
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Contingency Planning and Business Recovery Program *IT Security Roles and Responsibilities*

Information technology security roles are assigned to individuals to ensure accountability and compliance among the information technology processes. The role or working title and assignment of personnel for each security role may differ at each college however it is critical that each function be identified and the individuals assigned have the appropriate skill sets. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests.

Required:

College Presidents Agency Head (Jan 2010 revision) – The SVCC President, Dr. John Cavan, is responsible for college's IT systems and data. His IT security responsibilities include: Designate via e-mail to an ISO for the College and providing the employees name, title and contact information to VCCS annually or as personnel changes are made. The College President is strongly encouraged to designate at least one backup for the ISO, as well. **Agencies with multi-geographic locations or specialized business units should consider designating deputy ISO's as needed. (Jan 2009 Revision)**

The SVCC ISO and backup ISO are designated and documented via the ISO designation form (Section B 1 of the SVCC Security Plan).

1. Designate via e-mail to the VCCS **biannually (Jan 2010 revision)** an ISO for the College and providing the employees name, title and contact information to VCCS annually or as personnel changes are made. The College President is strongly encouraged to designate at least one backup for the ISO, as well.
2. Determine the optimal place of the IT security function within the College hierarchy with the shortest practicable reporting line to the College President.
3. Maintain an IT security program that is sufficient to protect the College's IT systems, and that is documented and effectively communicated.
4. **Review the IT System Security Plan for each sensitive agency IT system and disapprove those that do not provide adequate mitigation of risks to which the IT system is subject. (Jan 2010 revision)**

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

Contingency Planning and Business Recovery Program
IT Security Roles and Responsibilities

5. Review and approve the College's Business Impact Analyses (BIA), a Risk Assessment (RA), and a Continuity of Operations Plan (COOP), to include an IT Disaster Recovery Plan, if applicable.
6. Accept residual risk as described in section 2.5 of the *IT Security Audit Standard* (COV ITRM Standard SEC502-00).
7. Maintain compliance with *IT Security Audit Standard* (COV ITRM Standard SEC502-00) and the guidance provided in the VCCS Contingency Planning and Business Recovery Program. This compliance must include, but is not limited to:
 - a. Requiring development and implementation of the College Contingency Planning and Business Recovery Program, and submitting the Annual Statement of Compliance to the System Office;
 - b. Requiring that the planned IT security audits are conducted;
 - c. Receiving reports of the results of IT security audits;
 - d. Requiring development of Corrective Action Plans to address findings of IT security audits; and
 - e. Reporting to the System Office all IT security audit findings and progress in implementing corrective actions in response to IT security audit findings. .
8. Facilitate the communication process between IT staff and those in other areas of the College.
9. Establish a program of IT security safeguards.
10. Establish an IT security awareness and training program.
11. Provide the resources to enable employees to carry out their responsibilities for securing IT systems and data.
12. Ensuring managers in the colleges at all levels provide for the IT security needs under their jurisdiction and they take all reasonable actions to provide adequate IT security and to escalate problems, requirements, and matters related to IT security to the highest level necessary for resolution.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Contingency Planning and Business Recovery Program *IT Security Roles and Responsibilities*

13. Maintain an organization chart that depicts the reporting structure of employees with specific responsibilities for the security of IT systems and data and their specific IT security roles and responsibilities. (Jan 2009 Revision 4)

14. Review System Security Plans for all sensitive agency IT Systems. Approve those System Security Plans that provide adequate protection against security risks. Disapprove System Security Plans that do not provide adequate protections against IT security risks, and require that the System Owner implement additional security controls on the IT System to provide adequate protection against IT security risks. (Jan 2009 revision)
Approval given in Compliance Statement, Section K.

15. Review the position descriptions of all employees assigned to IT security roles annually, or more often as necessary, and verify that the position descriptions accurately reflect assigned IT security duties and responsibilities. (July 2008 revision) IT security roles and responsibilities will be given on the proper EWP's. The appropriate supervisors will use the EWP to review and validate the assignment of the roles and responsibilities during annual employee evaluations.

16. Each Agency Head or designated ISO shall: (Jan 2010 revision)
 1. Identify a System Owner who is generally the Business Owner for each agency sensitive system. Each System Owner shall assign a Data Owner(s), Data Custodian(s) and System Administrator(s) for each agency sensitive IT system.
 2. Document each sensitive IT system owned by the agency, including its ownership and boundaries, and update the documentation as changes occur.
 3. Identify individuals to the System Owner role required by this *Standard* and have the System Owner assign other roles.

