Policy Manual

Title: Cybersecurity	**Number:** 6Hx2-8.08
Legal Authority: §§ 119, 815, 1001.65, Fla. Stat. (2018)	**Page:** Page 1 of 2

GENERAL STATEMENT

The President shall establish procedures as necessary to protect the devices and information within the custody and control of Broward College ("College"). Being able to access complete and accurate information is vital to the College's ability to operate efficiently and successfully. The College also has a duty to safeguard legally protected information.

All members of the College community are responsible for protecting the security, confidentiality, integrity and availability of information entrusted to them, and for taking affirmative steps to prevent its unauthorized disclosure or loss. This policy sets forth the security requirements that all members of the College community must follow to meet that responsibility.

THE POLICY and THE STUDENT

The College provides all of its students with access to the College Network and Internet in order to obtain current information useful for their advancement in academics. It is the student's responsibility to understand what constitutes proper use of the College Network, as outlined in Procedure A6Hx2-8.01B College Network and Software Usage by Students.

THE POLICY and THE FACULTY AND STAFF

All members of the College community, and anyone accessing the College Network and Internet, are responsible for adhering to the College information security requirements, including but not limited to the following:

1. **Protecting System and Network Access**

   a. Know and follow the requirements in College Policy 6Hx2-8.01 College Network and Software Usage.

   b. Do not use College systems in a way that negatively impacts the functioning or availability of those systems.

   c. Treat credentials for access to College systems (e.g. usernames and passwords) as confidential. Such credentials are non-transferable and should never be shared.

   d. Use strong passwords to access College systems and to secure personal computers according to password guidelines.

   e. Do not write down passwords where they are easily accessible to others.

   f. Do not attempt to access College systems unless authorization has been provided.

History: *Adopted June 27, 2017; revised October 23, 2018*			
Approved by the Board of Trustees	**Date:** 10/23/18	**President's Signature**	**Date:** 10/23/18

g. Do not adjust or change the anti-virus and end point security software deployed on College equipment.

h. Do not download or install unauthorized computer programs or software onto College equipment.

2. **E-mail**. Adhere to College Policy 6Hx2-8.03 College Communication via Email.

3. **Disposing of Information and Equipment Properly**. Dispose of all College computer equipment and documents only in accordance with the College Policy 6Hx2-7.04 Property Control and College Policy 6Hx2-2.09 Reproduction, Duplication, Maintenance, and Destruction of College Records.

4. **Additional Requirements for Off-Campus Computing.** Employees who work from off-campus locations must take additional steps to protect information and adhere to the College Policy 6Hx2-3.54 Telecommuting.

5. **Reporting Potential Information Security Breaches.** Immediately report potential information security breaches, or evidence of potential illegal activity, to Technology Services, and to your immediate supervisor. Do not take steps to investigate a potential security incident unless you are also on the Technology Services Incident Response Team.

IMPLEMENTATION and OVERSIGHT

The Vice President for Information Technology has responsibility for the implementation and oversight of this policy. Technology Staff will review, analyze, evaluate and monitor equipment and information for purposes of setting goals, standards, specifications and strategies to ensure compliance with this policy. Technology Staff will also follow all federal and state laws and guidance, including but not limited to that provided by National Institute of Standards and Technology (NIST), Federal Information System Controls Audit Manual (FISCAM), the Florida Agency for State Technology (AST).

VIOLATION OF POLICY

Information Technology and Human Resources have the right to investigate all incidents. Employees in violation of these established procedures and requirements may be subject to disciplinary action, up to and including termination. Students in violation of these established procedures and requirements may be subject to disciplinary action as outlined in the Student Handbook. All individuals in violation may also face fines, fees for damages, civil or criminal penalties from Florida or U.S. Courts.

History: *Adopted June 27, 2017; revised October 23, 2018*			
Approved by the Board of Trustees	**Date:** 10/23/18	**President's Signature**	**Date:** 10/23/18