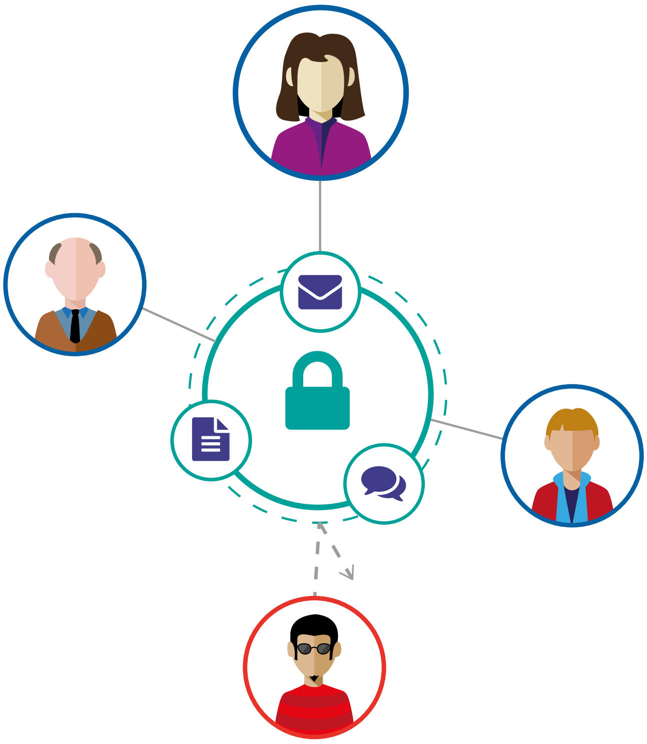
Enterprise Mobility and Security – what's the reality?

Alan Eardley, Head of Solution Design, CPS

Accessibility and transmission of data has never been so easy, but how can organisations and users safeguard themselves from sharing the wrong information?



In the modern workplace, organisations are changing the way they collaborate for two reasons:

- ✓ The increasing use of multiple social media platforms in the personal sphere is influencing the way we communicate within our professional lives
- ✓ The increase in use of multiple mobile devices enables us all to access content and applications from everywhere at any time

POLICY ADHERENCE

As an enabler for change, technology is providing new ways to share and consume content. This makes the process of securing content more essential to ensure the safeguarding of data and prevention of accidental data loss.

Every organisation relies on files being shared, both internally and externally. In the modern collaborative workplace that Office 365 provides, security is key.

It is essential for every user to understand the available security tools and for those tools to be used in the everyday applications that users are familiar with.

With **Microsoft 365**, mobility and security are provided for every user as part of the license. This allows the organisation to implement policies and procedures which support the prevention of accidental loss of data and automatic identification, tagging and securing of personal information. These capabilities allow organisations to create a more robust environment enabling secure sharing of content both internally and with external partners.

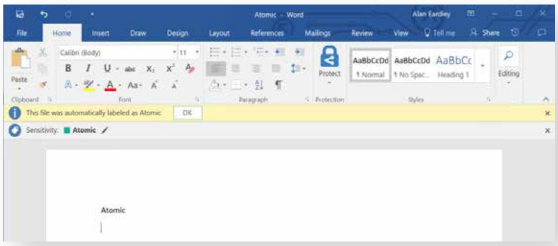
Within this paper we explore how the use of **Microsoft 365** can secure the enterprise and its users.

I WANT TO SECURE A DOCUMENT

As the creator of a document, a user needs to be confident and comfortable with the security that is being applied. It is possible to apply security policies automatically based on the content within the document. For example, a policy scans for the word 'Atomic' and if it is used within a document the security policy is automatically applied (Figure1).

With over 80 classifications of personal identifiable information types, such as passport, driving licence, and credit card, including custom options, there's lots of flexibility for users to configure documents from a set of pre-defined labels.
When a document is labelled, formatting options can be automatically applied as outlined in Figure 2.

Formatting of a document has multiple options, including a custom header, footer and watermark. All of these can be used separately or in combination and the they cannot be changed in the document, only via the classification label.

