How important is it for your email communications to be secure? Customers, colleagues, and partners want the peace of mind that comes from knowing that electronic conversations remain private and confidential. The Policy Based Encryption solution ensures that the specific security needs of your organization are met automatically.

Automatic Encryption
The Policy Based Encryption gateway automatically encrypts specific emails based on company-defined policies — that is, a set of rules designed to analyze all email, and encrypt any email that matches the pre-defined conditions. This cloud-based boundary encryption service does not require a client, or any user interaction to ensure the data is encrypted to the correct recipient. It simply and cost-effectively protects business data and helps to ensure regulatory compliance.

All of your stakeholders will benefit from adopting this solution. It is easy for service administrators to set up and configure, instantly rolling out the protection throughout the organization. The service is transparent to your users; individual senders do not need to decide what is and isn’t sensitive data and no extra steps are needed to encrypt messages. Email recipients can retrieve the encrypted messages easily, while encrypted replies provide two-way email security.

Key Benefits
- Automatic enforcement of company policies based on customizable rules
- Helps organizations meet regulatory compliance requirements for private and secure communications
- Centralized control of corporate email policies
- Protection against liabilities associated with privacy and security
- Improves employee productivity by eliminating manual work-arounds for sending secure data
Standard Features

- Enables sending and receiving of secure, encrypted email
- Re-directs and prevents confidential email from being distributed to the wrong people
- Enables organizations to audit employee usage and make changes
- Supports industry standard encryption
- Allows encrypted messages to be digitally signed and validated for compliance purposes
- Hides encryption complexities from the end user ensuring ease of use

How it Works

The service is completely cloud-based and does not require installation of appliances or software by senders or recipients—regardless of whether organizations or individuals exchanging emails with your business are also Policy Based Encryption clients or have their own encryption capabilities.

- Outbound email travels between the email server and the gateway via a TLS (Transport Layer Security) encrypted tunnel
- When used in conjunction with our email security services, you benefit from an added layer of security when your company’s email security and protection policies are applied to the encrypted email
- Each message has a unique AES encryption key to provide a higher level of security
- Secure portal allows external users to retrieve and reply to secure messages

Why Go Hosted?

Hosted Services provide all of the benefits of enterprise-class communication and collaboration solutions without the costs and headaches associated with managing them in-house. Benefits include:

- Instant access to enterprise-class communication and collaboration tools
- Reduced Total Cost of Ownership, no startup or maintenance costs associated with expensive on-premise hardware and software
- Easy to administer
- Simple and cost-effective to scale as business requirements change
- Free 24/7 customer support
- World-class security and reliability