Microsoft

Azure Information Protection

End user adoption guide

Contents

Information in this document, including URL and other Internet website references, is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Introduction

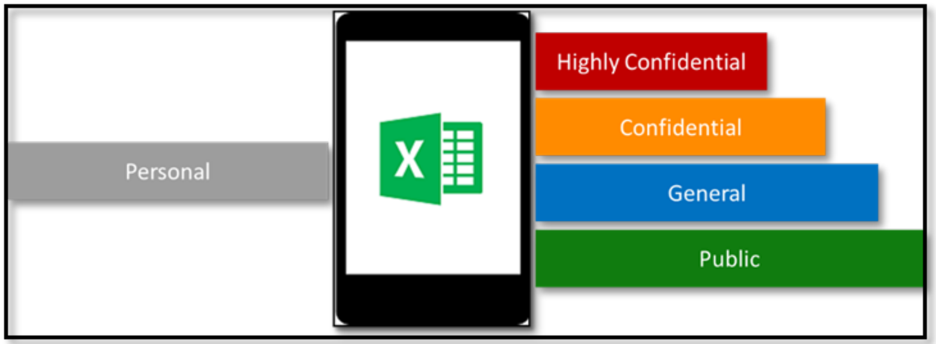
Data is traveling between users, devices, apps, and services more than ever before. Businesses are working with customers, partners, and remote or outsourced employees and sharing sensitive information inside and outside of organizational parameters. How do you know organizational data is safe? To ensure the protection of sensitive information, you need to start by identifying which data is sensitive, what kind of protection it requires, how to apply protection, and how to track usage of traveling data.

According to the Identity Theft Resource Center (ITRC), in 2016, US agencies and companies suffered 1,093 data breach instances. This is a record 40 percent increase over 2015. Information is a critical asset of any organization, and serious steps need to be taken to protect it from exposure and breaches.

The first step in overcoming these concerns about information protection is to classify the information's need for protection and implement policies and labels. Microsoft Azure Information Protection, a cloud-based solution, ensures persistent classification and protection of sensitive data no matter where it's stored or who it's shared with. It also provides end-to-end protection and control for sensitive data, including data classification and labeling, data protection, data usage monitoring, and responding to malicious data usage activities.

Classifying & protecting data

When information is accessed and shared, there's a chance of leaked intellectual property, customers' personally identifiable information (PII), financial information, health information, or sensitive company memos. Information classification and protection provides a framework to determine the appropriate level of security against unauthorized disclosure and breaches. You need to define classifications with standard recommended labels—Personal, Public, General, Confidential, and Highly Confidential—to handle different levels of information sensitivity and apply appropriate information protection.



Levels of information sensitivity

Protect sensitive information anytime, anywhere

Azure Information Protection helps you classify and label your sensitive data for protection throughout its lifecycle. It provides flexibility to integrate and protect Microsoft cloud services and applications like Microsoft Office 365, SharePoint Online, Exchange Online, and OneDrive for Business. No matter where your data is, information protection in the form of encryption, watermark, or DLP policies can be applied to sensitive data. Classification labels and protection are persistent, traveling with the data so that it's identifiable and protected always—regardless of where it's stored or with whom it's shared. With Azure Information Protection, you can meet your compliance and regulatory requirements, including FIPS 140-2, HSMs, ISO/IEC 27001:2013, SOC, HIPAA BAA, EU Model Clause, PCI DSS, and more.

With Azure Information Protection, you get:

- **Simplified and intuitive controls** that help you make the right decisions and stay productive. Data classification and protection controls are integrated into Microsoft Office and common applications. One-click options make it easy to classify data.
- **Persistent protection that follows sensitive data** to ensure it's always protected—regardless of where it's stored or with whom it's shared.
- **More visibility and control over shared data** through tracking of shared data usage with powerful logging and reporting that allows you to monitor and analyze this data. Access to data can be revoked if required.
- **Safer sharing with customers and partners** through definitions of who can access data and what they can do with it based on a use rights policy. For example, some users might be able to view and edit certain files but not print or forward them.
- **Deployment and management flexibility** to protect data whether it's stored in the cloud or on-premises. You can choose how encryption keys are managed, including Bring Your Own Key (BYOK) options.

