Microsoft

Cybersecurity Simplified: Sensitive data

In today's collaborative, work-from-anywhere world, files containing your company's sensitive information often leaves the four walls of your business. An employee may download a file to a USB drive to work on it at home. You may send financial information to your banker or accountant.

Wouldn't it be nice to control who can access these documents, even after they have been shared or saved outside your company? Now you can.

Microsoft 365 Business protects your sensitive documents

With Microsoft 365 Business, you can

- Limit access to files or email, so only employees or invited guests can access them
- Disable access to classified documents when an employee leaves the company

How it works

Control access to email. With Microsoft 365 Business, you can ensure that only the intended recipient of an email has access to the information, with controls like "Do Not Forward" or "Do Not Print". And for even more added security, you can easily encrypt an email message and its attachments, so it can only be read by the person you sent it to.

Control access to documents and files. Microsoft 365 Business allows you to restrict access to a file – a spreadsheet containing names and contact information of your customers, for example – so that it can be accessed only by people in your company. You can control whether that document can be edited, restricted to read-only, or prevent it from being printed.

You control

- Access to a document
- Who can edit a document
- If a document can be printed or forwarded

Restrict access, even if the file is saved outside the company – the restrictions and protections stay with the files and emails regardless of the location. Even if the file is emailed outside the company, or saved to an employee's personal computer, you remain in control of your data.

Here's an example

Megan is the Sales Manager for the Contoso company. She creates the company's annual sales forecast and classifies it as "Highly Confidential". This essentially locks the document, because at her company "Highly Confidential" files are automatically encrypted, and only accessible to company employees. After Megan shares the file with her team, Carlos, a Contoso sales person, attempts to open the file. When he opens the file, Microsoft 365 Business verifies that he is a Contoso employee, and decrypts the file for him. This verification occurs each time that the file is accessed.

This protection stays with the document even if it is saved outside the company. Let's say that Carlos saves the document to a USB drive, and then gets a job at another company. Even though Carlos still has Contoso's sales forecast, it is useless to him, because when he tries to open the file, he is unable to decrypt it, since he is no longer a Contoso employee.

The same technology used by many of the world's largest companies

The encryption and data protection capabilities included in Microsoft 365 Business are powered by Azure Information Protection, which many of the world's largest companies rely on to help control access to their data and documents even when that information travels beyond the boundary of the company's network. And since it is included as part of your Microsoft 365 Business subscription, there are no additional 3rd party solutions to buy, install, or manage.

Get started:

Learn more about Microsoft 365 Business at www.microsoft.com/microsoft365/business