

## The Email Security Policy

Email and text messages are quickly becoming the most globally used form of communication. Text communications are a quick and easy way to contact multiple people at the same time with the same message, allow us to send files without wasting paper, and can help us to get important and emergency messages. Email encryption is simply a way to make sure that the email you send to someone actually came from you and that it was not modified on its route. Email Security can be implemented into a security policy along with other important topics.

Here are some sample statements that can be implemented in an email security policy regarding email security:

- Personnel should understand the rights granted to them by the organization in respect of privacy in personal e-mail transmitted across the organization's systems and networks. Human Resources Department should incorporate a suitable wording into employee contracts to ensure that this privacy issue is fully understood.

- Personnel should not open emails or attached files without ensuring that the content appears to be genuine. If you are not expecting to receive the message or are not absolutely certain about its source, do not open it.

- Confidential and sensitive information should not be transmitted by e-mail - unless it is secured through encryption or other secure means.

- Personnel should be familiar with general e-mail good practice e.g. the need to save, store and file e-mail with business content in a similar manner to the storage of letters and other traditional mail. E-mails of little or no organizational value should on the other hand be regularly purged or deleted from your system.

More information can be found in the Information Security Policy Templates available at <http://www.information-security-policies.com> .

As an individual it would be beneficial for you to find out what your organization's email security policy is and if your organization supports an email encryption application. If it does not have one or either of these, it may be time to address this issue with your IT support team and your management team. These types of policies not only help an organization meet compliances for security required by your organization's policies and even legislative acts but also help you and your organization maintain their good names.

Beyond your organization's security policy you should make sure you have a solid understanding of your security role within an organization. SCP's Security Awareness e-course contains in-depth discussions on policy and good email practices from the view point of the end-user. For more information contact your local SCP Authorized Training Partner or contact the SCP Team.

*Tracy Richter, [Security Certified Program](#) Channel Manager*