This guide assumes that you've already implemented the deployment roadmap. If you haven't, complete the steps here and then configure Office 365 by following the steps here.

End user adoption—success guide

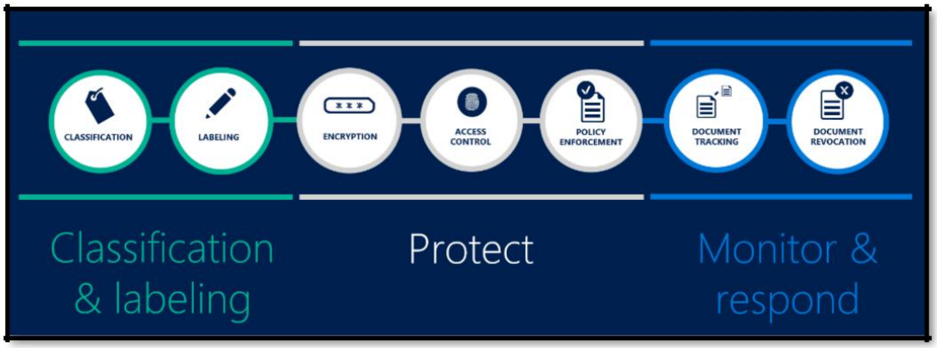
Implementing Azure Information Protection within your organization

Creating an information protection launch strategy requires complete organizational preparation—from developing a communication and awareness plan for end users to identifying power users who can help end users in adopting best practices for information protection. Let's start by considering the end-to-end information protection process that you can enable by using Azure Information Protection.

Defining Azure Information Protection to classify and protect information

Azure Information Protection provides classification, labeling, and protection to track and control how information is used. The following process enables your organization to identify sensitive information and define security and controls on data.

- **Classification and labeling.** Data can be classified based on content, context, and source, either automatically based on defined policies or manually by users.
- **Protect data.** Documents can be encrypted. Authentication requirements and definitions of use rights can be added to data.
- **Monitor and respond.** Users can track activities on shared files and revoke access in cases of unexpected activity.



Classify and protect information

Communications timeline for deployment

- T minus 15 business days: Review of the LT and org-wide communications, including approval of distribution dates and recipients. Participants in this review process will include all stakeholders.

- T minus 10 business days: Executive support and help desk briefed on the upcoming release details and equipped with information needed to answer user questions.

- T minus 7 business days: Leadership awareness communication sent to SLT (CVPs, EVPs, EVP Executive Administrators, EVP Chiefs of Staff, Office of the CEO) in affected organizations.

- T minus 1 business days: Organization-wide awareness communication sent to users in affected organization.

- T plus 7 business days: A communications analysis provided to stakeholders. This information will include email read and engagement stats and user feedback and questions. The information will be used to revise future communications related to the Azure Information Protection deployment.

Getting started checklist

Use this checklist as a guide through the process of planning, building, launching, and promoting Azure Information Protection to your organization.

Plan

✓ **Develop your vision.** Understand what's in it for the organization and develop a clear value proposition. This will be especially useful in pitching an adoption campaign to senior leadership.

✓ **Get senior leadership buy-in.** Socialize the idea with senior leadership first—give them a heads up, get approvals, and request their support and feedback on the adoption.

✓ **Keep it simple.** Develop a simplified security approach to enable quick and easy information-protection adoption across the organization. More security options or complex security options might lead users to the wrong choice or to making no choice.

✓ **Set policies and guidance.** Set up proper support channels and escalation paths for users who encounter issues or have questions. Work with leadership to develop a usage policy.

Build

✓ **Customize configurations for Azure Information Protection.** Customize classification labels to fit your specific business needs. If your company is already using a different data classification method or nomenclature, educate users on the upcoming change.

✓ **Engage deployment teams.** Engage the deployment teams early to get the apps packaged and distributed to endpoints. This includes the Azure Information Protection client and viewer apps.

