

February 6th-7th

NIE
20/20 VISION

Oslo Spektrum



NIC

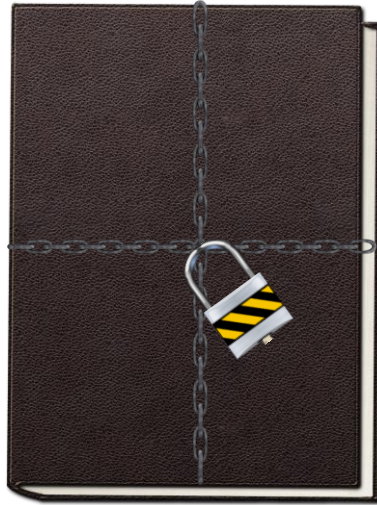
20/20 VISION

Secure Your Information, Not Your Devices



Sparebanken
Vest

When did YOU start to protect your information?



NIC

Historic Protection



Information Protection

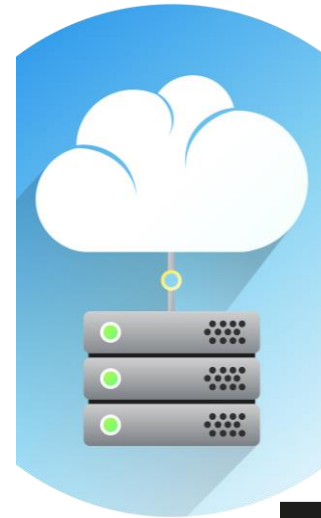
Access



Share

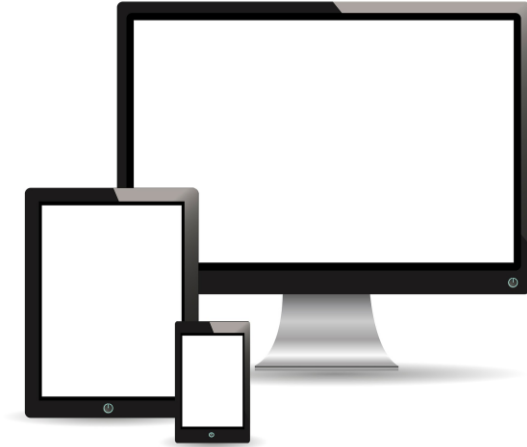


Store



NIC

Not your devices????



NIC

Device Management Examples

- Active Directory
- Office 365
- Intune
- Sccm / Intune
- Jamf
- Android Enterprise

Intune Supported OS!

- Windows

- PCs running Windows 10 (Home, Pro, Education, and Enterprise versions)
- Windows 10 Mobile
- Devices running Windows 10 IoT Enterprise (x86, x64)
- Devices running Windows 10 IoT Mobile Enterprise
- Windows Holographic & Windows Holographic Enterprise
- Windows Phone 8.1, Windows 8.1 RT, and PCs running Windows 8.1 (Sustaining mode)
- Windows 7 and later PCs, except Windows 10 Home edition, can also be managed with the Intune software client.

- Apple

- Apple iOS and iPadOS 9.0 and later
- Mac OS X 10.9 and later

- Google

- Google Android 4.0 and later (including Samsung KNOX Standard 4.0 and higher)
- Google Android for Work



Android 4.0 - Ice Cream Sandwich

Microsoft Azure Search resources, services, and docs (G+/) > DemOlav@M365x30295... CONTOSO

All services > All Users - Properties > Edit restriction

Edit restriction

Device type restriction

[Platform settings](#) [Review + save](#)

Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. [Learn more](#)

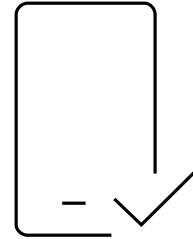
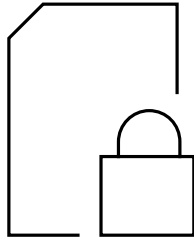
Type	Platform	versions	personally owned
Android Enterprise (work profile)	Allow Block	Allow min/max range: Min Max	Allow Block
Android device administrator	Allow Block	Allow min/max range: 7.0 ✓ Max ✓	Allow Block
iOS/iPadOS	Allow Block	Allow min/max range: Min Max	Allow Block
macOS	Allow Block	Restriction not supported	Allow Block
Windows (MDM) ⓘ	Allow Block	Allow min/max range: Min Max	Allow Block
Windows Mobile	Allow Block	Allow min/max range: Min Max	Allow Block



