**I. OVERVIEW..... 1**
**II. CYBERSECURITY INCIDENTS..... 1**

## I. OVERVIEW

The College operates and maintains an Information Security Program ("ISP") to ensure the confidentiality, integrity, and availability of college data, based on classification, and those related information systems and services that are necessary to the support of the mission of the college and the students while maintaining compliance with local, State, and federal standards, policies, and laws.

The College uses the Statewide Information Security Manual published by the North Carolina Department of Information Technology as the principal cybersecurity framework for a system-wide information security and risk management program. The College's use shall be consistent with the provisions of the State Board Code.

## II. CYBERSECURITY INCIDENTS

The College shall not submit payment or otherwise communicate with an entity that has engaged in a cybersecurity incident on an information technology system by encrypting data and then subsequently offering to decrypt that data in exchange for a ransom payment.

Consistent with State law, the College consults with the NCCCS Office and North Carolina Department of Information Technology regarding cybersecurity incidents. The President shall inform the Board of Trustees of any cybersecurity incident in which the College consults with the NCCCS Office or North Carolina Department of Information Technology.

**REFERENCES**

| | |
|---|---|
| **Statutory References** | N.C.G.S § 143-800 |
| **Regulatory References** | 1B SBCCC 700 |
| **Relevant Guidance** | None |
| **Policy Manual** | None |

| | |
|---|---|
| **Cross-References** | |

**POLICY HISTORY**

| | |
|---|---|
| **September 12, 2023** | Adopted. |