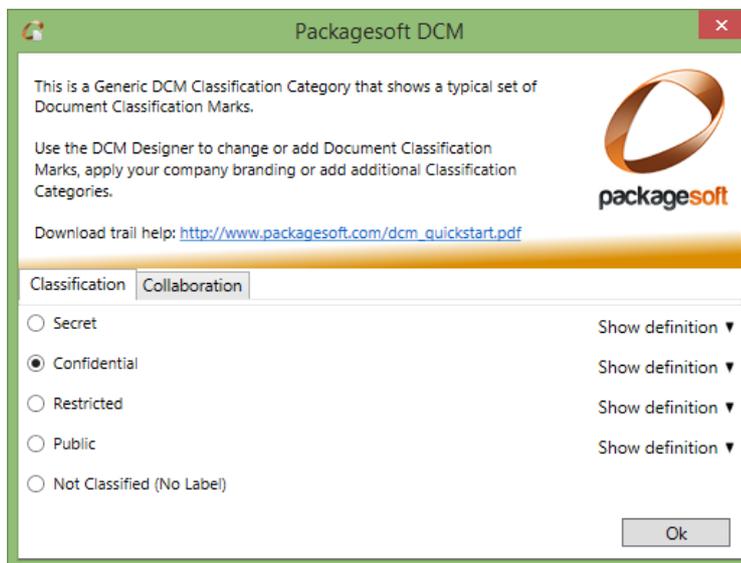




Information is the lifeblood of today's organisations; needing to be shared both internally and externally but at the same time, needing to be protected.

The dilemma is, how to protect the data without stemming its flow to those who need it? **The crucial first step in protecting data is to classify it.**

There are two possible approaches to data classification; one is to rely on post-data-creation mechanisms that interpret the data and arrive at a classification based on the content; the other approach, taken by Packagesoft DCM is to empower the author to decide the classification at the point of creation. This approach both increases awareness of data protection within the workforce and is generally more accurate and cost-effective. Moreover, once data has been DCM classified, it facilitates greater control of the data within systems such as RMS, DLP and FCI.



Introducing Packagesoft DCM 2015 – crucial first step solved.



DCM Office 2015 provides an extension to Microsoft Office that ensures all documents are classified before they can be saved, printed, or sent via email. Packagesoft DCM 2015 seamlessly integrates into an organisation's IT governance process and information security management system (ISMS) and requires little or no training. Regardless of the regulatory standard your organisation adheres to **ISO27001**, **ISO9001** or **Sarbanes-Oxley** for example, Packagesoft DCM 2015 can be configured to suit.

DCM SharePoint 2015 provides a consistent approach to document classification regardless where the document is created; stand-alone MS Office or from a SharePoint Library. DCM SharePoint controls which documents can be added to a library based on the document's classification and library settings.

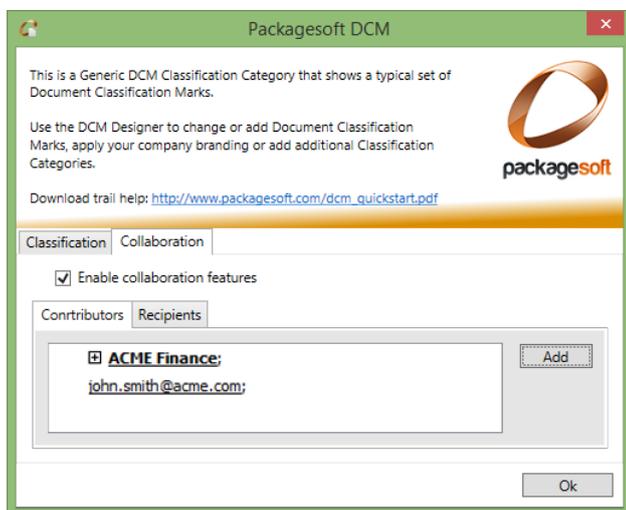
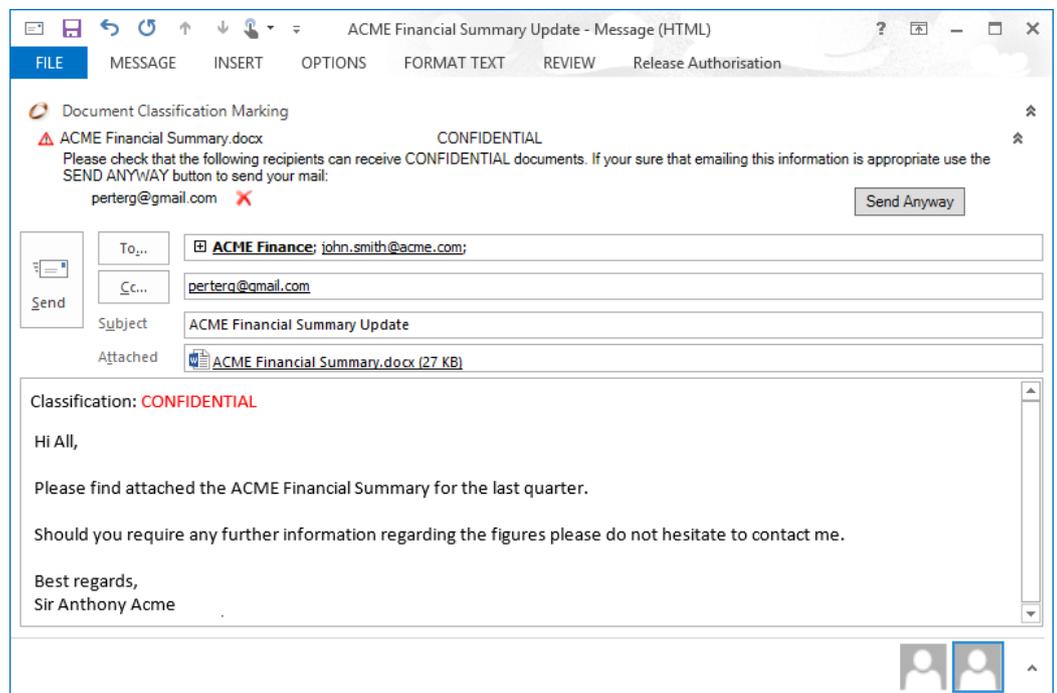




DCM Outlook 2015 provides policy driven control over domains to which DCM classified attachments can be emailed. Additional tags can be automatically added to an email's subject line/email body to indicate the classification of an email or to provide a release authorisation statement. DCM Outlook 2015 monitors **Emails, Meeting Requests** and **Appointments**.

Policies are easily defined against classifications or a specific document to deny, warn or allow the sending of classified information.

In the email example to the right, the Author has marked the attached document as Confidential. The Confidential classification policy is set to warn the sender giving them a chance to reflect on the security implications of sending such an attachment to, in this example, a recipient with a Gmail account.



DCM Collaboration allows the document author to grant specific users or groups (i.e. Contributors) the right to change the document classification - by default the classification of a document can only be changed by the author.

To the left we see that members of the ACME Finance group and one other has been granted this right within a document.

Authors and Contributors also have the right to add a specific email recipient(s); overriding the global Classification policy to enable a document to be sent to a given recipient(s) without the standard DCM Outlook attachment notification.