Lost Devices vs Lost Data



Information Protection VS Device Management



Levels And Layers



NIC

First Layer

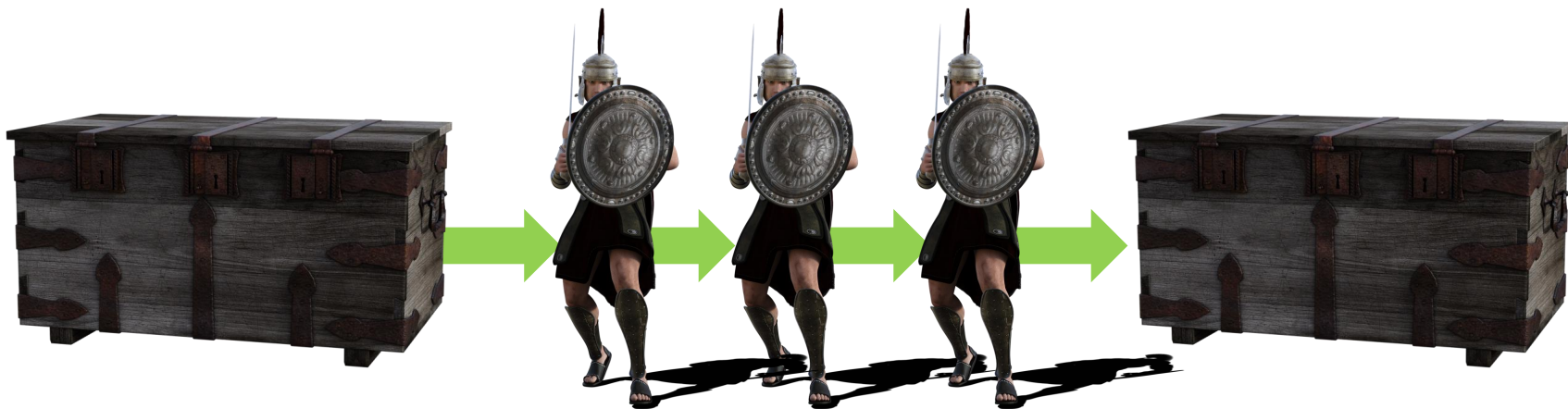


NIC

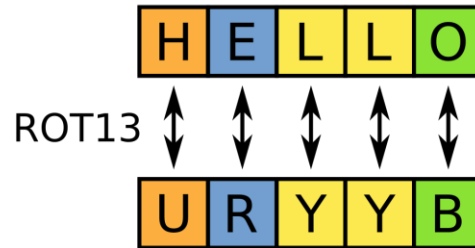
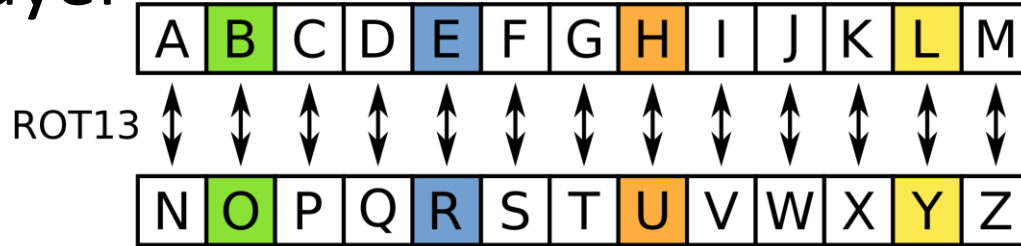
Second Layer



