VO Encrypt™
Security and Compliance in Action

Protecting your data is critical. VO Encrypt secures data in motion and at rest, locking down sensitive information sent or received through the VO Mail*plus* system. VO Encrypt supports company security policies and also requirements for compliance-governed fields such as banking, finance or healthcare.

Built-in Data Leak Prevention (DLP)

VO Encrypt encrypts and decrypts your incoming and outgoing email at the gateway level.

The built-in Data Leak Prevention (DLP) module can be used to prevent predetermined information, such as account numbers or personal client information to leave the organization via email.

Two methods of encryption (user-initiated and automatic) provide greater flexibility and security.

Users can initiate encryption of individual emails when the content is known to include sensitive data; and the DLP module will also continuously monitor to ensure that sensitive data is automatically captured and secured before it leaves your company's server.

Phone: (602) 297-5255
info@vofficeglobal.com

VIRTUAL OFFICE
The freedom of global collaboration

General features

- Settings can be specified at the domain and user level
- Automatic and manual encryption generation

PDF email encryption features

- Email is automatically converted to an encrypted PDF (including all attachments).
- PDF is encrypted with AES-128.
- PDF passwords are automatically generated and sent to the recipient by text message.
- The recipient can reply with the built-in secure portal.

128-BIT CIPHER
(AES 128)

PDF email encryption features

- Outgoing email can be scanned on keywords and regular expressions.
- Keywords and regular expressions can be specified at gateway, domain and user level.
- Messages can be blocked or quarantined when a rule is violated.
- Email encryption can be forced when a rule matches.
- Email bodies, attachments and nested attachments of type text, html, xml and other text-based formats are supported

How VO Encrypt Works

Each time an email is marked for encryption, the contents of the email, including any attachments are automatically converted to a secure password protected PDF format and emailed to the recipient.

After the process of encryption is complete, a separate notification with the password is sent to the recipient by text message. The recipient is required to enter their password to open the protected PDF message. This protocol protects sensitive information from potential cyber thieves by ensuring that securely encrypted content and the password required to access it are not stored in the same location.