

Introduction to

Azure Information Protection





User Identity



Devices



Apps



Data

| Data Protection



Data

- Secure Collaboration
- Intellectual Property
- Trade Secrets
- Personal, Financial, Health
- Data Loss Prevention
- Rights Management
- Secure Storage (cloud, network, local)
- Encryption
- Classification

| Agenda

Information Protection:

- What is AzureIP
- How does it work
- Getting started
- Plan for deployment

Azure Information Protection

Classify



Label



Protect



| What is AzureIP

Components:

- Azure Portal for policy management
- Office Add-in for classification and labelling
- Rights Management for protection

Requirements:

- EMS Subscription (E3 or E5)
- Office 365 subscription with Azure RMS (E3, E4, or E5)
- Office 2010, 2013, 2016
 - Mobile and Web apps are on the roadmap

| Securing the Data





Classify

Sensitive Data Policy

Default Labels

- Priority Ordering
- Enforcement

Least Sensitive



Most Sensitive



Enforce labelling

Enforce justification

Azure Information Protection
"PREMIUM P2" Service Plan - PREVIEW






Columns Save Discard Publish Export

Configure a title and tooltip for the Information Protection client on user devices

* Title
Sensitivity

Tooltip
Information Sensitivity consists of four distinct levels (Public, Internal, Confidential, Secret), allowing the user to identify the risk of exposing the information to unauthorized users inside or outside the business.

Configure the name, tooltip, and additional settings of each label; Order the labels according to their sensitivity level

LABEL NAME	TOOLTIP	MARKING	PROTECTION
 Personal	For personal use only. This data will not be monitored		...
 Public	This information can be used by everyone inside or ou		...
 Internal	This information includes a wide spectrum of internal l	✓	...
 Confidential	This data includes sensitive business information. Expo	✓	...
 Secret	This data includes highly sensitive information for the l	✓	...

+ Add a new label

All documents and emails must have a label (applied automatically or by users)

Off On

Select the default label

None

Users must provide justification to set a lower classification label, remove a label, or remove protection

Off On

| Classification Policies

Policy Based:


- Automated, or recommended
- Enforced, or user driven
- Known sensitive data types
- Keywords/Phrases
- Custom policy (regular expressions)
- Stamped in metadata


| Detection Policy


Built-in:

Condition

PREVIEW

 Save

 Discard

 Delete

Choose the type of condition

Built-in

Custom

* Select built-in

* Minimum number of occurrences

1

Count occurrences with unique values only

Off

On

| Sensitive Data Types

- 5 available today
- 80 available in O365 DLP

Choose the type of condition

☒ Built-in ☐ Custom

★ Select built-in

SWIFT Code
Credit Card Number
ABA Routing Number
USA Social Security Number (SSN)
International Banking Account Number (IBAN)

| Automation

Considerations for testing:

Must meet specific requirements:

- SWIFT Code - [Swift# ANTSGB2LTSY](#)
- Credit Card Number - [4242 4242 4242 4242](#)
- USA Social Security - [SSN 555 55 5555](#)

Reference: [https://technet.microsoft.com/en-us/library/jj150541\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/jj150541(v=exchg.160).aspx)

| Detection Policy

Custom:

Choose the type of condition

Built-in

Custom

* Name

* Match the exact following phrase ⓘ

Match as a regular expression

Off

On

Match with case sensitivity

Off

On

* Minimum number of occurrences

1

Count occurrences with unique values only

Off

On

Metadata

Unique per policy with a reusable “Sensitivity” field:

- Create DLP rules based on this field
- Use CAS detection policies
- Integrate with SPO columns

Secure Document.docx Properties

General Summary Statistics Contents Custom

Name:

Checked by
Client
Date completed
Department
Destination
Disposition

Add
Delete

Type: Text

Value: ☐ Link to content

Properties:

Name	Value
MSIP_Label_759...	True
MSIP_Label_759...	https://api.informationprote
MSIP_Label_759...	richa@SURFACEPRO3
MSIP_Label_759...	2016-09-11T16:35:05.5840
MSIP_Label_759...	Confidential
MSIP_Label_759...	Manual
Sensitivity	Confidential

< >

OK Cancel



Label

Visual Marking

| Labelling

- Based on classification
- Header / Footer
- Water marks
- Variables

| Labelling Options

Header / Footer:

Set visual marking (such as header or footer)

Documents with this label have a header

* Header text

Please enter header text.

* Font size

10 

Color

Black 

Alignment

| Labelling Options

Watermark:

Documents with this label have a watermark

* Watermark text

Please enter watermark text.

