

# **INFORMATION SYSTEMS**

## **Policy 50150: Information Technology Access Control**

### **1. Purpose**

The College is responsible for assuring the integrity of its computer systems, applications, and utilities. All systems, applications, and utilities are deemed to be the property of the College and not an individual user or department.

### **2. Policy**

The Security Officer for the College shall be the Technology Support Services Manager. The Security Officer shall be responsible for determining appropriate physical security, access control, and contingency plans for information and communication services. Certain duties of this assignment may be delegated to others, such as initiating, modifying, and terminating access to users for various applications and/or to the network. All applications should employ a system of user identifications and passwords, at a minimum, to limit access to valid users. If provided, features limiting access to screens, modules, or other sub-units within software should be employed. Every user is accountable for safeguarding his or her access codes and for the integrity of the systems and data. Every user is responsible for periodically changing passwords in compliance with the application, system, and/or utilities requirements.

### **3. Procedures**

The Security Officer shall work with the custodian of each system, application, and/or utility to determine the appropriate security measures. If a custodian is designated as a security officer for an application, information about the designee and the scope of responsibility shall be recorded and filed by the College Security Officer. Department and work unit managers are responsible for ensuring employees are provided the necessary access to successfully complete their assignments.

Employees leaving their current areas of responsibility for any reason shall have access to all computer applications, systems, and utilities unique to that position revoked in a timely manner. The supervisor of the employees shall verify that the employee has requested revocation of information technology access to the appropriate security officer. Human Resources is also charged with notifying the College Security Officer of the termination of any employee. The College Security Officer shall ensure all rights to information technology no longer required by the employee are revoked.

All users of the Germanna Community College and Virginia Community College System networks are responsible for being aware of this policy. Violations of this policy that result in inappropriate or improper use of College resources or that subject the College to unnecessary risk are subject to disciplinary action as prescribed by College, VCCS, and/or State guidelines, policies, and/or procedures. Anyone who has reason to suspect breach of this policy by another person should immediately report it to the Technology Support Services Manager.

#### **4. Definitions**

Custodian – individual or unit responsible for “keeping” the data and the applications and systems supporting it.

Risk – the likelihood or probability that critical applications or confidential or sensitive information will be subject to unavailability, loss, unauthorized modification, or improper disclosure.

User – one who has access to a system.

#### **5. References**

Commonwealth of Virginia, Council on Information Management, ITRM Standard 95-1, Information Technology Security.

Virginia Polytechnic and State University, Administrative Policy 2020: Policy on Protecting Electronic Access Privileges.

Virginia Polytechnic and State University, Administrative Policy 2015: Acceptable Use of Computer and Communication Systems.

#### **6. Point of Contact**

Created by Richard L (Rick) Brehm, Vice President for Administrative Services

#### **7. Approval and Revision Dates**

Approved by President’s Council on August 6, 2001.