Note: Data and systems, belonging to a single agency, that have the same technical controls and account management procedures (i.e. Microsoft SharePoint, PeopleSoft), may be classified and grouped as a single set of data or systems for the purpose of inventory, data classification, risk assessments, security audits, etc.

College Information Security Officer (ISO) - The ISO at SVCC is responsible for making recommendations to President's Staff for the development and administration of the college Contingency Planning and Business Recovery Program as well as the college local IT security architecture. The final plan must be approved in writing by SVCC President's Staff. The ISO for

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Contingency Planning and Business Recovery Program *IT Security Roles and Responsibilities*

SVCC is Mr. Will Hamilton, IT Security Analyst and Contingency Planning Coordinator. The ISO is expected to perform the following duties:

1. Recommend to SVCC administration a college IT security program that meets or exceeds the requirements of VCCS and COV IT security policies and standards in a manner commensurate with risk. All aspects of the program are subject to the written approval of SVCC administration (President's Staff). SVCC President's Staff is responsible for the content of the final plan and all associated appurtenances thereto.
2. Develop and maintain an IT security awareness and training program for the college staff, including contractors and IT service providers.
3. Coordinate and provide IT security information to the VCCS ISO as required.
4. Recommend to SVCC President's Staff a course of action to implement and maintain the appropriate balance of protective, detective and corrective controls for college and VCCS IT systems commensurate with data sensitivity, risk and systems criticality. All aspects of the program are subject to the written approval of SVCC administration (President's Staff). SVCC President's Staff will determine the content of the final plan and all associated supporting documentation.
5. Mitigate and report all IT security incidents in accordance with §2.2-603 of the *Code of Virginia* and related VCCS requirements and take appropriate actions to prevent recurrence.
6. Maintain liaison with the VCCS ISO.

Note: The ISO should report directly to the Agency Head where practical and is responsible for developing and managing the agency's information security program. (Jan 2010 Revision)

Privacy Officer- An agency must have a Privacy Officer if required by law or regulation, such as the Health Insurance Portability and Accountability Act (HIPAA), and may choose to have one where not required. The Privacy Officer provides guidance on:

- a. The requirements of state and federal Privacy laws.
- b. Disclosure of and access to sensitive data.
- c. Security and protection requirements in conjunction with IT systems when there is some overlap among sensitivity, disclosure, privacy, and security issues. (Jan 2010 Revision)

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Contingency Planning and Business Recovery Program *IT Security Roles and Responsibilities*

System Administrators - The System Administrator is an analyst, engineer, or technician who implements, manages, and/or operates a system or systems. The System Administrator assists College and System Office management in the day-to-day administration of the IT systems, and implements security controls and other requirements of the local IT security program on IT systems for which the System Administrator have been assigned responsibility. Typically in the VCCS these are SIS Security Officers, LAN Administrators, Network Security Engineers, etc. The System Administrators for SVCC are as follows: Ms. Robin Daniel, Peoplesoft Administrator, AIS Security Administrator, and Ms. Kelly Goscinski, Blackboard Administrator, Chad Wollenberg, IT Network Engineer.

SIS / AIS Security Administrator - The Security Administrator manages security controls over networks and systems to prevent improper or unauthorized use of data. The Security administrator, Ms. Robin Daniel, will be so designated on her SVCC Employee Work Profiles (EWP).

Superuser - As a part of the AIS and SIS security model VCCS provides a special set of permissions, often described as the "Super User" role, which has access to all panels (navigations) available in the system except those supporting security administration and the "Enrollment" panel. The role as defined also permits those who are assigned this role full authority to read, change, and delete the information stored in the associated databases. The Superusers, Robin Daniel, Anne Yancey, Wendy Ezell, will be so designated on her SVCC Employee Work Profiles (EWP).

