

From: Devin Allman
Sent: Friday, August 31, 2018 10:42 AM
Subject: Weekly Cybersecurity Tips

Weekly Cybersecurity Tips

As a government entity, many of the regulatory compliance frameworks to which Lancaster County must adhere require employees to encrypt all private, confidential, or otherwise sensitive information that is transmitted via e-mail.

Per most standard compliancy requirements, the definition of *sensitive information* typically ranges from social security and credit card numbers to birth dates, medical information and everything in between.

While the ideal scenario would be to never send sensitive information across e-mail, this is not a practical expectation. When employees encounter situations in which circumstances require that sensitive information be transmitted via e-mail, it is important that appropriate steps be taken to properly secure such transmissions from interception and dissemination.

The most effective way to secure e-mail communication is through the use of encryption. To encrypt an e-mail, employees must place either the *encrypt* or *SECURE* keyword at the beginning of an e-mail's subject line.

Examples:

Subject: encrypt Civil Process Reminder
Subject: SECURE Background Check Results
Subject: SECURE FW: Warrant Request
Subject: encrypt RE: Litigation Information

If you ever find yourself questioning whether or not an e-mail should be encrypted, then you already have your answer – trust your gut instinct and encrypt the message. When it comes to cybersecurity, it is always best to err on the side of caution – *better safe than sorry*.

– The IT Department



LANCASTER COUNTY
South Carolina

Tickets: support.lancastercountysc.net
E-mail: support@lancastercountysc.net