Transportation between second layers



Third layer



Caesar Cipher: **Uzufq Daowe**

NIC

- Old School



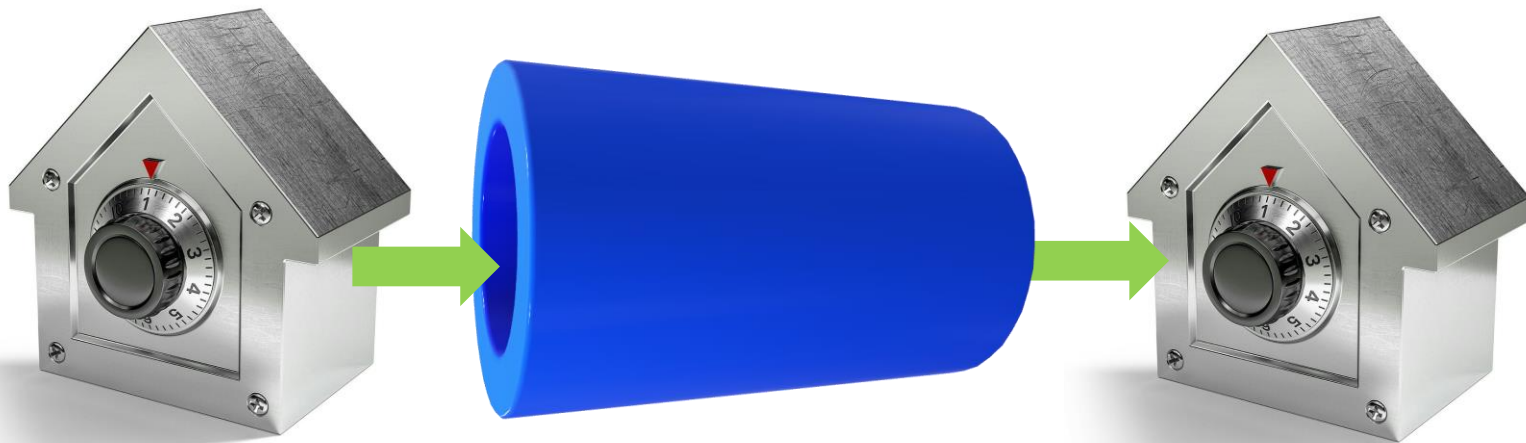
ROT13

H	E	L	L	O
↑	↑	↑	↑	↑
U	R	Y	Y	B

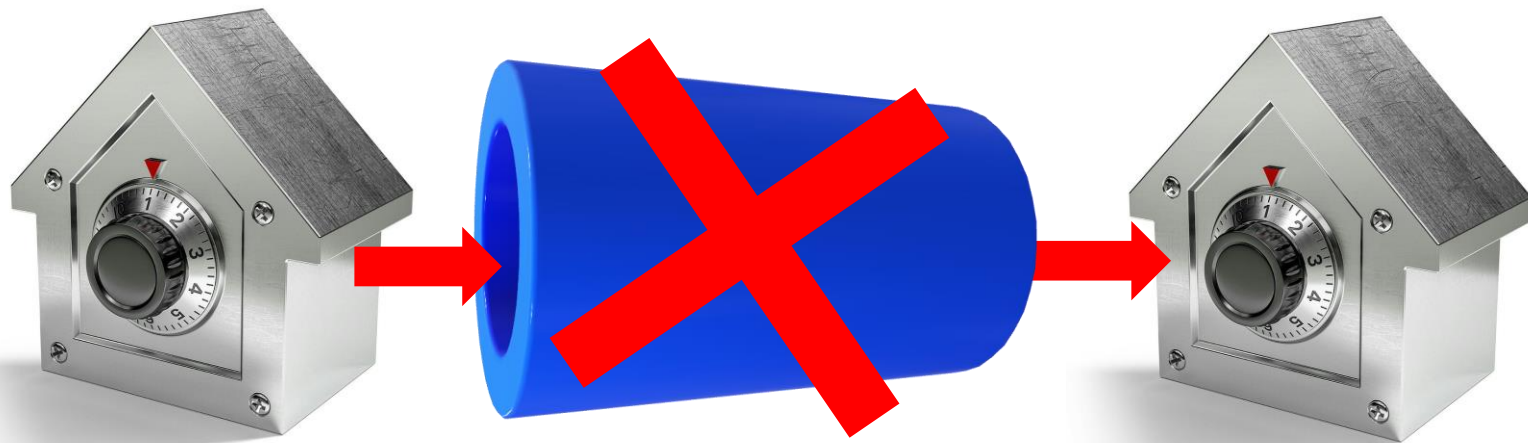
- Modern



Transportation between second layers



Transportation between second layers



Levels and Layers in Microsoft 365

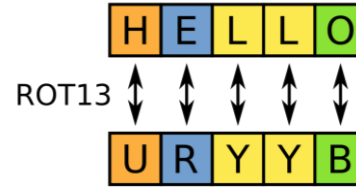


		Office 365	EMS E3	EMS E5
Layers		Basic	Extended	Advanced
	Information	<ul style="list-style-type: none"> Controlled Access 	<ul style="list-style-type: none"> Manuel Protection & labelling Monitoring 	<ul style="list-style-type: none"> Automatic Protection & labelling
	Devices	<ul style="list-style-type: none"> Enrolled Basic MDM 	<ul style="list-style-type: none"> Encryption Monitoring MDM 	<ul style="list-style-type: none"> Monitoring with automated responses
	Identity	<ul style="list-style-type: none"> Cloud presence Passwords 	<ul style="list-style-type: none"> MFA Conditional Access Monitoring 	<ul style="list-style-type: none"> Monitoring with automated responses Automation
		Levels		

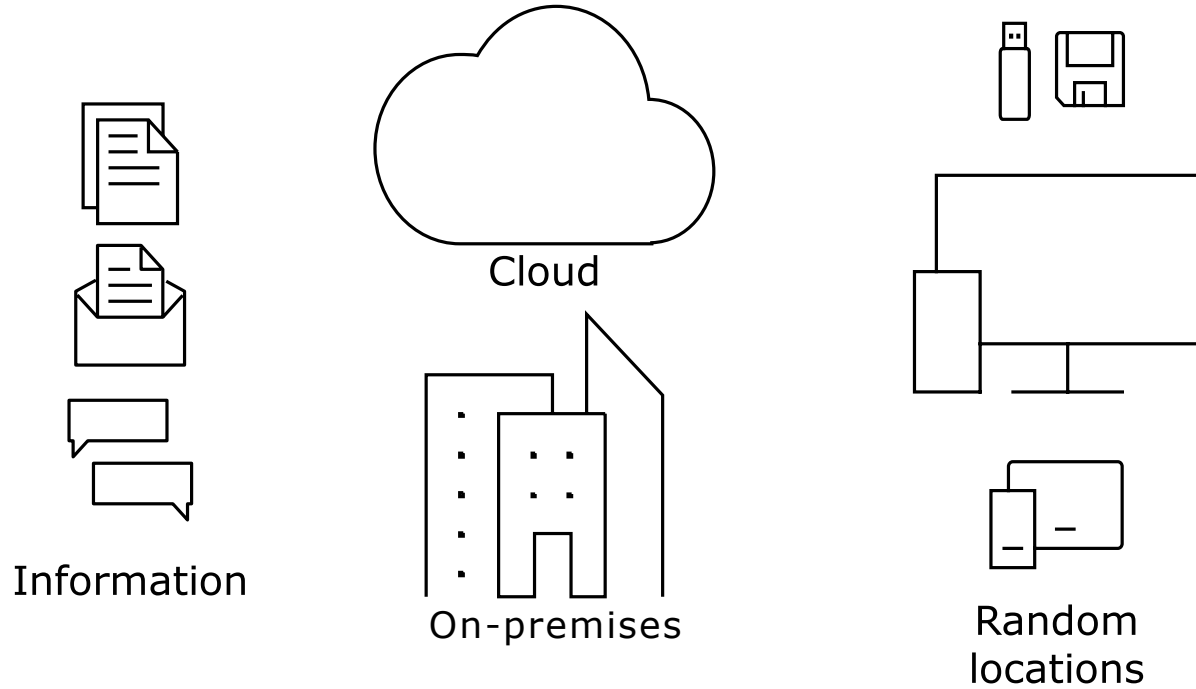
Layers

Microsoft 365 E3			Microsoft 365 E5
	Basic	Extended	Advanced
Information	<ul style="list-style-type: none">Controlled Access	<ul style="list-style-type: none">Manuel Protection & labellingMonitoring	<ul style="list-style-type: none">Automatic Protection & labelling
Devices	<ul style="list-style-type: none">EnrolledBasic MDM	<ul style="list-style-type: none">EncryptionMonitoringMDM	<ul style="list-style-type: none">Monitoring with automated responses
Identity	<ul style="list-style-type: none">Cloud presencePasswords	<ul style="list-style-type: none">MFAConditional AccessMonitoring	<ul style="list-style-type: none">Monitoring with automated responsesAutomation
Levels			