In accordance with COV SEC501-01 standard and the VCCS Personnel Security standard the principle of least privilege must be used by each college and the System Office in the assignment of security roles and responsibilities. Faculty, staff, administrators, and other users requiring access to enterprise systems should be granted only those privileges necessary to perform their normal work duties as documented in their employee work profile or other formal documents that detail job duties. Therefore given the current authority and scope of access assigned to the *Super User* security role access must be strictly limited to those personnel as determined by the needs of the colleges and System Office. However the following must apply:

1. Assignments in the production instance (except VCCS security administrators) shall not exceed 90 days and the request must be submitted with a start and end date. Upon expiration of the time period *Super User* access shall be removed immediately.
2. All requests should be fully documented outlining the specific work to be accomplished.
3. Request for access to the production instance must be authorized by the immediate supervisor, agency head or their designee, the data owner, and system owner.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Contingency Planning and Business Recovery Program *IT Security Roles and Responsibilities*

4. The entity (college or System Office) who grants an individual the *Super User* role is responsible for ensuring that the individual(s) assigned to this role has all the required knowledge, training, and related skill sets necessary to effectively perform the work under the *Super User* security role.
5. Each use of the “Super User” role shall be documented in written and/or electronic form showing the date of use and scope of use (print screens for example). For table changes, document the state of the table information before and after the change and/or the state of the table information before and after use.
6. The information security officer must maintain a file of all requests and written and/or electronic documentation for *Super User* for periodic review by the Internal Audit Office and VCCS Security Office. These records shall be stored and safeguarded in a manner consistent with all applicable record retention policies and guidelines and made available upon request.
7. Any exceptions to this standard must be fully documented by the college and the information forwarded to the VCCS Security Office for verification and review.

Access methods, like the *Super User*, are at risk for potential abuse primarily through well-intentioned misuse. In the extreme, changes to the production application and database using the *Super User* can leave elements of the database in an error state, and the validity and integrity of student and institution data could be compromised. This standard proposes a set of practical procedures for safeguarding the VCCS IT enterprise applications and data.

IT System Users - System users will be so designated on their SVCC Employee Work Profiles (EWP). Users are defined as COV employees having access to an information system or its data and not specifically given any other IT security role. All users of COV IT systems including employees and contractors are responsible for the following:

1. Read and comply with VCCS Contingency Planning and Business Recovery program requirements as well as VCCS and college IT policies, standards, and guidelines.
2. Report breaches of IT security, actual or suspected, to their college management and/or the ISO.
3. Take reasonable and prudent steps to protect the security of IT systems and data to which they have access.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Contingency Planning and Business Recovery Program *IT Security Roles and Responsibilities*

System Owner - The System Owner is the manager responsible for operation and maintenance of an IT system. With respect to IT security, the System Owner's responsibilities include the following: (Jan 2010 Revision)

- a. Require that all IT system users complete required IT security awareness and training activities prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.
- b. Manage system risk and developing any additional IT security policies and procedures required to protect the system in a manner commensurate with risk.
- c. Maintain compliance with COV IT security policies and standards in all IT system activities.
- d. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.
- e. Designate a System Administrator for the system.

Note: Where more than one agency may own the IT system, and the agency or agencies cannot reach consensus on which should serve as System Owner, upon request, the CIO of the Commonwealth will determine the System Owner.

The System Owners for SVCC are listed below:

Business Unit

Academic & Student Affairs
Administrative and Financial Services
Adult Education
Dual Enrollment

Enrollment Management
Financial Aid
Information Technology
Institutional Advancement
Institutional Effectiveness
Library, Learning Resources
Middle College
Off Campus Instruction

System Owner

Roberts, Sykes: Provosts
Hunt: VP of Finance
Sheffield: VP of Adult Ed & Grants
Feinman: Dean of Instruction; Hawkins,
Coordinator of DE

Richey: Dean of EM
Richey: Dean (as above)
Ancell: Dean of Information Services
Elkins: Dean of IA
Patton: Dean, IE
Ancell: Dean of LR & IT
Sheffield: VP of Adult Ed & Grants
Smiley: Coordinator of OCI

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Contingency Planning and Business Recovery Program *IT Security Roles and Responsibilities*

President's Office
Southern VA Higher Ed Center
Student Services
Workforce Development & Continuing Education

Cavan: President
Roberts: Provost
Roberts, Sykes: Provosts
Roberts: VP of WD and CE

Data Owners: – the entity, group or individual that has ultimate responsibility for the creation and modification of information stored in a database or other system. The data owner is responsible for ensuring that the System Owner has implemented sufficient security in the system platform to safeguard the applications and data stored on that server.

