Sangamon County Email Security Protocols

Sangamon County is committed to securing information that is sent and received through the Sangamon County Email System. It is very important to understand that we deal with some very sensitive information for County employees and residents. Personal Identifiable Information (PII) encompasses social security numbers, date of birth, checking account numbers, credit card numbers, medical information, and much more.

There are applications available to send and request this information securely, and we encourage departments to contact us about utilizing these applications to protect the Information being shared back and forth in email.

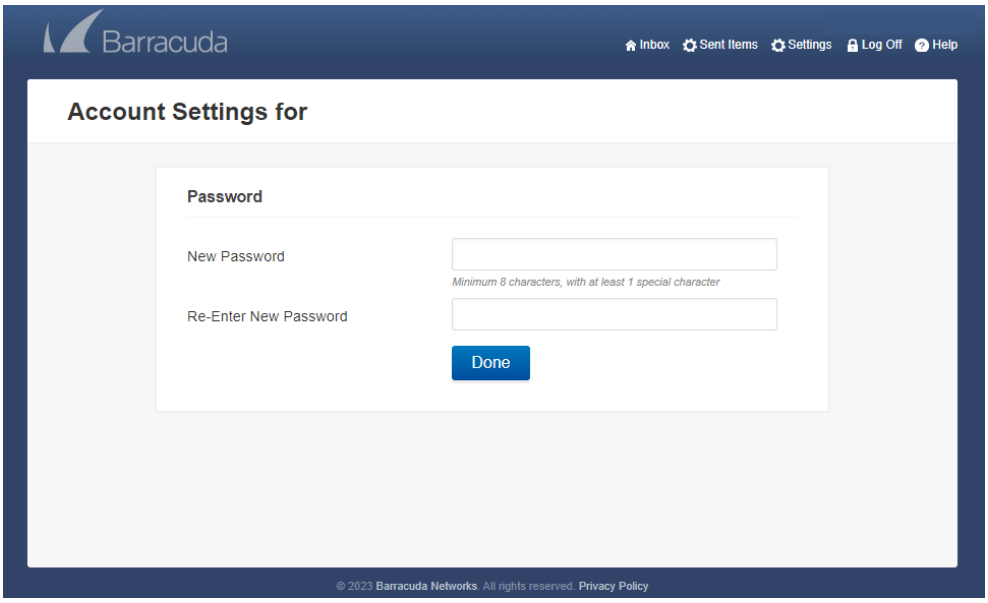
Secure FTP & Secure Mail Site: a product used by Sangamon County to request and send sensitive Information via secure mail. This product can also be used to send securely. It is also very useful for sending attachments that are too large for the email system.

Email Filtering: a product used by Sangamon County to filter emails coming in and going out for potential viruses, spam, and other malicious emails. Although there is no product on the market that will stop all malicious emails, a significant amount of malicious traffic is blocked every day.

Email Encryption: Email Encryption simply means the email you are sending is sent from our email system to the Barracuda Message Center. This is triggered via automatic or manual encryption (discussed below.) An email is sent to the recipient from no-reply@barracuda.com with a link. This link will take the recipient to the Barracuda Message Center where they will login to view the email you sent. Once they login, they will be able to view it and/or download it.

Tip #1: Before sending an encrypted email to someone, send them an email letting them know to expect an encrypted email from you. If you speak to the person regularly, you could even give them a call.

Tip #2: If you are sending an encrypted email to someone you have never sent an encrypted email to before, you could include a note that once they click the link to view the email they will be asked to set a password. This will only happen the first time they receive an encrypted email from you. The password does not expire, so they will need to make a note of the password. If forgotten, they can reset the password.



Automatic Encryption: There are two types of PII that will cause the email to automatically encrypt: social security numbers and credit card numbers (or anything that uses the same format.)

Manual Encryption: When typing an email, you may add either of the following words with quotes to encrypt the email: “secure” “encrypt”

User’s Guide for Barracuda Message Center: Click to open for instructions on how recipients of encrypted emails will access the encrypted email. If you would like to familiarize yourself with what the recipient sees, you can send test encrypted emails to an email account outside of the County email system that you have access to. Information Systems is available to do a demo of the process by contacting our Help Desk at ext. 3171. Internal emails do not go through the email filter, so those emails will not be encrypted even if you type “secure” or “encrypt” in the email.