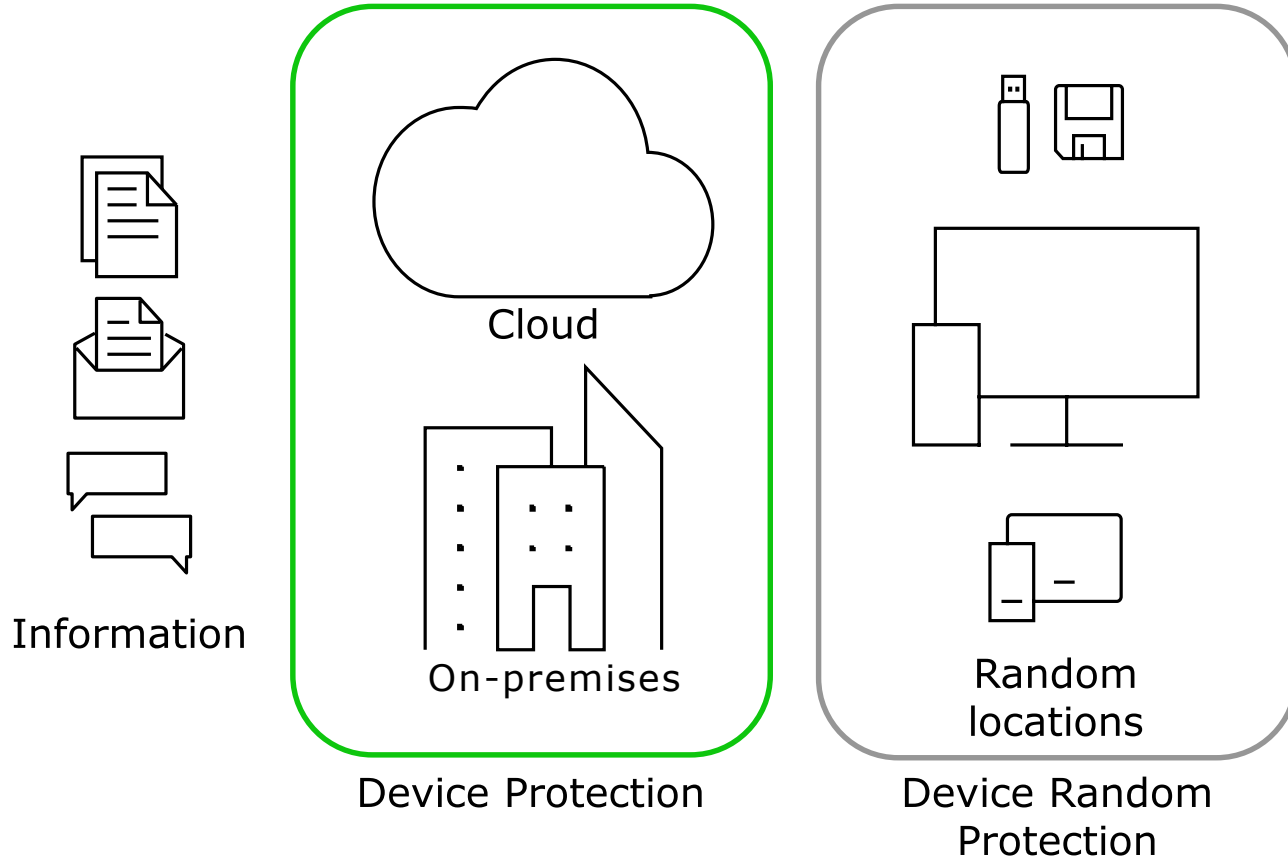
Information Protection



Information Protection



Information Protection



DLP And Retention





Home

Alerts

Reports

Secure score

Classification



Sensitivity labels

Retention labels

Sensitive info types

Label analytics

Policies

Permissions

More resources

Customize navigation

Retention labels

Labels

Label policies

When published, retention labels appear in your users' apps, such as Outlook, SharePoint, and OneDrive. When a label is applied to email or docs (automatically or by the user), the content is retained based on the settings you chose. For example, you can create labels that retain content for a certain time or ones that simply delete content when it reaches a certain age. [Learn more about retention labels](#)

+ Create a label

Publish labels

Auto-apply a label

Refresh

Name	Created by	Retention duration	Last modified
Personal Financial PII	Megan Bowen	1095 days	09/20/2019
Medical Records Retention Policy	Megan Bowen	7 years	09/20/2019
Olav in a negative way	Dem Olav	1 week	11/05/2019
Employee Records	Megan Bowen	Unlimited	09/20/2019
Confidential	Megan Bowen	7 years	09/20/2019
Private	Megan Bowen	1825 days	09/20/2019
PII Retention Policy	Megan Bowen	7 years	09/20/2019
Product Retired	Megan Bowen	3650 days	09/20/2019
Public	Megan Bowen	1825 days	09/20/2019

0 items selected. 10 items loaded.





Home

Alerts

Reports

Secure score

Classification

Sensitivity labels

Retention labels

Sensitive info types

Label analytics

Policies

Permissions

More resources

Customize navigation

Sensitivity labels

Labels

Label policies

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label

Publish labels

Refresh

Name	Created by	Last modified
Personal	... MOD Administrator	09/19/2019
General	... MOD Administrator	09/19/2019
Internal	... MOD Administrator	09/19/2019
Confidential - Finance	... MOD Administrator	02/06/2020
Confidential - PII	... MOD Administrator	02/06/2020
Highly Confidential	... Megan Bowen	11/05/2019
Protected	... Dem Olav	02/06/2020
Labeled	... Dem Olav	02/06/2020
IP-Preview	... Dem Olav	02/06/2020
test03	... Dem Olav	02/06/2020
Test04	... Dem Olav	02/06/2020
AIP - SharePoint	... Olav Tvedt	02/06/2020

0 items selected. 12 items loaded.