Size

Color

Black 

Layout

| Variables in text string

You can use the following for your header, footer, or watermark:

- `${Item.Label}` for the selected label.
- `${Item.Name}` for the file name or email subject.
- `${Item.Location}` for the path and file name for documents, and the email subject for emails.
- `${User.Name}` for the owner of the document or email, by the Windows signed in user name.
- `${User.PrincipalName}` for the owner of the document or email, by the Azure Information Protection client signed in email address (UPN).
- `${Event.DateTime}` for the date and time when the selected label was set.



Protect

Rights Management

| Protection

Apply Rights Management:

- Based on classification
- Azure RMS & AD RMS
- Track & Revoke (specific license required)

| Outlook

Specific behaviours:

- Applies on send (user may not be aware)
- Conditions must be Automatic (recommended doesn't work, yet)
- Do Not Forward (specific to email)

Deployment Planning

| Deployment Planning

Classification comes first:

is the only mandatory scenario, as it puts in place the fundamentals of the solution and is the foundation on which the other scenarios are built.

- What endpoints do you have
- What OS and Office version
- Data policy – do you have a defined one
- Sensitivity levels (these will become your labels)
- Who can access - can it be shared
- What level of protection (if any) to apply

| Deployment Planning

Policy Conditions:

- Automated
- Recommended
- Manual

Apply Protection:

- Azure RMS
- AD RMS
- Unprotected

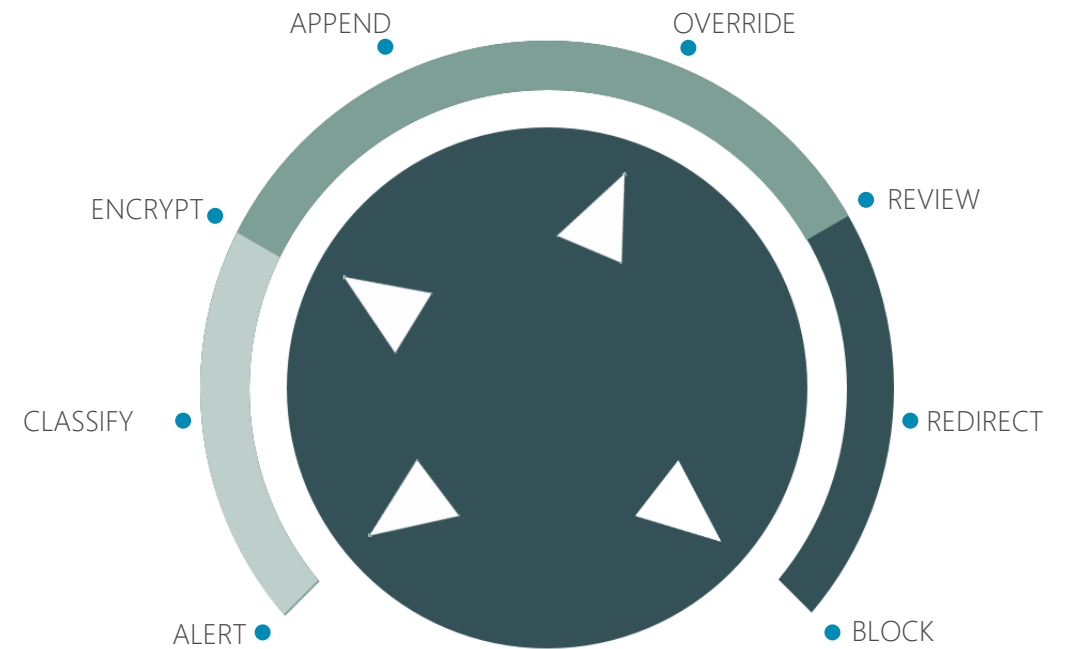
Reporting:

- Classification activity
- Document lifecycle
- Data leaks
- Abnormal behaviour

| Gradual enablement

Flexible tools for policy enforcement that provide the right level of control

- Classification (AzureIP)
- Visual Labelling (AzureIP)
- Rights Management (RMS)
- Data Loss Prevention (DLP)



Next steps

Follow @ <https://twitter.com/TheRMSGuy>

Learn more @ <http://aka.ms/rmshome>

Discover @ <http://aka.ms/rmsgetstarted>

For questions email AskIPteam@Microsoft.com

IT Pro blog @ <http://aka.ms/rmsblog>

Get involved @ <https://www.yammer.com/AskIPteam>

Download @ <http://aka.ms/AIPclient>



Thank you !



@rdiver

| Questions



www.ignia.com.au



08 9365 8400



info@ignia.com.au



Perth | Melbourne | Sydney

