COLLEGE of CHARLESTON

OFFICIAL POLICY

10.19	Data Loss Prevention Policy	07/01/16

Policy Statement

College IT Resources exist for the purpose of conducing legitimate business for the College. The College is bound by state and federal law to protect certain information that is transmitted using College IT systems, hardware, and networks. Pursuant to these objectives, the College has a duty to actively prevent the loss of Protected Information.

It is the policy of the College to engage in sustained and substantial efforts to provide for the confidentiality and integrity of Protected Information; to promptly discover and remedy any Security Breach or misuse of Information Technology Resources; and to expeditiously take those measures needed to reduce the probability of a Security Breach or a misuse of Information Technology Resources. This Policy is intended to further and not replace, in whole or in part, approved College Policies dealing with the collection, storage, maintenance, transmission and use of Data.

Policy Manager and Responsible Department or Office

Chief Information Security Officer - Information Security

Purpose/Reason for the Policy

This Policy establishes the principles by which the College of Charleston ("College") will identify, protect and respond to the unauthorized disclosure of Protected Information by electronic means. The specific purposes of this Policy are to:

(a) further enable and affirm the particular responsibilities of the Chief Information Security Officer for monitoring and reporting compliance with College Policy.

(b) authorize the College's Office of Information Security to take reasonable measures to secure Protected Information by using, among other techniques and methods, Data Loss Prevention (DLP) software and equipment to monitor, identify and block the unauthorized disclosure of Protected Information;

(c) prescribe mechanisms that help to identify and address areas of high risk for the unauthorized release of Protected Information and the misuse of Data, applications, the College Network and College Computers; and

(d) further reduce the risk of exposure and identity theft when a Social Security Number or other personal identifying information is used by the College as a primary identifier and to provide for the consistent, secure and proper management of such information.

Departments/Offices Affected by the Policy

This Policy is applicable to all members of the College Community including faculty, staff, students, invitees and contractors who have access to College Data regardless of the electronic medium in which such Data are stored and regardless of where such Data may be located.

Procedures Related to the Policy

1.0 DEFINITIONS

The terms listed below have the meanings ascribed next to each:

(a) "CIO" – means the College's Chief Information Officer and Senior Vice President for Information Technology or any successor position.

(b) "CISO" – means the College's Chief Information Security Officer or any successor position.

(c) "College Computer" – means any computer that is owned, leased or rented by the College of Charleston whether such computer is located on or off College premises.

(d) “College Network” – means any part of the College’s Data, voice or video network physically located on any College owned, leased, or rented property or located on the property of any third party with the permission of that party. This includes devices on such network assigned any routable and non- routable IP addresses and applies to the College's wireless network and the network serving the College’s student residence halls and houses, and any other vendor supplied network made available to the College community.

(e) “Data” means electronic information whether stored digitally or in text, voice, code or visual representation or in any other electronic medium.

(f) "Data-At- Rest"- means stored or archived Data and includes, but is not limited to, Data stored on Information Technology Resources.

(g) "Data-In-Motion" -- means Data that is traversing the College Network or otherwise being transferred electronically and includes, but is not limited to, email, instant messages, ftp, and web traffic utilizing Information Technology Resources.

(h) "Data-in-Use"- means Data that is being manipulated by a user, and includes, but is not limited to, transferring Data to a USB drive or copying, altering and/or pasting Data.

(i) “IT”— The College’s Division of Information Technology.

(j) “Information Technology Resources” – The College Network and all College Computers and computer components, electronic storage devices, wiring, and electronic transmission devices owned, leased, rented or operated by the College and all College owned or licensed software.

(k) "Protected Information"- Protected Information is a single term that includes all of the following: Confidential Information, Educational Records, Employee Records, Identifying Information, Medical Record or Health Information, Personal Information, and Proprietary Data of the College.

(l) "Security Breach"- the unauthorized disclosure of Protected Information. The College’s Information Security Office will classify such Breaches by various levels of severity that will, in turn, specify the types of College responses appropriate to the level of severity the breach is assigned.