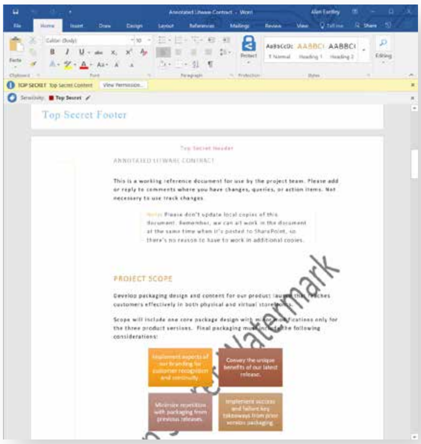


This file was automatically labeled as Atomic

Sensitivity: Atomic

Atomic

Figure 1 - Automatic application of policy


Annotated Litware Contract - Word
Alan Eardley
File
Home
Insert
Draw
Design
Layout
References
Mailings
Review
View
Tell me
Share
Protect
Editing
View Permission...
Top Secret Footer
Top Secret Header
Top Secret Watermark
Implement aspects of our branding for customer recognition and continuity
Convey the unique benefits of our latest release.
Minimize repetition with packaging from previous releases.
Implement success and failure key takeaways from prior version packaging

TOP SECRET Top Secret Content

Sensitivity: Top Secret

ANNOTATED LITWARE CONTRACT

This is a working reference document for use by the project team. Please add or reply to comments where you have changes, queries, or action items. Not necessary to use track changes.

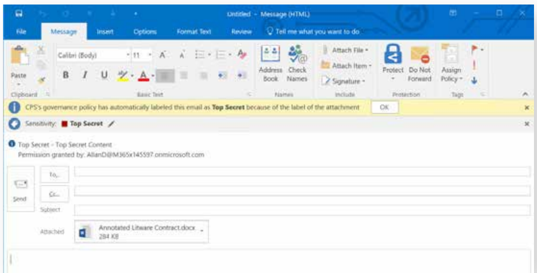
Note: Please don't update local copies of this document. Remember, we can all work in the document at the same time when it's posted to SharePoint, so there's no reason to have to work in additional copies.

PROJECT SCOPE

Develop packaging design and content for our product launch that reaches customers effectively in both physical and virtual storefronts.

Scope will include one core package design with minor modifications only for the three product versions. Final packaging must include the following considerations:

Figure 2 - Automated formatting



CPS's governance policy has automatically labeled this email as **Top Secret** because of the label of the attachment

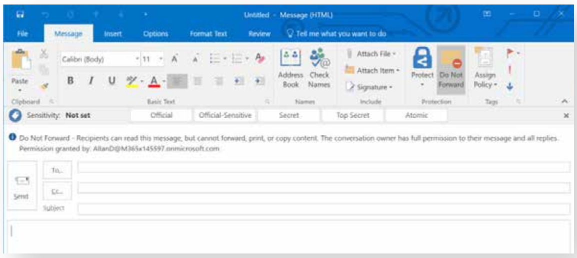
Sensitivity: Top Secret

Top Secret - Top Secret Content
Permission granted by: AllanD@M365x145597.onmicrosoft.com

Subject

Attached: Annotated Litware Contract.docx 284 KB

Figure 3 - Identifying label of attachment



Sensitivity: Not set

Do Not Forward - Recipients can read this message, but cannot forward, print, or copy content. The conversation owner has full permission to their message and all replies.
Permission granted by: AllanD@M365x145597.onmicrosoft.com

Subject

Figure 4 - Do not forward

I WANT TO EMAIL A DOCUMENT

Outlook is one of the applications that respects the classification labels of content. In fact, Outlook will automatically label an email based on the classification of an attachment.

As can be seen in the yellow bar in Figure 3, when Outlook identifies the label of the attachment, a custom message can be displayed to indicate the reason for the change in label.

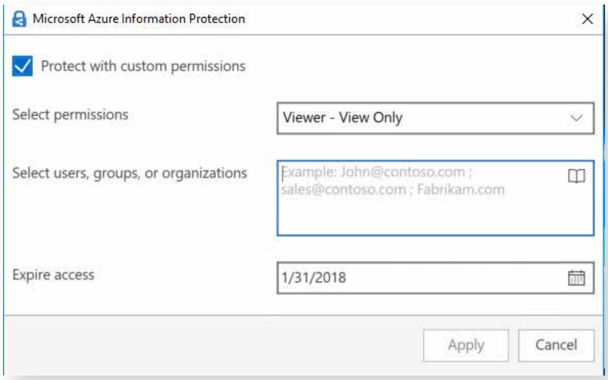
It is not only classifications that can be used to restrict the capabilities of the recipient, in fact, users can easily select 'Do not forward' in the ribbon and prevent the recipient from forwarding, printing or copying content from the email as depicted in Figure 4.

> With Microsoft 365, mobility and security are provided for every user as part of the license.

I WANT TO SET CUSTOM PERMISSIONS ON A DOCUMENT

Classification labels are sets of permissions which can be created centrally by the IT department and published to the rest of the organisation. Although, some users may have a need to create a document with custom permissions, which is possible too.

As noted within Figure 5, the author of the document can choose to apply a set of permissions to one or more users, groups or even a complete organisation. In addition, access to the document can expire on a set day.



