

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## **Personnel Security – *Email Communications Standard***

### **PURPOSE**

To ensure that:

1. VCCS uses email in an ethical manner in compliance with applicable laws and with rules for acceptable use established by VCCS.
2. Email users are alerted to concepts of privacy and security as they apply to emails.
3. The risks of disruptions to VCCS email and other services and activities are minimized.

### **SCOPE**

This document applies to all email produced on VCCS IT resources or transmitted or received by VCCS for informational purposes.

### **APPLICABILITY**

The Email Communication Security Standard is applicable to the System Office and all colleges.

### **STANDARD**

The confidentiality of email cannot be assured. It can easily be modified, saved, copied, forwarded on to others and intercepted by unscrupulous individuals. Users should exercise extreme caution when using email to communicate, and should not assume their email is private or confidential.

No user of email services should have any expectation of privacy in any message, file, image or data created, sent, retrieved or received by use of VCCS equipment and/or access.

The VCCS and SVCC has the right to monitor any and all aspects of their mail systems including email sent or received by VCCS users. Such monitoring may occur at any time, without notice, and without the user's permission.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## **Personnel Security – *Email Communications Standard***

### **Requirement:**

Email must not be used to distribute or obtain copies of information designated as **Sensitive or Confidential** without authorization from the appropriate supervisor or as defined in the IT Information Security Standard (SEC501-01 r4 dated July 24, 2008). Emails containing information classified as **Sensitive or Confidential** should not be sent over any email system, unless encrypted.

The IT Network administrator at SVCC and the System Office are responsible for identifying and implementing procedures and supporting software, where applicable, for encrypting email content.

### **Requirement:**

The following describe prohibited and acceptable use of VCCS email:

#### **Prohibited Use:**

- The VCCS email system shall not to be used for the creation or distribution of any messages that could be construed as disruptive or malicious. These messages include text or content that assigns and announces blame to another individual, or incite disgruntlement among the VCCS students, faculty, staff or patrons. Employees who receive any emails with this content from any VCCS employee should report the matter to their supervisor immediately.
- The VCCS email system shall not to be used for the creation or distribution of any offensive messages. Employees who receive any emails with this content from any VCCS employee should report the matter to their supervisor immediately.
- Knowingly sending chain letters or any other types of email spam from or to a VCCS email account is prohibited. These restrictions also apply to the forwarding of email received by a VCCS employee.
- Any activity that violates any provision of this standard, any supplemental standard adopted by VCCS, or any other policy, regulation, law or guideline as set forth by local, State, or Federal law.
- The use of VCCS email distribution lists for commercial and personal purposes is prohibited.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## **Personnel Security – *Email Communications Standard***

### **Acceptable Use:**

- Using a reasonable amount of VCCS resources for personal emails may be acceptable; as defined in the System Office and college standards.
- Work and non-work related email should remain separate. Use a personal email address for receiving or sending non-work related email such as: email subscriptions, personal financial information, and personal health information.

### **Requirement:**

Email distribution lists may be used for purposes directly related to the VCCS mission and goals and may not be used for commercial or personal purposes.

### **Optional:**

The Virginia Information Technology Agency (VITA) recommends that all agencies consider adopting an email disclaimer to be appended to every email originating from a COV owned system. Emails sent from Commonwealth systems are public records of the Commonwealth of Virginia and must be managed as such. They may contain information that is private and for use in accordance with VCCS business only. Appending an email disclaimer may provide some protection from liability in a court of law or prevention of a lawsuit being filed.

An email disclaimer is a set of statements that are either pre-pended or appended to emails in whole or by providing a link to the disclaimer. These statements are frequently used to create awareness of how to treat the data in the email. An email disclaimer is not a substitute for judgment on what content to put into an email.

Our review of other agencies and external organization indicate that those who elect to use an email disclaimer do so by appending the full text to each email. A survey of the VCCS College Information Security Officers (ISOs) and College Chief Information Officers (CIOs) resulted in a recommendation to use the full text. However, there is no COV or legal requirement that the full text is displayed or that by doing so will limit our liability. Therefore, it is possible to use abbreviated language with a “hot link” to the full text.

---

**SOUTHSIDE VIRGINIA COMMUNITY COLLEGE  
INFORMATION TECHNOLOGY  
SECURITY PLAN**

---

**Personnel Security – *Email Communications Standard***

After consultation with the College Information Security Officers and the System Office Legal Services Office the following language is approved as voted on by the Tech Council for adoption for system wide use:

*“CONFIDENTIALITY NOTICE: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information or otherwise be protected by law. Any access, use, disclosure or distribution of this email message by anyone other than the intended recipient(s) is unauthorized and prohibited. If you are not an intended recipient (or an agent acting on an intended recipient’s behalf), please contact the sender by reply e-mail and immediately destroy all copies of the original message. Virus scanning is recommended on all email attachments.”*