✓ **Identify data stewards.** Identify a data steward in each group (HR, Legal, Finance, and so on) who will champion this effort and encourage secure behavior. Train these stewards to assist end users in assessing data's importance, value, and sensitivity, and in the handling and protection of data.

✓ **Start small by enabling a few test cases.** Starting with early adopters allows for feedback and optimization before Azure Information Protection is rolled out to the larger organization. Provide tools to onboard these users smoothly, including training and support channels. If your organization supports it, an internal website allows for two-way communication of feedback, questions, and support.

✓ **Develop a communication plan and materials.** Get the most out of your launch by making end users aware of and prepared for adoption. This should include emails, training materials, best practices, and FAQ. Create physical assets like posters, and digital assets like internal sites, directories, and TV screens available everywhere—in hallways, kitchens, cafes, and so on.

Launch and sustain

✓ **Raise awareness and launch to your network.** After a successful wave 1 launch and optimization, launch to the whole organization. Promote the launch with posters and e-signs throughout your organization. Consider setting up an in-person launch event to encourage adoption and answer questions.

✓ **Provide support.** Let users feel empowered. Offer tools to onboard them smoothly, like wizards and support channels, and encourage feedback to empower them during and after the launch.

✓ **Drive ongoing usage.** Develop a communication plan to share and monitor progress to keep the momentum going by encouraging open dialog, questions, and suggestions.

Power user guide

Get prepared to adopt Azure Information Protection

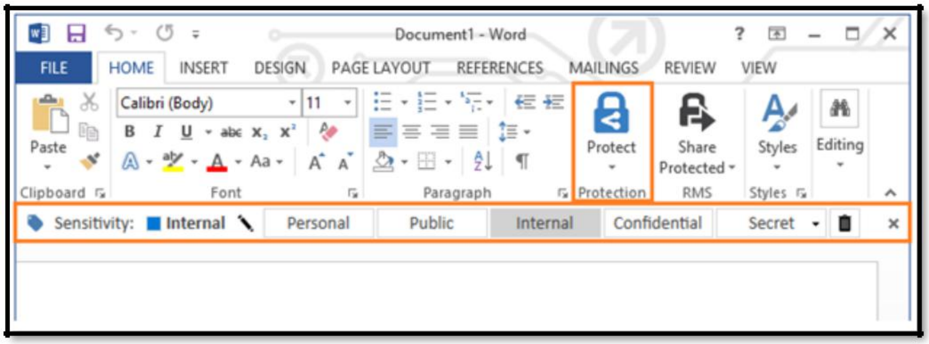
First, you need to understand the importance of information protection and how end-to-end information protection can be applied through Azure Information Protection. Next, you need to mentor end users so they can understand Azure Information Protection and follow best practices. The following steps will help you understand Azure Information Protection and how it can be used to protect your data.

Start with Microsoft Azure Information Protection client

Azure Information Protection client helps keep important documents and emails safe from people who shouldn't see them, even if email is forwarded or documents are saved to another location. Azure Information Protection client is used to classify documents and open documents that other people have protected by using the Rights Management protection technology from Azure Information Protection.

Default classifications and policies are defined at the organization level by the IT team and are enforced by Azure Information Protection client. Azure Information Protection client checks for any changes whenever a supported Microsoft Office application starts, and downloads the changes as its latest Azure Information Protection policy. Users must have Azure Information Protection client installed on their machines to define classifications and open protected documents. The client can be pushed centrally by the IT team to all employees. You can also ask users to download Azure Information Protection client from the Microsoft Azure website.

After the Azure Information Protection client is installed, a new Azure Information Protection bar will appear across Microsoft Office applications. This is used to classify and label sensitive documents.



Azure Information Protection bar

Intuitive data classification and labeling

To meet business requirements for information security, security policies are defined at the organization level in Azure Information Protection to enable data classification that will be automatically enforced whenever any document is created or modified. If an automatic classification needs to be changed based on the content type, you can do this by manually classifying the documents. Azure Information Protection provides predefined classifications, like Personal, Public, General, Confidential, and Highly Confidential. For user-driven classification, you can select the sensitivity label applicable to the document. Actions like visual marking of the document and encryption can be enforced based on the label. Labels are metadata that is embedded within the document in clear text so other systems can read it. Labels are persistent and travel with the document.

