# DLP

**Data Leak Prevention (DLP) is a premium feature that is included as part of the Securemail Premium package.**

## **Why** DLP?

**Securemail's DLP helps IT managers who want to prevent sensitive and confidential information leaking out of the organisation via email. DLP reduces the opportunities and therefore mitigates the risk of such information leaking out through both employee ignorance, or criminal intent.**

Create peace of mind by implementing business rules and policies that effectively prevent the transmission of emails that contain sensitive content.

# **What** is Email Data Leak Prevention?

**The DLP module provides administrators with the means to enforce policies on outgoing email for the purposes of restricting, or monitoring, the transmission of certain classes of personal or company sensitive information as proscribed by either legislation or internal company policy.**

These classes of information relate to unauthorised transmission or sharing via email of personal or financial information of staff or customers as well as company proprietary or secret information which should not be disseminated externally. DLP can therefore be used to prevent and identify email based dissemination of this information by company users who perform these acts through either ignorance or genuine criminal intent.

## **How** does email DLP work?

- ✓ **DLP examines email subjects,** body text, body HTML, attachment file names as well as the body of any text based file attachments for content that matches sensitive or personal information.

- ✓ These patterns are either exact matches of **keywords and key phrases** defined by administrators, or system defined patterns (regular expressions) that can be selected to **identify major credit card numbers** and **SA ID numbers.**

- ✓ Administrators will be able to **apply a policy to a domain** by choosing what to scan for, and deciding whether or not to hold (quarantine) or allow these mails through with policy matches.

- ✓ Administrators can also **access reports that show the policy that was triggered** (e.g. SA ID number) and gain insight into where the data was found in the email as well as who sent it. They can also **choose to view the mail entirely** if the policy was set to hold and the mail is still quarantined on the Securemail platform. The mail may also be released at the administrators discretion.

## **What** does email DLP not cover?

Email based DLP cannot prevent employees from using other means to remove and disseminate sensitive information from company networks through the use of, for example, removable media drives or internet-based file sharing services. **Therefore, it is advisable to combine email DLP with a cohesive data management policy solution for endpoint and mobile devices.**

## **Benefits**

✓ **Protect against employee error or ignorance** from sending sensitive or confidential information outside of your organisation.

✓ **Understand the volume, frequency, and location of the matched data within mails** based on the rules and policies created.

✓ **Reduce the potential of costly backlashes** from occurring as a result of leaked information.

✓ **Manage an easy to use email DLP solution** with customisable rules and pattern matching policies.