Microsoft Azure Information Protection

☑ Protect with custom permissions

Select permissions: Viewer - View Only

Select users, groups, or organizations: Example: John@contoso.com ; sales@contoso.com ; Fabrikam.com

Expire access: 1/31/2018

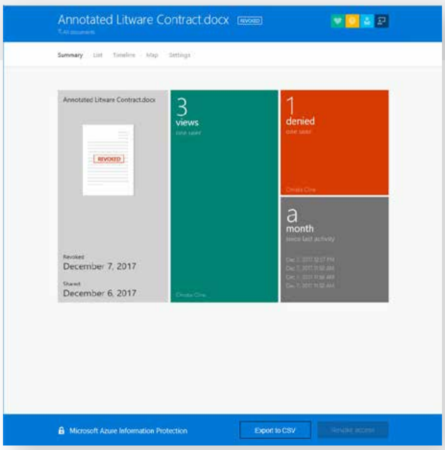
Figure 5- Custom permissions

I WANT TO SEE ACCESS TO A DOCUMENT

Once a document has been shared, you might want to know who has opened it.

From Word, it is possible to track access to the document, and importantly, revoke access too. The tracking of a document opens a dashboard that allows the author to view the number of times that the document has been accessed and the number of times access has been denied (reference Figures 6-8).

At the bottom of the screen is a button that allows the user to revoke access to the document quickly and easily. As well as the dashboard, there are also different views of the access, including a list view, but also a timeline and a map showing where the document was accessed from.



Annotated Litware Contract.docx

Annotated Litware Contract.docx

3 views

1 denied

a month

Revoked December 7, 2017

Shared December 6, 2017

Figure 6 - Track and revoke dashboard

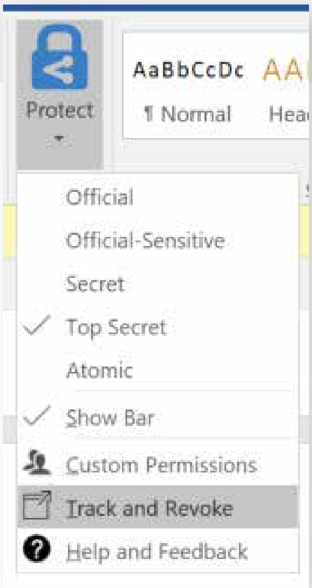
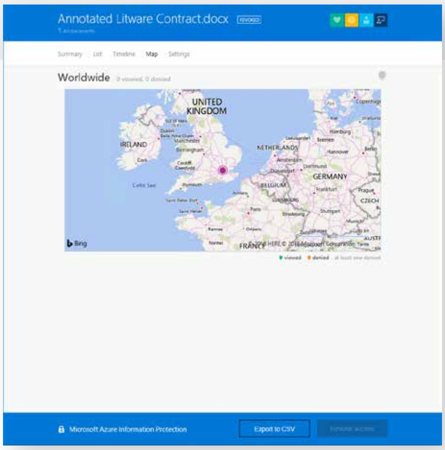


Figure 7- Track and revoke



Annotated Litware Contract.docx

Figure 8- Track and revoke map

SUMMARY

For security to be effective, it must be built into familiar tools that are frequently used.

The ability to define classification labels and to assign them automatically based on common Personal Identifiable Information (PII) data formats, custom words or patterns, reduces the risk that content containing sensitive data will be accidentally shared, and allows that content to be tracked.

These tools won't prevent sharing of sensitive data but will ensure that the end user is more aware of the sensitivity of the content and aware of the security implications.

Microsoft 365 provides the tools needed for users to easily create content and automatically assign classifications. Organisational security tools within Microsoft 365 allows end users to intuitively apply security without complex training. The applications provide clear visual prompts through the information bars, that reinforce the need to apply security and adhere to policies that safeguard the organisation and its employees and partners.

Enterprise Mobility and Security must be core to the design of any security policies and the implementation and usage of any Cloud Platform. Without the application of security policies and governance, the risk to organisational reputation and financial damage is increasing with the imminent legislative changes resulting from General Data Protection Regulation (GDPR).

WHO ARE CPS?

We know the importance of workplace productivity and transformation, which is why we help our clients reach their business objectives by supporting their journey to digital transformation.

Underpinned by Microsoft technologies, our consultants take pride in delivering tangible technology solutions that solve both technical and business issues.

We don't believe in a 'one size fits all' approach. Our consultants spend time with clients to appreciate their current IT landscape and what might need to change, adapt or evolve to meet business goals and directives.

To find out how we can support you on your journey, contact us today.

e hello@cps.co.uk
w www.cps.co.uk

Microsoft Partner
Microsoft

Gold Cloud Productivity
Gold Project and Portfolio Management
Gold Collaboration and Content
Gold Cloud Customer Relationship Management
Gold Messaging
Gold Application Development
Silver Cloud Platform
Silver Data Platform