Home

Alerts

Reports

Secure score

Classification

Sensitivity labels

Retention labels

Sensitive info types

Label analytics

Policies

Permissions

More resources

Customize navigation

Sensitivity labels

Labels

Label policies

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label



Publish labels


Refresh


Name	Created by	Last modified
Personal	... MOD Administrator	09/19/2019
General	... MOD Administrator	09/19/2019
Internal	... MOD Administrator	09/19/2019
Confidential - Finance	... MOD Administrator	02/06/2020
Confidential - PII	... MOD Administrator	02/06/2020
Highly Confidential	... Megan Bowen	11/05/2019
Protected	... Dem Olav	02/06/2020
Labeled	... Dem Olav	02/06/2020
IP-Preview	... Dem Olav	02/06/2020
test03	... Dem Olav	02/06/2020
Test04	... Dem Olav	02/06/2020
AIP - SharePoint	... Olav Tvedt	02/06/2020


0 items selected. 12 items loaded.





- 
-  Home

 Alerts

 Reports

 Secure score

 Hunting


 Classification

Sensitivity labels

Retention labels

Sensitive info types

Label analytics

 Policies

Permissions

More resources


Customize navigation


Show all


Sensitive info types

The sensitive info types here are available to use in your security and compliance policies around the globe, as well as any custom types you have created.

[Manage sensitive info types in the Office 365 Security & Compliance Center](#)

 Create policy

 Refresh

Name	Type
Argentina National Identity (DNI) Number	Entity
Chile Identity Card Number	Entity
China Resident Identity Card (PRC) Number	Entity
Norway Identity Number	Entity
Portugal Citizen Card Number	Entity
Croatia Personal Identification (OIB) Number	Entity
International Classification of Diseases (ICD-10-CM)	Entity
International Classification of Diseases (ICD-9-CM)	Entity
<div></div> Olav related info	Entity

Olav related info



-  Edit
-  Test type
-  Delete

- Description

Olav gets mentioned negatively

Edit
- Regular expression

Edit
- Keywords

Olav
Sucks

Edit
- Dictionary (Large keywords)

Edit

Close

Microsoft 365 compliance

Home

Compliance score

Data classification

Data connectors

Alerts

Reports

Policies

Permissions

Solutions

Catalog

More resources

Customize navigation

Show all

Data classification (preview)

Sensitive info types

The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created.

Create info type

Refresh

101 items

Search

Name	Type	Publisher
Credit Card Number	Entity	Microsoft Corporation
France Passport Number	Entity	Microsoft Corporation
U.K. Driver's License Number	Entity	Microsoft Corporation
EU Debit Card Number	Entity	Microsoft Corporation
International Classification of Diseases (ICD-9-CM)	Entity	Microsoft Corporation
Japan Passport Number	Entity	Microsoft Corporation
U.S. Individual Taxpayer Identification Number (ITIN)	Entity	Microsoft Corporation
U.S. / U.K. Passport Number	Entity	Microsoft Corporation
German Passport Number	Entity	Microsoft Corporation
<input checked="" type="radio"/> Canada Social Insurance Number	Entity	Microsoft Corporation
EU Driver's License Number	Entity	Microsoft Corporation
Japan Bank Account Number	Entity	Microsoft Corporation
U.K. National Insurance Number (NINO)	Entity	Microsoft Corporation

Need help?

Feedback

NIC

Home

Alerts

Reports

Secure score

Classification

Sensitivity labels

Retention labels

Sensitive info types

Label analytics

Policies

Permissions

More resources

Customize navigation

Retention labels

Labels Label policies

When published, retention labels appear in your users' apps, such as Outlook, SharePoint, and OneDrive. When a label is applied to email or docs (automatically or by the user), the content is retained based on the settings you chose. For example, you can create labels that retain content for a certain time or ones that simply delete content when it reaches a certain age. [Learn more about retention labels](#)

Create a label Publish labels Auto-apply a label Refresh

Name	Created by	Retention duration	Last modified
TVEDT.one Protected files - Internal	Olav Tvedt	Unlimited	02/06/2020
Personal Financial PII	Megan Bowen	1095 days	09/20/2019
Medical Records Retention Policy	Megan Bowen	7 years	09/20/2019
Olav in a negative way	Dem Olav	1 week	11/05/2019
Employee Records	Megan Bowen	Unlimited	09/20/2019
Confidential	Megan Bowen	7 years	09/20/2019
Private	Megan Bowen	1825 days	09/20/2019
PII Retention Policy	Megan Bowen	7 years	09/20/2019
Product Retired	Megan Bowen	3650 days	09/20/2019
Public	Megan Bowen	1825 days	09/20/2019

0 items selected. 10 items loaded.





Home

Alerts

Reports

Secure score

Classification

Sensitivity labels

Retention labels

Sensitive info types

Label analytics

Policies

Permissions

More resources

Customize navigation

Retention labels

Labels

Label policies

When published, retention labels appear in your users' app. You choose. For example, you can create labels that retain

[+ Create a label](#)
[Publish labels](#)
[Auto-apply a label](#)

Name

TVEDT.one Protected files - Internal

Personal Financial PII

Medical Records Retention Policy

☒ Olav in a negative way

Employee Records

Confidential

Private

PII Retention Policy

Product Retired

Public

1 item selected. 10 items loaded.

Olav in a negative way

[Edit label](#)
[Publish label](#)
[Auto-apply a label](#)
[Delete label](#)
[Explore items](#)

Name

Olav in a negative way

Description for admins

description

[Edit](#)

Description for users

Don't say that

[Edit](#)

File plan descriptors

Business function/department: Legal

Authority type: Legal

[Edit](#)

Retention

7 days

Delete only

Based on when it was created

[Edit](#)