Defining classification labels and setting custom permissions[1]

- **Classification recommendations.** The Azure Information Protection toolbar recommends classification types based on the content available in the document you are creating or editing. These recommendations appear above the Azure Information Protection toolbar. You can change the suggested classification from there.

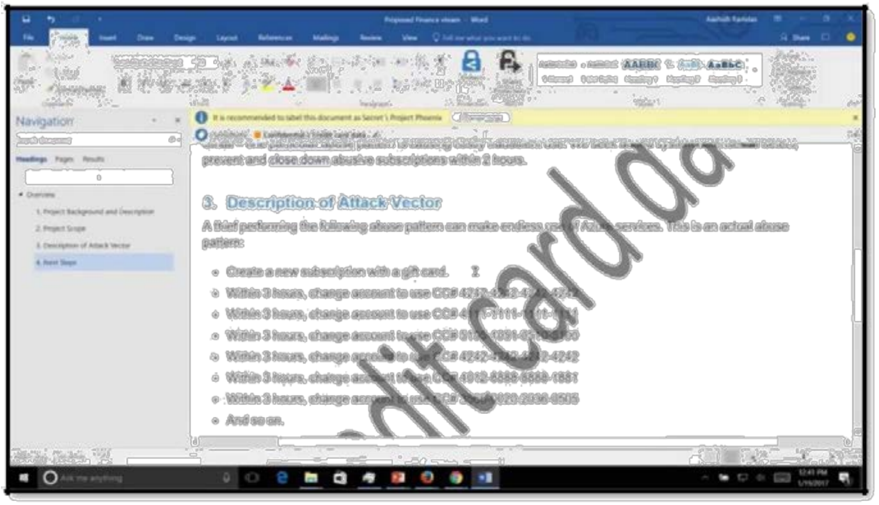
- **Automatic classifications.** Based on organizational information protection policies and the content in a document, Azure Information Protection automatically enforces the appropriate classification and labels for the document. Even if you don't specify a classification for your document before you save it, Azure Information Protection automatically applies a suitable classification.

- **Visual labels.** After information has been classified, visual labels like headers, footers, and watermarks are added to the document. These labels help users by making them aware of the sensitivity of the document at a glance.

- **Manual reclassifications.** To change the automatically enforced classification, you can reclassify the document manually. If you're changing the classification to a lower sensitivity level, you might be asked to provide an appropriate justification.

You can learn more about data classification and labeling in the Azure documentation and in this blog post.

[1] Actual classification labels and the ability to create custom labels are defined by your IT department.



It is recommended to label this document as Secret \ Project Phoenix

Confidential \ Credit card data

prevent and close down abusive subscriptions within 2 hours.

3. Description of Attack Vector

A thief performing the following abuse pattern can make endless use of Azure services. This is an actual abuse pattern:

- Create a new subscription with a gift card.
- Within 3 hours, change account to use CC# 4242-[illegible]-4242
- Within 3 hours, change account to use CC# 4[illegible]-1111-[illegible]
- Within 3 hours, change account to use CC# [illegible]
- Within 3 hours, change account to use CC# 4242-[illegible]-4242
- Within 3 hours, change account to use CC# 4012-8888-8888-1881
- Within 3 hours, change account to use CC# [illegible]-2030-0505
- And so on.