2.0 SECURITY REVIEWS

2.1 Scope.
Based upon a determination made by the CIO or CISO in accordance with the provisions of Section 2.2, the College may:

(a) access and examine College Computers and other Information Technology Resources and all Data (whether Data-In-Motion, Data-At-Rest, or Data-In-Use) utilizing Information Technology Resources in any manner whatsoever;

(b) monitor the College Network activities of individual computer users of Information Technology Resources;

(c) conduct a forensic analysis of Information Technology Resources, and the use and usage of such Resources.

2.2 Determinations.
The Chief Information Security Officer (CISO) may exercise the rights of the College and take one or more of the actions described in Section 2.1 if the CIO and CISO reasonably determines that such action is necessary or appropriate to –

(a) protect the integrity or security of Protected Information or Information Technology Resources;

(b) protect the College from incurring liability;

(c) reduce the risk of the deliberate or unwitting disclosure of Protected Information or security features of the College's Network that are not publically known;

(d) investigate unusual or excessive activity typically associated with illegal activity or activity that may be in violation of acceptable use of College Information Technology Resources or data;

(e) investigate credible allegations of illegal activity or violations of College policy; or

(f) comply with law or compulsory legal process (such as a lawfully issued subpoena or a request under the South Carolina Freedom of Information Act).

3.0 PROBABLE VIOLATIONS

3.1 Confirmation.
In the event that IT personnel identify or are made aware of a probable violation of a policy through the misuse of an Information Technology Resource, the incident shall be recorded in secure Information Security records system and a notification and description of the incident shall be sent to the Chief Information Security Officer for further review and analysis. If the Chief Information Security Officer concurs that a probable violation has occurred or is likely to occur, such Officer shall promptly notify the CIO.

3.2 Notifications.
Upon receiving notification pursuant to Section 3.1, the CIO shall then determine what additional notifications, if any, should be made, except that in all cases of suspected criminal activity the Office of Legal Affairs shall be promptly notified and in all cases when a Security Breach is suspected.

4.0 CONFIDENTIALITY

4.1 Confidentiality Agreements.
IT personnel having knowledge of, or access to, the equipment, software, data or methods shall be required to sign a Confidentiality Agreement as a condition of employment and continued employment by the College's IT Office. Such Agreement shall be in a form and substance as mutually agreed upon by the CIO and the CISO. The Agreement will be maintained by the Information Security Office and reviewed annually.

4.2 No **Expectation of Privacy.**
PERSONS WHO USE COLLEGE INFORMATION TECHNOLOGY RESOURCES FOR DATA STORAGE, DATA TRANSMISSION OR DATA DISSEMINATION, OR FOR THE PROCESSING OF DATA SHOULD NOT EXPECT THAT:
(A) SUCH DATA IS PRIVATE AND ONLY ACCESSIBLE BY THEM; OR (B) THAT SUCH DATA IS EXEMPT FROM RETRIEVAL, MONITORING OR ANALYSIS UNDER THIS POLICY. THE COLLEGE MAY TAKE ACTIONS AUTHORIZED UNDER THIS POLICY WITH OR WITHOUT PRIOR NOTICE.

5.0 POLICY COMPLIANCE AND MAINTENANCE

5.1 Sanctions.
College employees and students are expected to cooperate with the IT Office with respect to the implementation of this Policy. Any person who knowingly attempts to circumvent, bypass, defeat, or disrupt any device, method, or technology implemented by the College for the purpose of implementing this Policy shall be subject to appropriate disciplinary and remedial actions, up to and including termination of employment, expulsion from the College, and/or legal action.

6.0 DISTRIBUTION AND TRAINING
Executive Vice Presidents of the College shall ensure that this Policy is distributed to all supervisors and managers under their direct or indirect supervision. The CISO shall be responsible for devising and implementing such employee and student training programs and information as the CIO believes necessary and appropriate to effectively implement this Policy.

7.0 OPERATING PROCEDURES
The CISO shall adopt such operating procedures to implement this Policy as maybe appropriate, provided that, such operating procedures are not in conflict with any provision of this Policy or any other College Policy and are made readily available to the College Community.

8.0 AMENDMENTS

This Policy and Procedure may be amended at any time in accordance with the Colleges Campus Wide Policy Making Procedures.

Related Policies, Documents or Forms

Review Schedule

Issue Date: 07/01/16	**Next Review: 07/01/21**

APPROVAL

By: Glenn E. McConnell President **Date:** 8/22/16

Board of Trustees and/or President