



**OFFICIAL POLICY**

10.0

**Employee Security Awareness  
Training**

1/24/19

**Policy Statement**

The purpose of the Human Resource and Security Awareness Policy is to define information security roles, responsibilities and required training for the College's employees who access the College's Information Technology systems.

---

**Policy Manager and Responsible Department or Office**

The Chief Information Security Officer (CISO) and the Office of Information Technology are responsible for the implementation of this policy.

---

**Policy**

**Security Policy and Procedures**

Security Awareness training is required for all employees with access to the College's Information Technology resources.

- The College shall define security roles and responsibilities of employees and shall document the assigned roles.

**Screening and Third-Party Personnel Security**

- The College shall ensure that background verification checks are conducted on all candidates selected for employment, as appropriate. Contractors and third party users are required to provide documentation that appropriate background checks have been conducted.

### **Termination and Transfer**

- Upon termination / transfer of employment for employees, termination of engagement for non-employees, or immediately upon request, personnel shall return to the College all agency information technology property and materials in their possession or control.

### **Access Agreements**

- As part of their information security training obligation, employees are subject to the College's Acceptable Use Policy 10.20, which shall state responsibilities for information security.

### **Security Awareness Training and Information Security Workforce**

- College management shall require employees to apply security in accordance with established policies and procedures of the organization.

### **Role-Based Security Training**

- The College shall impart appropriate awareness training and regular updates in organizational policies and procedures to all employees of the organization as relevant for their job function.
- Security training will be completed yearly or as deemed necessary to allow for new information security regulations to be incorporated into the training curriculum.
- User access to College information assets and systems will only be authorized for those users whose cyber security awareness training is current (e.g., having successfully completed the most recent required training stage). Failure to comply may result in revocation of system access and disciplinary action in accordance with the College's Code of Conduct and Disciplinary Actions Policy. Newly hired employees will be required to complete the training within 30 days of employment.

### **Testing, Training and Monitoring**

- The College's Information Security Office will appoint a cyber-security awareness training coordinator to manage training content, schedules and user training completion status.
- The College's cyber security training coordinator, along with the agency Chief Information Security Officer (CISO) or security manager will review training content on an annual basis to ensure that it aligns with State of South Carolina policies.

---

### **Departments/Offices Affected by the Policy**

All offices of the College are affected by this policy.

---

**Procedures Related to the Policy**

--

---

**Related Policies, Documents or Forms**

9.1.2 Employee Code of Conduct 9.2.1 Background Checks 10.20 Acceptable Use  South Carolina Information Security Policy – Human Resource (HR) and Security Awareness ( <a href="http://www.admin.sc.gov">www.admin.sc.gov</a> )
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

---

<b>Issue Date:</b> 1/24/19 <b>Date of Policy Revision:</b> 1/24/19	<b>Next Review Date:</b> 1/24/25
-----------------------------------------------------------------------	----------------------------------

<b>POLICY APPROVAL</b> <b>(For use by the Office of the Board of Trustees or the Office of the President)</b>	
Policy Number: 10.0	
President or Chairman, Board of Trustees <i>Stephen C. DeBourne</i>	Date: <u>1/24/2019</u>