Created by

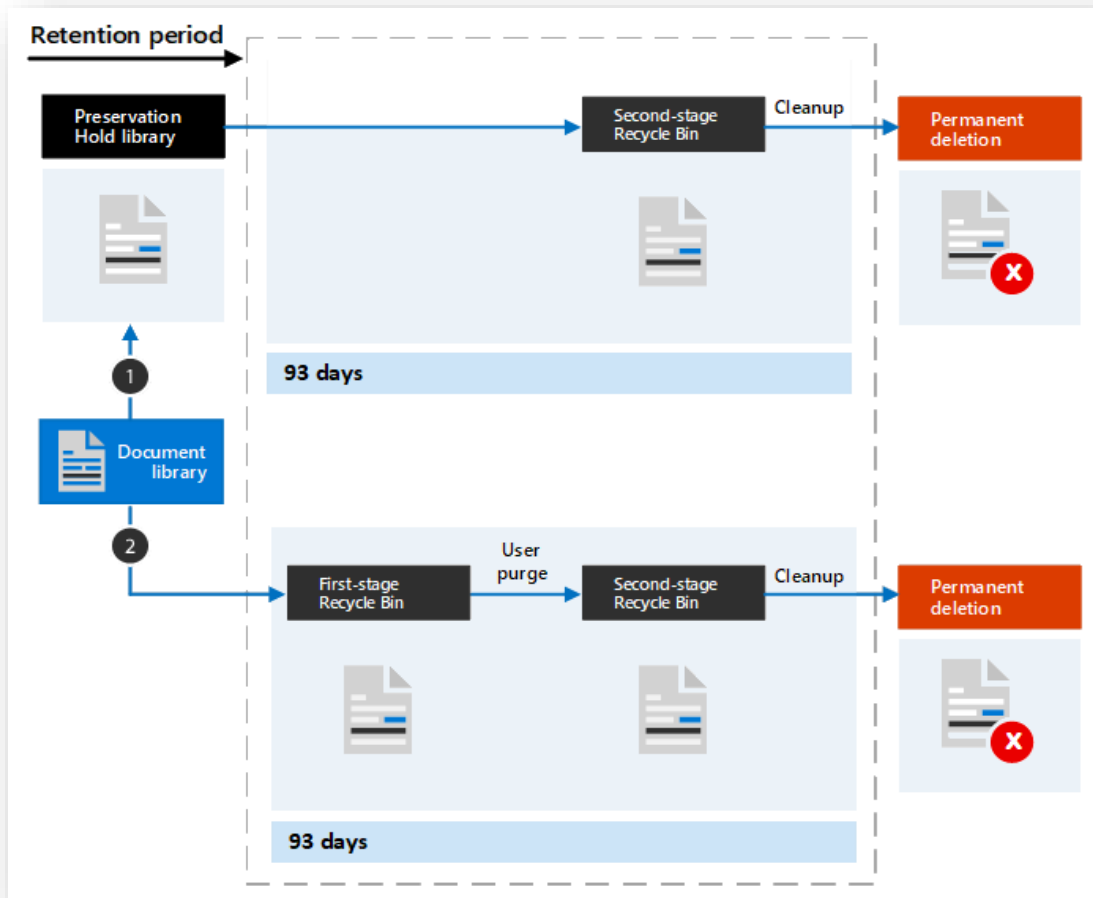
Dem Olav

Created

5 November 2019

[Close](#)

Retention



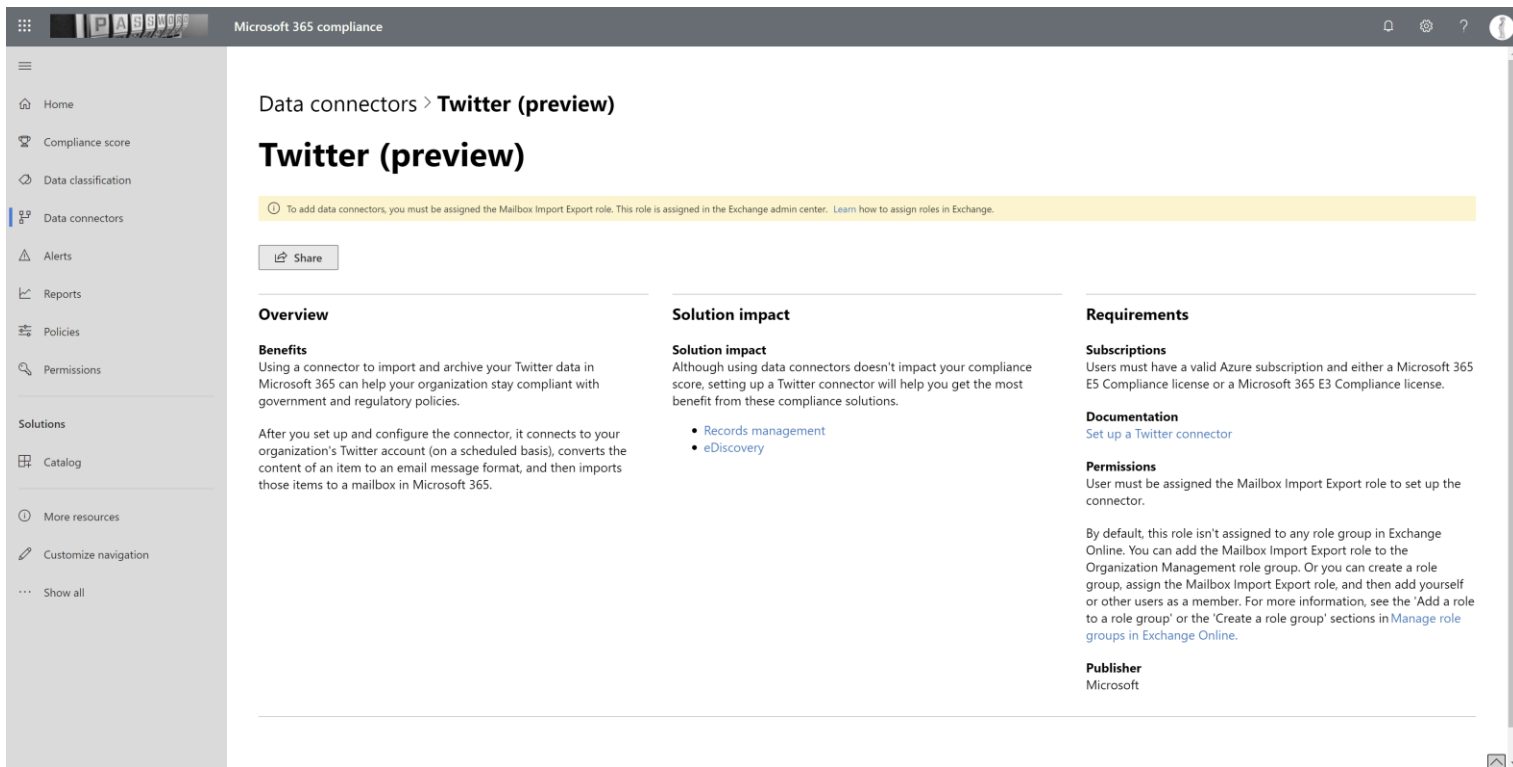
Where are your information?