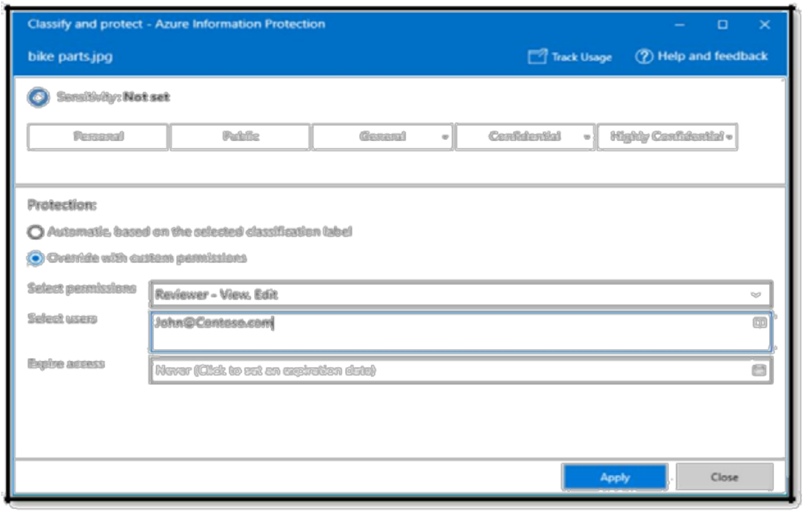
A watermark in a Word document

Persistent information protection

Protection can be applied to sensitive data once it has been classified or labeled. This includes encrypting the document, which requires authentication of the user and enforces user rights that define what can be done with the data. Protected files are potentially safe to share even outside the organization because recipients can view protected documents and emails but they can’t copy, print, or forward them.

Enabling safe sharing with customers and partners

- **Define access controls.** When information is shared externally, organizational policies automatically enforce appropriate information classification and labeling to ensure information protection. If you need to, you can also define your own access controls by making a copy of a file and using custom permissions to protect the file from within an Office application or File Explorer. You can then share the file by using your standard sharing mechanism—for example, as an attachment to an email or an invitation to a Microsoft SharePoint Online document.



Classify and protect - Azure Information Protection

bike parts.jpg

Sensitivity: Not set

Protection:

○ Automatic, based on the selected classification label

● Override with custom permissions

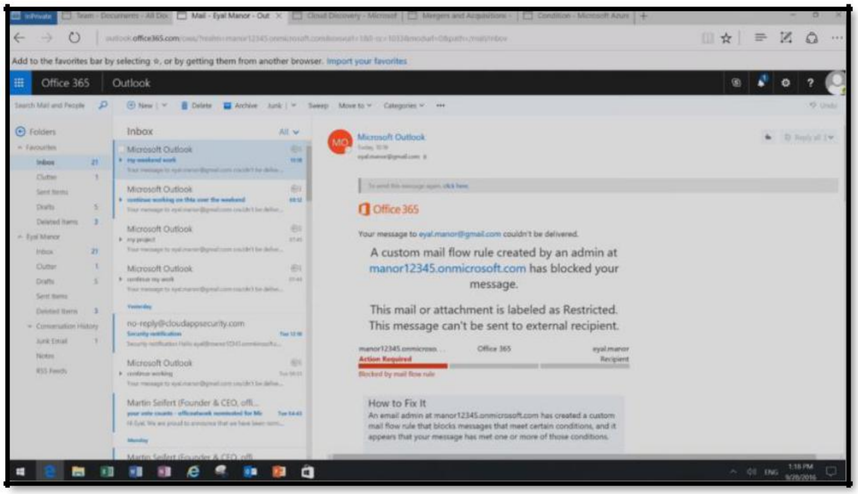
Select permissions: Reviewer - View, Edit

Select users: John@Contoso.com

Expire access: Never (Click to set an expiration date)

Defining custom access controls

- **Ensure persistent protection that travels with your data.** Azure Information Protection provides persistent protection even when sensitive information travels, either as an email attachment or through SharePoint. If you attempt to share internal sensitive information outside your organization, Azure Information Protection prevents you from sending the email and lets you know why the message has been blocked.



Office 365

Your message to eyal.manor@gmail.com couldn't be delivered.

A custom mail flow rule created by an admin at manor12345.onmicrosoft.com has blocked your message.

This mail or attachment is labeled as Restricted. This message can't be sent to external recipient.

How to Fix It

An email admin at manor12345.onmicrosoft.com has created a custom mail flow rule that blocks messages that meet certain conditions, and it appears that your message has met one or more of those conditions.

