possible, use different tools to separate your personal and professional life. Use a laptop for work, and a different laptop for home. Access your company data exclusively on your company laptop. If the company provides a phone, make sure you read your work emails on this device only.

If you have to keep personal and professional data on the same device, use different accounts of the same application. It might mean switching between accounts, but it will be worth it to avoid any potential confusion for where your data is being stored.

Improve security on your work applications

A few small improvements can improve drastically the protection of your data. You can do a few of these things:

- Use unique, sophisticated passwords in your applications. 'Iam!HappY12' makes it much harder for anyone to access your data, without making it too hard for you to type in.
- Use two-factor authentication when available. Most popular applications offer two-factor authentication, which requires you to confirm your identity with a mobile device every once in a while. This, combined with a strong password, will make your system much more secure.
- Lock down your devices with a password when you are not using them. Add passwords to your phones and laptops. Log out from your session if you are about to leave your desk.

Be aware of your sharing

It is important that you are aware of what data you share, and who you share it with. Keep in mind that the person that you share it with might not carry the same concern for privacy as you do.

All company's data is confidential. In particular, some data can be very sensitive:

FINANCIAL DATA

Revenues, profit, balance sheet

STRATEGIC DATA

Planning, hiring and layoffs, new products, intelligence

CUSTOMER DATA

List of customers, contact information, strategic data (Sony case > Snapchat)

EMPLOYEE DATA

List of employees, personal information, salaries

INTELLECTUAL PROPERTY DATA

Source code, trade secrets, processes