Enterprise Securemail Service

January 14, 2019

Rates (per month)

- **Authorized** Securemail user (internal @nebraska.gov e-mail addresses) $1.20
- **Registered** Securemail user (external non @nebraska.gov e-mail addresses) No charge

Service Description

Securemail is a service that secures e-mails by encrypting e-mail and e-mail attachments and then delivering the e-mail to recipient mailboxes. This allows users to send or receive e-mails that contain sensitive information securely. Both internal (@nebraska.gov) users and external (@yahoo.com, @gmail.com, etc.) users are able to use Securemail to provide increased security for sensitive information shared via e-mail. The e-mail message body and attachments are encrypted, the TO, CC, BCC, and subject headers are not encrypted.

To use Securemail, an internal person must be an **Authorized State of Nebraska Securemail user** and an external person must be a CRES **Registered user**. **Authorized** users are configured by the Office of the CIO as part of the Securemail service via request to the OCIO Helpdesk, **Registered** users are configured by the e-mail recipient during the registration process that is initiated when they open their first secured e-mail.

The Securemail system is integrated with the State’s Enterprise directory services, messaging service email security infrastructure, and Cisco’s Registered Envelope Service (CRES). It offers two types of e-mail encryption, **FLAG** encryption done at the gateway or **DESKTOP** encryption done locally on the recipient workstation.

**FLAG** encryption is done with a predefined text string [Send Secure] in the subject of an outgoing e-mail and will only encrypt e-mails sent to an external recipient. See illustration below:

```
Subject: [Send Secure] Here is the information you requested
```

**DESKTOP** encryption is done with a preconfigured Outlook plug-in and can encrypt an e-mail to either an external recipient or an internal @nebraska.gov recipient. See illustration to the right.

When e-mails are encrypted by Securemail the e-mail message body and attachments are encrypted and then attached to a notification e-mail as an attachment titled securedocdatetime.html. The notification e-mail will have instructions for the recipient telling them that they have received a secured
e-mail and what steps they need to take to view the secured e-mail message.

![You have received a secure message](example_image)

Once registered external users can use [https://res.cisco.com/websafe](https://res.cisco.com/websafe) to initiate, respond, and forward secured e-mails. They also have the ability to store contacts, manage existing encrypted e-mails they have sent, and manage their CRES profile. E-mails sent from the CRES environment to @nebraska.gov recipients are sent via an encrypted connection to our gateway but the contents are not encrypted unless the TLS connection could not be established using encryption.

When a secured e-mail is sent using **FLAG** encryption to an external recipient the Exchange environment will recognize that the recipient of the email is not an internal mailbox, the e-mail will then be routed to the IronPort infrastructure. Once there, the IronPort infrastructure will detect the subject string and verify that the sender is an **Authorized Securemail** user and encrypt the e-mail and deliver the e-mail to the recipient system. If the sender is not an authorized user, the original email will be bounced back to the sender, along with a notification e-mail explaining that the **[Send Secure]** string is for **Securemail Authorized** users only. If saved these e-mails are stored unencrypted in the sender’s mailbox.

When a secured e-mail is sent using **DESKTOP** encryption to an internal or external recipient the Outlook plug-in will encrypt the e-mail locally and then send the e-mail. If saved, these e-mails are stored encrypted in the sender’s mailbox.

When the **securedocdatetime.html** attachment is opened, the recipient’s internet browser (or Outlook plug-in if installed) will send a request to the CRES environment to verify that the recipient is a **Registered** user. This process occurs in the background, if the recipient is registered, the user will be prompted for their CRES password to authenticate. In the background once the recipient is
authenticated an encryption key will be delivered to their workstation, the e-mail will be decrypted, and be displayed for the recipient to view. If the recipient is not registered, they will be prompted to register. Registration is a one-time process and consists of answering a few questions and setting a password in the CRES environment. If the password is forgotten there is an automated process for resetting the password.

The outlook plugin is available from the Office of the CIO and also provides SPAM, Phishing, Virus reporting capabilities for internal users. The plugin is not required for senders or recipients unless they want to initiate secured DESKTOP encrypted e-mails.

The service currently supports approximately 3,000 authorized internal users and 30,000 registered external users. The system secures on average 1,500 e-mails per day.

**Benefits**
- Sensitive information can be transferred via e-mail securely
- Helps entities retain regulatory compliance for protecting sensitive information (e.g., HIPPA, NITC security standards)

**Scope of Services**
Services include:
- Ability for internal and external users to send and receive secured emails
- Ability of external partners to initiate sending secured emails
- Self-registration by users once they receive an encrypted e-mail
- Automated password resets for Registered users
- Ability to lock e-mails by setting an expiration date on individual e-mails
- Ability to have a read receipt sent when encrypted e-mails are opened
- Decryption keys for encrypted e-mails are only available to the sender and recipient(s) accounts of the encrypted e-mail.
- OCIO can provide the Outlook Plug-in required to do DESKTOP encryption along with configuration file
- OCIO maintains the service infrastructure on redundant equipment and is made available 24x7x365 with scheduled monthly downtimes on the 3rd Tuesday of every month.
- OCIO performs troubleshooting for any service disruptions and has 24x7 support from the vendor.
Services provided by OCIO do not include:

- End-user training or assistance beyond documentation available
- End-user workstation troubleshooting
- External recipient support
- CRES Support for recipients having trouble opening e-mails:  
  https://res.cisco.com/websafe/help?topic=ContactSupport

For further information about Securemail, please contact:

Office of the CIO Help Desk

cio.help@nebraska.gov

402-471-4636 or 800-982-2468