Message explaining blocked attempt to send attachment

- **Access Protected Information.** You can access a rights-protected file from File Explorer or as an attachment in an email message by simply double-clicking it. Enter your credentials if prompted by Azure Information Protection client to do so. The file opens in the application that's associated with the original file name extension, and a restriction banner is displayed at the top of the file. The banner might display the permissions that are applied to the file, or it might provide a link to display them. Open operations on the file might be audited and remain audited if the file is protected. If a file is accessed from a mobile email client that doesn't support viewing rights-protected messages, you can either use OWA or the Azure Information

Protection mobile app. This app also lets you view rights-protected PDF files, pictures, and text files

Learn More about setting custom permissions for a document.

Monitor and respond

After you share protected information, Azure Information Protection allows you to track activities on shared files. Rich logs and reporting tools are also available to help IT monitor and analyze data for compliance and regulatory purposes. If needed, you can easily revoke access to shared data. To ensure a timely response to suspicious activity, access to business data can be revoked either by end-users who want to revoke their own documents or by an administrator on behalf of any user.

- **Document usage tracking.** To track document usage for protected and shared documents, you can use a document tracking site that can be accessible from Windows computers, Mac computers, and even from tablets and phones. On this site, you can track who tried to open the files that you protected and whether they were successful—that is, whether they were successfully authenticated. You also see each time they tried to access the document, and their location at the time. This dashboard gives you visibility into:
  - Number of views on shared documents.
  - Unauthorized access attempts.
  - Last activity on your shared document.
  - Usage tracking based on geo-location.

  You can export this data to CSV.

- **Respond to suspicious activity.** If you detect suspicious activity on a shared document, like invalid login attempts or the same user account accessing shared information from different geo-locations, you can immediately revoke user access for the shared document. When you revoke access, the shared document isn’t deleted, but authorized users can no longer open it. If you want, you can also notify users that you’re revoking access to the document you previously shared by providing a customized message.

Learn more about tracking and revoking a protected document.

Summary

Azure Information Protection provides a comprehensive solution for protecting your organization’s sensitive data, from identifying the sensitivity of business data to protecting and tracking information usage. It helps you comply with organizational requirements for security and compliance. Protection can be enforced on sensitive information when a document is being created or modified, and users have the flexibility to reclassify information sensitivity when they have a justified reason. Users can define their own access controls when sharing information outside the organization and always track and revoke access even after a document has left the organizational perimeter.

FAQ—customizable example

Question	Answer
What are data classification labels?	They enable you to classify data based on source, context, and content at the time of creation or modification, either automatically or manually. Once data is classified, a persistent label is embedded in it, and actions like visual marking and encryption can be taken based on the classification and label.
Why did <company name> change the existing data classification labels?	<company name> changed the labels to make them more intuitive and to align them with industry standards.
Why do I need to classify my emails?	Enormous amounts of data and information are created and stored every day across <company name>. Properly classifying and protecting this data is critical to our business.
Do the new classification labels apply to all content and data?	Yes. Content and data created or edited in Microsoft Office products, on Microsoft SharePoint, and in Microsoft Outlook must be labelled.
Do I need to use the new information protection toolbar to label all the documents I’ve created over the years?	No, but if you edit an existing document you must classify it by using the toolbar.
What are the classification labels that <company name> is using?	Highly Confidential, Confidential, General, Public, and Personal. <insert any custom labels here>