The Data Owner is the agency manager responsible for the policy and practice decisions regarding data, and is responsible for the following: (Jan 2010 Revision)

- a. Evaluate and classify sensitivity of the data.
- b. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.
- c. Communicate data protection requirements to the System Owner.
- d. Define requirements for access to the data.

Data Owners for SVCC are listed below:

Business Unit

Data Owner:

Academic & Student Affairs

Feinman, Shannon: Wisbey, Tom:
Deans of Instruction

Adult Education

Thompson, Sandra: Director

Administrative & Financial Services (listed below)

Payroll

Williams, Virginia: Payroll Tech

Human Resources

Harris, Bethany: HR Manager

Human Resources

Lenhart, Janet: Leave Tech

Business Office

Daniel, Diane: Business Manager

Facilities Management

Wooding, Dale; Wray, Roger: B&G
Supervisor

Assessment, Research, and Planning

Yancey, Anne: IE coordinator

Dual Enrollment

Feinman, Shannon, Hawkins, Rosa:
Coordinators

Enrollment Management

Richey: Dean of E M

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Contingency Planning and Business Recovery Program *IT Security Roles and Responsibilities*

Financial Aid
Information Technology

Institutional Advancement
Library, Learning Resources
Middle College

Off Campus Instruction

President's Office
Student Services

Southern VA Higher Ed Center
Workforce Development & Continuing Education

Tharrington, Sally: Director
Ramsey, Lydia, Chandler, Aaron;
Lewis, Marysue; Jenkins, Linda,
Wollenberg, Chad: Techs
Elkins, Mary: Dean of IA
Blanton, Libby; Lewis, Ernestine: Sup.
Griles Lois; Pegram, Kathy
Admin & Office Specialist
Gilliam, Bonnie; Cifers, Gary;
Smiley, Debra; Quicke, Duncan:
Site Directors
Turner, Nancy: Administrative Assistant
Sizemore, Dorothea; Shepherd, Judy:
Directors
McDaniel, Earl: Director
Campbell, Debbie; White, Anita:
Admin Assistants
Smith, Dennis: Director

In order to satisfy the ITRMSEC501-01 and the VCCS standard for Contingency Planning and Business recovery Program: *IT Roles and Responsibilities*, some people will need to have changes made to their EWP's. The changes indicate their IT roles and responsibilities as defined in the standard and during the BIA process. Employees and the additions to the EWP's are as follows:

Employee:

Ancell, Jack
Blanton, Libby
Campbell, Debbie
Cavan, John
Chandler, Aaron
Cifers, Gary
Daniel, Diane
Daniel, Robin

Elkins, Maryjane
Ezell, Wendy
Feinman, Shannon
Gilliam, Bonnie
Goscinski, Kelly

Addition to EWP:

System Owner
Data Owner
Data Owner
System Owner
Data Owner
Data Owner
Data Owner
System, Security Administrator,
SIS Superuser
System Owner, Data Owner
Data Owner, Superuser
Data Owner, System Owner
Data Owner
Data Owner

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Contingency Planning and Business Recovery Program *IT Security Roles and Responsibilities*

Griles, Lois	Data Owner
Hales, Christie	Data Owner
Hamilton, Will	ISO, Contingency Planning Coordinator, IT Disaster Planning Coordinator, BIA/RA Coordinator IT COOP Plan Coordinator
Sizemore, Dorothea,	Data Owner
Harris, Bethany	Data Owner
Hawkins, Rosa	Data Owner
Hunt, Peter	System Owner
Jenkins, Linda	Data Owner
Lenhart, Janet	Data Owner
Lewis, Ernestine	Data Owner
Lewis, Marysue	Data Owner
Mc Daniel, Earl	Data Owner
Newman, Susan	Data Owner
Patton, Chad	System Owner
Quicke, Duncan	Data Owner
Ramsey, Lydia	Data Owner
Reynolds, Tom	System Owner
Richey, Brent	System Owner, Data Owner
Roberts, Al	System Owner
Seamster, Patricia	Data Owner
Sheffield, Linda	System Owner
Shepherd, Judy	Data Owner
Smiley, Debra	Data Owner
Smiley, Misty	Data Owner
Smith, Dennis	Data Owner
Smith, Shana	Data Owner
Sykes, John	System Owner
Tharrington, Sally	Data Owner
Thompson, Sandra	Data Owner
Townsend, Rosa	Data Owner
Turner, Nancy	Data Owner
White, Anita	Data Owner
Williams, Virginia	Data Owner
Wisbey, Tom	Data Owner
Wollenberg, Chad	Data Owner
Wooding, Dale	Data Owner
Wray, Roger	Data Owner

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Contingency Planning and Business Recovery Program *IT Security Roles and Responsibilities*

Yancey, Anne

Data Owner, SIS Superuser

IT Staff members will perform the following functions as stated in the SVCC Security Plan.

