



# Wisconsin Department of Revenue

## Common Questions: Sending Secure Encrypted Email

### General

1. [What is Email Encryption? Why Encrypt?](#)
2. [Is everyone on the State of Wisconsin Email System able to use it?](#)
3. [How does a message get sent encrypted? Can I send attachments?](#)
4. [What does the recipient see?](#)
5. [How will I know if a message I sent got encrypted, received or read?](#)
6. [What happens if the recipient's organization strips HTML attachments?](#)
7. [Can anyone register in the IronPort system? Can external users use our system to send inbound encrypted emails that are not replies to messages?](#)
8. [Is there a way to encrypt meeting requests with sensitive documents attached?](#)

### Mobile Devices

1. [Can a mobile devices send, receive and open encrypted email?](#)

### Security

1. [If there's a security breach, can DOR access email that were sent encrypted? Do we monitor who is sending encrypted emails?](#)
2. [What happens if I send an encrypted email to the wrong email address?](#)
3. [Can we block the recipients from forwarding a secure message?](#)
4. [Can I send encrypted mail listserv lists?](#)

### General

#### 1. **What is Email Encryption?**

An encrypted email is a secure message that allows only the sender and receiver to read the message and attachments in the message. Direct replies to encrypted messages are also encrypted. The encryption tool the State is using is Cisco IronPort, which transmits by Cisco Registered Envelope Service (CRES).

#### **Why encrypt?**

Encryption allows Department of Revenue (DOR) staff to communicate private information with individuals or third parties that are not part of the State of Wisconsin email system. This information, protected by State and Federal legislation, cannot be sent by regular email because it transmits in clear text.

#### 2. **Is everyone on the State of Wisconsin Email System able to use it?**

Yes. An "Encrypt Message" button has been added to your Outlook.

#### 3. **How does a message get sent encrypted?**

It can happen one of two ways:

- 1) By using the "Encrypt Message" button in Outlook. This button works like an on/off switch. Click once to encrypt email; click a second time to turn it off. When "Encrypt Message" is highlighted, it means encryption is turned on. Follow that by clicking "Send".
- 2) By manually typing [SEND SECURE], exactly as presented here including brackets, as the first thing in the message Subject field. This also will work with email sent through Outlook Web Access (OWA) via the internet.

**Can I send attachments?**

Attachments as large as 15MB can be included in your encrypted email. Some email systems may reject a message it considers too large. If you have multiple large attachments, you may want to send them in separate messages.

**4. What does the recipient see?**

The recipient gets a secure email message with instructions on how to open the email. The instructions will take the recipient through the steps to register (the first time) and open the encrypted email.

To better understand the recipients' experience and to assist them with questions, please review [Common Questions: Secure Encrypted Email](#) and the presentation [Opening a Secure Encrypted Email](#) found on the [DOR Internet](#). If you have additional questions, please contact the DOR Service Desk at (608) 266-8653.

**5. How will I know if a message I sent got encrypted, received or read?**

You can go to your Sent Mail and look for the message. Encrypted email will have [SEND SECURE] on the Subject line.

Encrypted messages generate a "read receipt" when the recipient opens the initial email that contains the link to the email. The "read receipt" confirms that the email was received, but not that the encrypted content was read.

**6. What happens if the recipient's organization strips HTML attachments?**

There are changes that can be made so people will receive encrypted emails. Please contact the DOR Service Desk if you encounter this problem.

**7. Can anyone register in the IronPort system?**

Yes. Registered users can log onto CRES at <https://res.cisco.com/websafe/root> to send a secure message. All messages sent this way will be encrypted prior to being delivered.

**Can external users use our system to send inbound encrypted emails that are not replies to a messages?**

A registered user can send secure messages to any recipient they choose, even if the intended recipient is not currently a registered user of CRES.

**8. Is there a way to encrypt meeting requests with sensitive documents attached?**

Meeting requests in Outlook do not have the "Send Secure" button on the tool bar so you will need to type [SEND SECURE] as the first entry of the subject line. The request will then be sent securely to outside invitees only.

**Mobile Devices****1. Can a Mobile Devices receive, open and reply to encrypted email?**

Yes, a mobile device can send a secure message, but you will need to type [SEND SECURE] as the first entry of the subject line. You can receive a secure messages as long as you can open the "securedoc.html" attachment on your mobile device.

## Security

**1. If there's a security breach, can DOR access email that were sent encrypted?**

DOR can access encrypted email.

**Do we monitor who is sending encrypted emails?**

DOR monitors who is sending encrypted emails.

**2. What happens if I send an encrypted email to the wrong email address?**

Contact the DOR Service Desk immediately to have the message blocked. Provide the Service Desk:

- 1) Your name and email address
- 2) The email recipients email address
- 3) The subject line of the email/
- 4) The Date and Time the email was sent.

Even if it has been read by the recipient, any more access can be blocked.

**3. Can we block the recipients from forwarding a secure message?**

This can be done by configuring rules for the agency By DOA/DET. The rules would apply to all encrypted email not on a message-by-message basis or for individual employees.

**4. Can I send encrypted e-mail to listserv lists?**

No. The list members would be instructed to go to CRES to open the message. The recipients can't open the encrypted email because their email address was not listed in the "To" field.