How do I know which classification label to use for my content and data?	Visit the <classification labels page> to see descriptions and examples for each of the labels. The Data Classification Wizard and your <data steward> are also great resources to help you understand when to use each of the labels.
When do I need to start using the toolbar to label my content and data?	The new classification labeling must be applied to all documents created in Outlook and other Office applications starting on the day that the Azure Information Protection tooling is deployed to your computer. Previously created documents edited after the Azure Information Protection tooling is deployed to your computer must also be classified with the new labels.
What if I choose not to use the new classification labels?	Properly labeling all <company name> data is required of all employees and contractors/vendors.
How will anyone know if I choose not to classify my emails and documents?	The information protection tool will identify groups and individuals that don't classify data. This information will be provided to the appropriate managers.
Will the Data Classification Wizard be updated with new labels? If so, when?	Yes. The wizard is currently aligned to the new labels and can help you determine the most appropriate classification label for your content and data. If you believe a new classification label is required, please inform your <data steward>, post to the <Information Protection Yammer Group or other discussion forum>, or contact help desk.
How should I label my SharePoint sites when I have a mix of data that includes Confidential and Highly Confidential?	All data repositories—such as SharePoint sites containing mixed data—should be labeled in alignment with the highest data handled by the repository. In addition, if the site handles large amounts of data, you should consider raising the classification to the next highest level.

What is the Personal label used for?	The Personal label is for documents and emails that aren't related to <company name>. Examples: an email to your sister regarding a family party, a flyer for a volunteer event that isn't a <company name>-sponsored event, a spreadsheet containing an inventory of your vinyl albums.
How does personal data align with the labels?	Personal data, from a privacy perspective, can occur in any of the labels. Your best resource to answer this question is your <privacy manager>. You can locate your <privacy manager> here<include link>.
Who can I contact if I have questions about the labels, or if I have feedback related to the new classification labels and/or tooling?	If you have questions about the new classification labels, contact your <data steward>. Post feedback to the <Information Protection Yammer Group or other discussion forum>.

Sample email template

Subject line: Introducing Azure Information Protection

A new way to protect your data

Dear Employee,

Sharing information with colleagues within and outside of our company is important to us all. We at <company name> encourage such collaboration and would like to help you work with sensitive information in a secure manner. For this purpose, we're deploying Microsoft Azure Information Protection to help you easily secure critical company data.

What is data classification?

Whatever your role at <company name>, you produce or work with sensitive and confidential information. Data is constantly being created, edited, shared, and stored by individuals, teams, groups, and sometimes partners. Data classification is a tool that will allow us to better understand, control, and protect this information. Properly classifying and protecting this data is critical to our business.

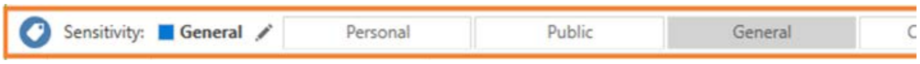
Azure Information Protection is coming soon to your devices

Starting on <date>, <company name> will begin to silently install the Azure Information Protection data classification tool on your devices. You'll soon see a new labeling toolbar in Microsoft Outlook and other Microsoft Office applications. Azure Information Protection is an intuitive data classification labeling and protection tool that aligns to <company name>'s new <insert company security initiative>.

Note: You might need to close and reopen Outlook or other Office applications to see the new toolbar.

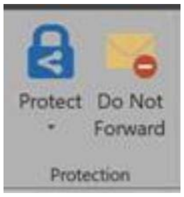
How it works in Office

Azure Information Protection enables secure sharing of emails and documents by allowing you to easily select the appropriate data classification label directly within the document or email. Only the individuals you authorize will have access to the documents you create.


Sensitivity: General

How it works in Outlook

In addition to enabling you to easily classify emails, Azure Information Protection also enables you to control how your emails will be shared by your recipients. If you select the **Do Not Forward** button, recipients of the email will not be able to forward, print, or copy the content of the email you have sent them.



Start using it!

1. Use the labeling features and take the guesswork out of the data classification process.
   a. **User selected.** Apply a label to the email or file you're working on with a single click.
   b. **Recommended.** Based on the content, the software will provide a suggested classification. Let us know how we're doing by selecting the recommended setting or hitting dismiss if we missed the mark.
2. Start classifying your emails and documents with the new classification labels:
   Personal, Public, General, Confidential, and Highly Confidential.

Additional information & support

For technical assistance, contact <IT Help Desk>.

