PRINCE GEORGE'S COUNTY PUBLIC SCHOOLS
Board of Education
Upper Marlboro, Maryland

0117
Policy No.

BOARD OF EDUCATION POLICY

BASIC COMMITMENTS

Information Technology Services – Information Security

I. Policy Statement

Prince George's County Board of Education (Board) is committed to ensuring the effectiveness, safety, and soundness of Prince George's County Public Schools (PGCPS) Information Technology Services. The Board believes that it is essential to put preventive measures in place to protect sensitive information in electronic format and maintain the safety and privacy of individuals...

II. Purpose

The purpose of this policy is to promote cybersecurity in all PGCPS electronic communications and accountability for PGCPS data and information assets.

III. Definitions

A. *Principle of least privilege* - the principle of least privilege (POLP) is a concept in computer security that limits users' access rights to only what is strictly required to do their jobs

B. *Role-based technology access* - a security approach that authorizes and restricts system access to users based on their role(s) within an organization**.** This allows users to access the data and applications needed to fulfill their job requirements and minimizes the risk of unauthorized employees accessing sensitive information or performing unauthorized tasks

IV. Standards

A. System Prevention Responsibilities

1. Implement appropriate measures to ensure confidentiality, integrity, availability, and accountability of PGCPS data and information assets in both electronic and physical formats.

2. Monitor, archive, audit, or purge the contents of electronic communications, files, and other material created or stored using the district technology, or data transmitted over the district network.

3. Provide role-based technology access to users, using individual account credentials and the principle of least privilege.

4. Secure the technology networks and physical access to the data centers and technology infrastructure against unauthorized access.

5. Account for district technology equipment at all times, and dispose of in accordance with National Institute of Standards and Technology media sanitization guidelines.

6. Implement multifactor authentication to access the network.

7. Develop and exercise a cyber incident response plan.

8. Require all employees to annually complete training in security awareness to help mitigate security risks.

B. Employee Responsibilities

1. It is the responsibility of all PGCPS employees and contractors to safeguard access to the PGCPS network (including students, parents, and staff) and refrain from disclosing usernames or passwords that would allow unauthorized access to PGCPS computer systems.

2. Employees are prohibited from accessing, using and/or disclosing personally identifiable information for any reason other than the legitimate performance of the individual's job duties or in ways that jeopardize the security of such information.

3. All employees are responsible for following the policy and procedures addressing acceptable usage guidelines.

C. Penalties

1. If it has been determined that an employee has improperly accessed sensitive information or has attempted to access sensitive information, the employee can expect disciplinary actions which may include, but are not limited to:
    a. Immediate suspension of equipment and/or information access.
    b. Letter of reprimand
    c. Suspension or dismissal

2. Any offense that violates local, State, or federal laws may result in any and all of the above disciplinary actions, including arrest or prosecution.

V. Implementations and Responsibilities

The Board directs the Superintendent to develop administrative procedures, including an information technology security plan to implement this policy.

VI. References

A. Legal

Electronic Communications Privacy Act, 18 U.S.C. §§2701-2711
Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232(g)
Student Data Privacy Act of 2015, Md. Code Ann., Educ. Art. §4-131)
Md. Code Ann., Lab. and Emp. Art. §3-712 (User Name and Password Privacy Protection and Exclusions

B. Other Board Policies

Board Policy 0115 – Information Technology Services – Acceptable Usage Guidelines

VI. History

Policy Adopted
9/28/06

Policy Amended
4/29/10

Policy Amended
03/21/2024