1. Develop the backup and restoration procedures for all IT equipment.
2. Perform the backups as determined above.
3. Maintain auditable copies of all documentation associated with functions 1 and 2. For example, backup-schedules, logs, media storage, etc.
4. Maintain published emergency backup and restoration plans approved by the System Owners.
5. Maintain auditable copies of IT systems security configurations.
6. Maintain auditable copies of data storage media handling logs.
7. Be the Data Custodians responsible for protection of data in their possession from unauthorized access, alteration, destruction, or usage.
8. Meet the requirements of the IT Systems Security: *Malicious Code Protection* standard.
9. Maintain auditable copies of all necessary documentation associated with the VCCS Threat Management standards.
10. Maintain auditable copies of password management documentation.
11. Maintain auditable copies of all necessary compliance documentation associated with the [ITRM Standard SEC514-03](#) (Removal of COV data from surplus computer hard drives and electronic media standard)
12. Maintain and update annually a list of approved software; All software must be properly licensed and documented for audit purposes.
13. Maintain auditable copies of all configuration and infrastructure changes as given on the SVCC change request form.

IT Network Administrators are responsible for the following as stated in the SVCC Security Plan.

1. Develop, implement, maintain, and document an IT system data backup and restoration plan.
2. Perform vulnerability scanning at least annually; Conduct Intrusion Detection and Intrusion Prevention log reviews.
3. Monitor and document all security and event logs for IT equipment as necessary.
4. Specify the type of actions a particular program or device can take, based on the possible security implications, when suspicious or malicious traffic is detected.
5. Provide a general description of system architecture and functionality. Indicate the operating environment, physical location of all campuses, building plans indicating general location of users, and partnerships with external organizations/systems. Include

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Contingency Planning and Business Recovery Program *IT Security Roles and Responsibilities*

information regarding any other technical considerations that are important for recovery purposes, such as backup procedures (reference [IT System and Data Backup and Restoration](#)). Provide a diagram of the architecture, including security controls and telecommunications connections.

6. Develop and maintain all security configurations for IT equipment; reapply after any changes to IT equipment.
7. Define, determine, and document local machine and LAN access for SVCC IT users.
8. Ensure that at least two employees have administrative account access to each IT system.
9. Document and store passwords securely.
10. Restrict and log the handling of all data storage media containing sensitive data to authorized personnel only.
11. Comply with the procedures given for removal of data from electronic or magnetic storage media as given in the [ITRM Standard SEC514-03](#).
12. Do risk analysis and approve changes to sensitive or critical hardware, software, or IT infrastructure using the SVCC configuration management change control procedure.

Members of the Incident Response Team need to be so designated in their EWP's. The team members are: Lydia Ramsey, Marysue Lewis, Chad Wollenberg, Christie Hales, Peter Hunt, Dale Wooding, Roger Wray, and Will Hamilton.

Members of the SVCC Security Committee will review and revise all security configurations. Committee members are: Dr. Al Roberts, Dr. John Sykes, Peter Hunt, Will Hamilton, Robin Daniel, and Jack Ancell. These functions will be added to the appropriate employees EWP or position descriptions following normal SVCC procedures during annual EWP supervisor reviews for the year 2007-2008.

Data Custodian - Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:

1. Protect the data in their possession from unauthorized access, alteration, destruction, or usage.
2. Establish, monitoring, and operating IT systems in a manner consistent with VCCS and COV IT security policies and standards
3. Provide Data Owners with reports, when necessary and applicable

Separation of Duties

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

Contingency Planning and Business Recovery Program
IT Security Roles and Responsibilities