Thank you,
<IT security name>

Classification examples

Azure Information Protection—end user data classification examples

Highly Confidential

Examples of data commonly classified as Highly Confidential include but are not limited to:

- Any code related to intellectual property or internal applications/sites
- Biometric markers
- Complete geolocation tracking data
- Credit card and transaction information
- Customer data used by <company name> to manage access to administrative roles or sensitive functions, such as private keys used to manage IT Infrastructure
- Customer payment data, such as non-protected credit card data (refer to the Payment Card Industry Data Security Standard (PCI DSS) or financial account information that identifies the individual’s information in its entirety
- Data covered under attorney-client privilege
- Data under strict regulatory handling requirements (that is, where the legal or regulatory body specifies the handling requirements for the data)
- Data used for authenticating or validating a person’s identity, or other information that can be used to directly or indirectly authenticate and authorize high-value transactions
- Design and functional specifications
- Executed contracts that are confidential to <company name>
- Future or active sales and marketing plans
- Hardware or software tokens
- Material financial data
- <company name> business secrets, such as new product design specifications
- <company name> prerelease financial results
- Private cryptographic keys
- Receipts and payment data
- Sales account data

- Sensitive personal employment data
- Source code, symbols, binaries, test cases, test results, builds, and specifications that could create a negative impact to <company name>'s competitive advantage or intellectual property rights if leaked

Confidential

Examples of data commonly classified as Confidential include but are not limited to:

- Addresses
- Bank account numbers
- Current system configuration data
- Customer support tickets that do not include Highly Confidential information, such as incident or breach information
- Customer system diagnostic data
- Customization information
- Data about <company name> employees, such as title or current role
- Data that's missing classification and unlabeled
- Data or software file shares
- Executive contracts
- Fax numbers
- Future or active processes or procedures
- IP addresses
- <company name> account IDs
- <company name> trade secrets
- Names (first and last)
- Non–Highly Confidential data that is subject to breach notification laws (for example, personnel number, personal contact information)
- Human Resources data that is not Highly Confidential
- Operating procedures or manuals
- Payment instructions
- Phone numbers

- Product documentation and supporting materials
- Product keys (individual)
- Receipts
- Sales account data
- Sales notes about <company name> customers
- Source code or binaries that, if reverse engineered or cloned, could result in serious material impact to the quality and/or integrity of <company name> products or brands (for example, user interfaces)
- Unreleased product schedules
- Network infrastructure configurations or designs
- Voice command recordings

General

This category represents the daily work product used and shared throughout <company name>. Examples of data commonly classified as General include but are not limited to:

- Age
- Commonly shared internal information, including operating procedures, policies, and interoffice memorandums
- Companywide announcements and information that all employees, contract staff, and those under NDA have been approved to read
- Email headers
- Gender
- Telemetry data
- ZIP Codes

Public

Examples of data commonly classified as Public include but are not limited to:

- Announced <company name> corporate financial data

- Marketing materials created for public product releases
- Materials used for presentations at open conferences and seminars and in podcasts
- Public cryptographic keys

Personal

Examples of data commonly classified as Personal include but are not limited to:

- Flyers sharing children’s summer camp information (if the event is not sponsored by <company name>)
- Individual non-<company name> data, such as your tax filings
- Invitations to work colleagues to a personal party (if the event is not sponsored by <company name>)
  Your personal emails to family, friends, and colleagues, if the emails are not related to <company name> business activities (for example, a lunch invitation)

More Information

For more information

- ***Know more about Azure Information Protection***

  https://www.microsoft.com/en-us/cloud-platform/azure-information-protection

- ***Azure Information Protection Documentation***

  https://docs.microsoft.com/en-us/information-protection/understand-explore/what-is-information-protection

- ***Add Azure Information Protection Quick Start Tutorial***

  https://docs.microsoft.com/en-us/information-protection/get-started/infoprotect-quick-start-tutorial

- ***Azure Information Protection user guide***

  https://docs.microsoft.com/en-us/information-protection/rms-client/client-user-guide

- ***Download and install the Azure Information Protection client***

  https://docs.microsoft.com/en-us/information-protection/rms-client/install-client-app
- ***Accelerate Azure information protection deployment and adoption***
  https://myignite.microsoft.com/sessions/53454?source=session