The screenshot shows the Microsoft 365 compliance center interface. The top navigation bar includes the Microsoft 365 logo, the title 'Microsoft 365 compliance', and user profile icons. A left-hand navigation pane lists various sections: Home, Compliance score, Data classification, Data connectors (highlighted), Alerts, Reports, Policies, Permissions, Solutions, Catalog, More resources, Customize navigation, and Show all. The main content area is titled 'Data connectors' and has two tabs: 'Overview' (selected) and 'Connectors'. Below the tabs, a section titled 'Connect to your data sources' explains that connectors help link important data sources to solutions, with a 'Learn more' link. A search bar is located in the top right of the main content area. Five data source connectors are displayed in a grid:

- Instant Bloomberg** (By Microsoft): Connecting to your Instant Bloomberg data is valuable for communication compliance, records management, and eDiscovery solutions. A 'View' button is present.
- HR (preview)** (By Microsoft): Connecting to your HR data is valuable for identifying and remediating internal risks using solutions such as insider risk management. A 'View' button is present.
- Facebook business pages (preview)** (By Microsoft): Connecting to your Facebook data is valuable for records management and eDiscovery solutions. A 'View' button is present.
- LinkedIn company pages** (By Microsoft): Connecting to your LinkedIn data is valuable for records management and eDiscovery solutions.
- Twitter (preview)** (By Microsoft): Connecting to your Twitter data is valuable for records management and eDiscovery solutions.

At the bottom right, there is a 'Need help?' button and a 'Feedback' button.

Where are your information?



The screenshot displays the Microsoft 365 compliance center interface. The top navigation bar includes the Microsoft 365 logo, the text "Microsoft 365 compliance", and user profile icons. A left-hand sidebar contains navigation links: Home, Compliance score, Data classification, Data connectors (highlighted), Alerts, Reports, Policies, Permissions, Solutions, Catalog, More resources, Customize navigation, and Show all. The main content area is titled "Data connectors > Twitter (preview)" and "Twitter (preview)". A yellow banner below the title states: "To add data connectors, you must be assigned the Mailbox Import Export role. This role is assigned in the Exchange admin center. [Learn how to assign roles in Exchange.](#)" Below this is a "Share" button. The content is organized into three columns: Overview, Solution impact, and Requirements. The Overview column includes a "Benefits" section explaining that the connector imports Twitter data into a mailbox in Microsoft 365. The Solution impact column includes a "Solution impact" section stating that using data connectors doesn't impact compliance scores and lists links for "Records management" and "eDiscovery". The Requirements column includes sections for "Subscriptions" (requiring a valid Azure subscription or Microsoft 365 E5 license), "Documentation" (with a link to "Set up a Twitter connector"), "Permissions" (requiring the Mailbox Import Export role), and "Publisher" (Microsoft).

Microsoft 365 compliance

Data connectors > **Twitter (preview)**

Twitter (preview)

To add data connectors, you must be assigned the Mailbox Import Export role. This role is assigned in the Exchange admin center. [Learn how to assign roles in Exchange.](#)

Share

Overview

Benefits

Using a connector to import and archive your Twitter data in Microsoft 365 can help your organization stay compliant with government and regulatory policies.

After you set up and configure the connector, it connects to your organization's Twitter account (on a scheduled basis), converts the content of an item to an email message format, and then imports those items to a mailbox in Microsoft 365.

Solution impact

Solution impact

Although using data connectors doesn't impact your compliance score, setting up a Twitter connector will help you get the most benefit from these compliance solutions.

- [Records management](#)
- [eDiscovery](#)

Requirements

Subscriptions

Users must have a valid Azure subscription and either a Microsoft 365 E5 Compliance license or a Microsoft 365 E3 Compliance license.

Documentation

[Set up a Twitter connector](#)

Permissions

User must be assigned the Mailbox Import Export role to set up the connector.

By default, this role isn't assigned to any role group in Exchange Online. You can add the Mailbox Import Export role to the Organization Management role group. Or you can create a role group, assign the Mailbox Import Export role, and then add yourself or other users as a member. For more information, see the 'Add a role to a role group' or the 'Create a role group' sections in [Manage role groups in Exchange Online](#).