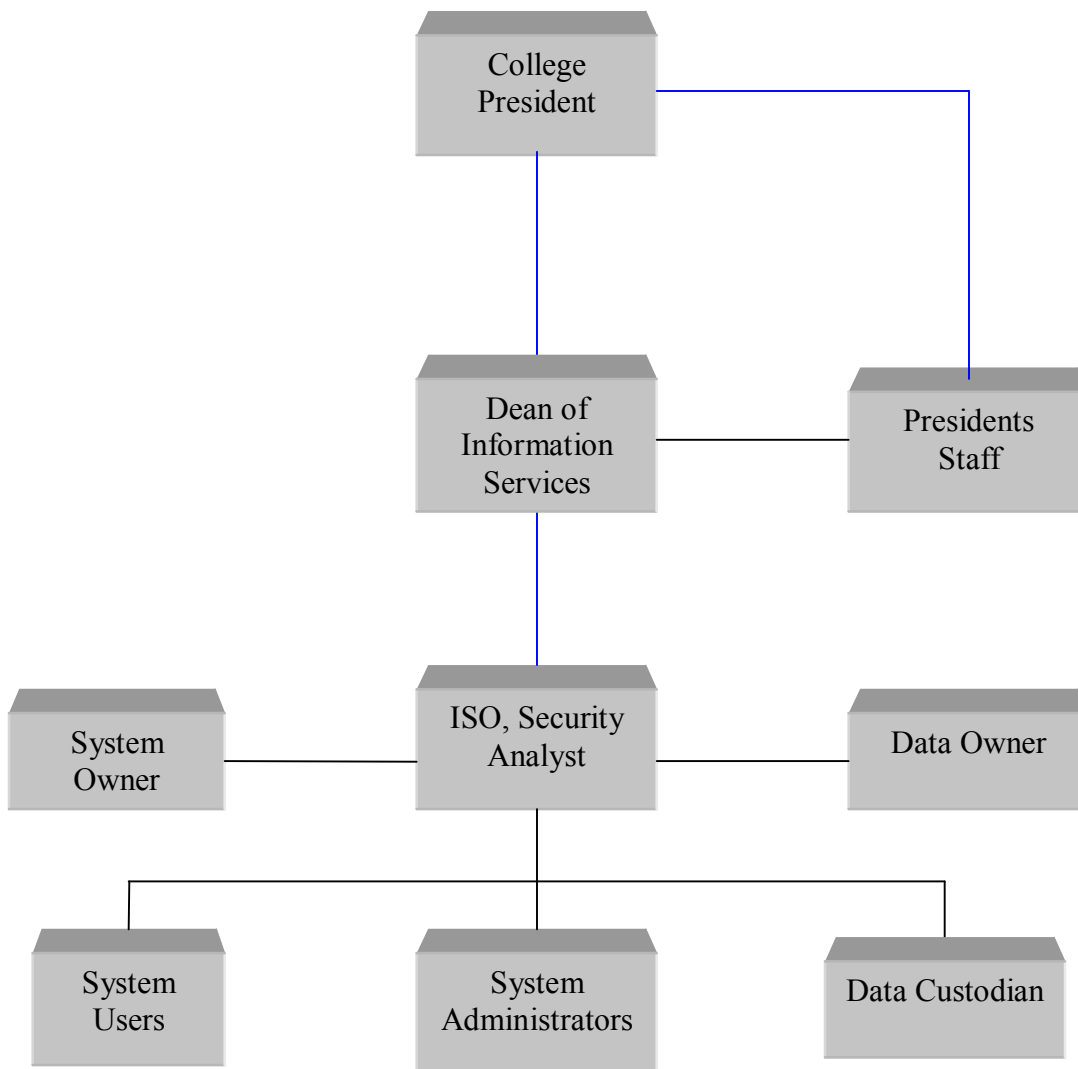
When assigning security roles the security concept of separation of duties should be maintained whenever possible. This includes assigning roles so that:

1. The ISO is not a System Owner or a Data Owner.
2. The System Owner and the Data Owner are not System Administrators for systems or data they own.
3. The ISO, System Owners, and Data Owners are Commonwealth of Virginia employees.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Contingency Planning and Business Recovery Program *IT Security Roles and Responsibilities*

I.T. Security Organizational Chart



Black lines: Communication
Blue lines: Reporting

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

Contingency Planning and Business Recovery Program
IT Security Roles and Responsibilities

The SVCC Information Technology Security Roles and Responsibilities and all associated documentation are approved as given in Section B1 of the SVCC Security Plan.

1. Date Reviewed: _____
2. Reviewed By: SVCC President's Staff _____
3. Approved By: _____
SVCC President: Dr. John Cavan