Publisher

Microsoft

**The ultimate
information protection
is when
the information protect itself**



NIC

IRM or MIP/AIP

- Current limitations AIP protected files stored in Office 365:
 - No Co-authoring, eDiscovery, search or other collaborative features
 - DLP (Data loss prevention) work with metadata, not content
- IRM encrypts when files are created

<https://docs.microsoft.com/en-us/office365/securitycompliance/protect-sharepoint-online-files-with-azure-information-protection>

nrc

Azure Information Protection



NIC

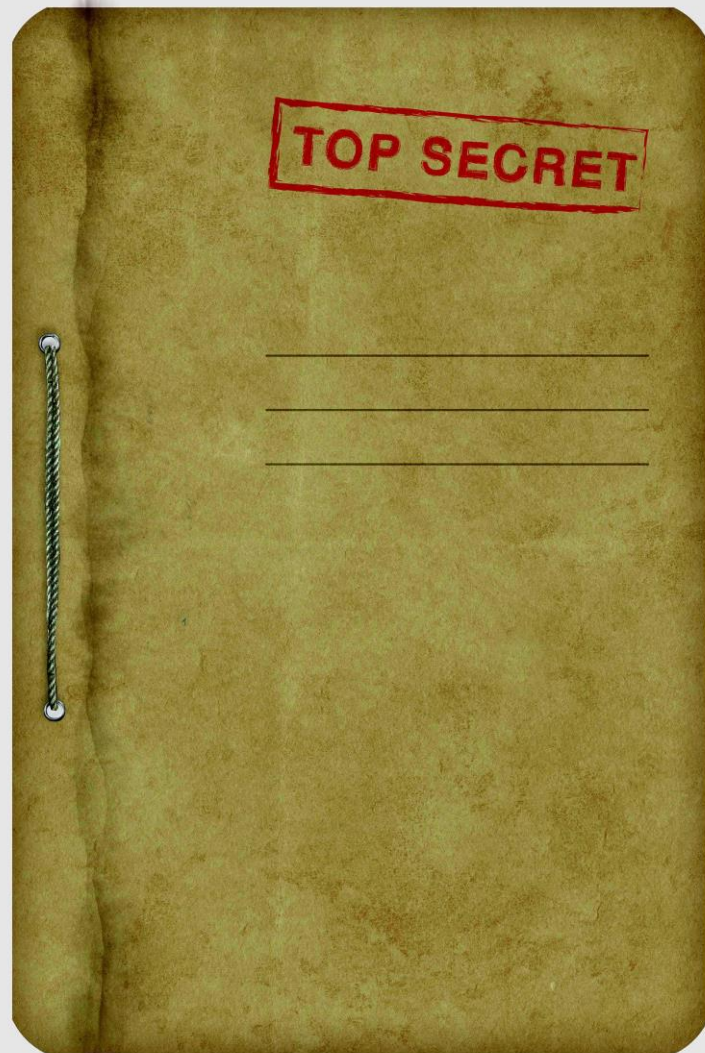
Classify



- **Automatic classification**
- Policies can be set by IT Admins for automatically applying classification and protection to data
- **Recommended classification**
- Based on the content you're working on, you can be prompted with suggested classification
- **Manual reclassification**
- Users can override a classification and optionally be required to provide a justification
- **User-driven classification**
- Users can choose to apply a sensitivity label to the email or file they are working on with a single click

Label

- **Metadata** written into document files
- **Travels** with the document as it moves
- Readable so that other systems such as DLP engines can **understand** and **take action**
- Used for the purpose of apply a **protection** action or **data governance action** – determined by policy
- Can be **customized** per the organization's needs



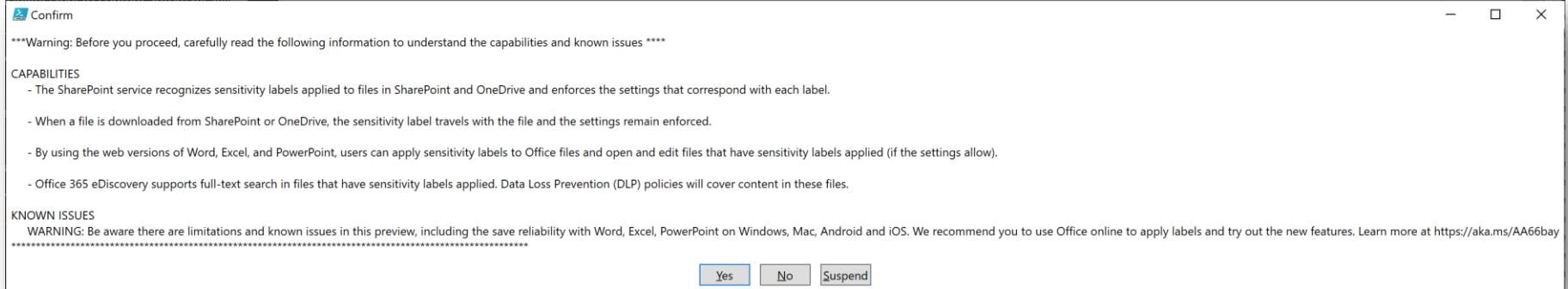
Protect

- **Encryption** that **cannot be removed** by others than the ones you specify.
- Can follow information for it's entire **lifecycle**.
- Allows you to **revoke access** if wanted/needed.



SharePoint and AIP (Preview)

```
PS C:\WINDOWS\system32> $orgName = "m365x302957"  
PS C:\WINDOWS\system32> Connect-SPOService -Url https://$orgName-admin.sharepoint.com  
PS C:\WINDOWS\system32> Set-SPOTenant -EnableAIPIntegration $true
```



Information Protection (AIP)

E3 (P1)

- Classification and labelling
- Encryption and rights management
- tracking and reporting

E5 (P2)

- Recommendations
- Automation
- AIP Scanner

Demo: Extending Information Protection



Protection On Device or Information Layer?

MDM/MAM

- Can require:
 - Encrypted storage
 - No sharing
 - Pin
 - Etc.
- Trusts the supported Platforms/Apps

MIP

- Securing the information
 - Manual
 - Recommended
 - Automatic
- Metadata
- Tracking
- Platform agnostic

Layers And Levels



Secure Your Information, Not Your Devices



Olav Tvedt

Twitter: @olavtwitt

Blog: <https://olavtvedt.blogspot.com>



Sparebanken
Vest

Podcasts: BlåSkjerm Brødrene

PodBean: <http://bit.ly/BlaSkj> - Apple: <http://bit.ly/blaskjerm> - Spotify: <http://bit.ly/blaaskjerm>

Slides and demos from the conference will be available at

<https://github.com/nordicinfrastructureconference/2020>

