



ADMINISTRATIVE PROCEDURE

INFORMATION TECHNOLOGY SERVICES
REMOTE ACCESS PROCEDURES

AP 0705
Effective Date:
October 3, 2024

- I. **PURPOSE:** To provide guidance for authorized users to access the Prince George’s County Public Schools (PGCPS) network remotely.

- II. **POLICY:** The Prince George’s County Board of Education (Board) is committed to ensuring the effectiveness, safety, and soundness of 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. (Policy 0117)

- III. **BACKGROUND:** Authorized users, including employees and contractors, may need to access the PGCPS network inside the firewall to complete work while off-site from a PGCPS location. Remote access to the school district’s information systems is required to be secure before allowing such access. This remote access requires that an authorized user connect to the school system’s network through appropriate procedures.

- IV. **DEFINITIONS:**
 - A. *Authorized user* – Employee or contractor who has requested and been granted the ability to access the network remotely due to a demonstrated need.

 - B. *Computing device*- technology tool use to connect to the PGCPS network.

 - C. *Multi-Factor authentication* – Multiple methods to verify the identity of an authorized user of the PGCPS network. *Multi-Factor authentication* can include a notification on a phone, rotating numeric token, or other methods as needed to obtain and maintain secure access.

 - D. *Multi-Factor authentication* – Multiple methods to verify the identity of an authorized user of the PGCPS network. *Multi-Factor authentication* can include a

notification on a phone, rotating numeric token, or other methods as needed to obtain and maintain secure access.

- E. *Remote access* – Access to the PGCPS network from an external network outside the school system’s firewall.
- F. *VPN (Virtual Private Networking) access* – A connection to the PGCPS network, through a wired or wireless high-speed internet connection using VPN software.

V. PROCEDURES:

A. VPN Access

- 1. VPN access is a service granted to PGCPS authorized users who have demonstrated a need to access the network remotely (*e.g.*, Payroll).
- 2. In conjunction with VPN software, all VPN users are required to use multi-factor authentication to connect remotely to the PGCPS network.

B. Requesting VPN Access

- 1. Employees
 - a. Employees needing access should place a Help Desk ticket via the online portal (<https://help.pgcps.org>).
 - b. The Employee Service Desk will review the request and upon approval, assist employees in establishing Multi-Factor authentication and connecting remotely. The Employee Service Desk will assist with software installation and technical support.

C. Authorized User and Responsibilities

- 1. VPN Access is a privilege. Any inappropriate use of this access as outlined in Administrative Procedure 0700, Information Technology Services -Acceptable Usage Guidelines, will result in immediate termination of service.
- 2. VPN access is to be used only by the user for which the request was granted (the authorized user). Sharing this access with any non-authorized person will result in immediate termination of access and may be subject to other disciplinary action.
- 3. VPN access is to be used only by the user for which the request was granted (the authorized user). Sharing this access with any non-authorized person will result

in immediate termination of access and may be subject to other disciplinary action.

- VI. **MONITORING AND COMPLIANCE:** IT staff will ensure that only authorized users, currently engaged in a remote access activity, have access to the PGPCS network by monitoring access regularly. Remote access is audit regularly, at least quarterly, in the same manner as direct access to the PGPCS network. Authorized user must adhere to the provisions of Administrative Procedure 0700, Information Technology Services - Acceptable Usage Guidelines, and are subject to monitoring that includes IT scanning of devices, remotely or physically by technical support staff, connected to the PGPCS network to ensure compliance.
- VII. **RELATED ADMINISTRATIVE PROCEDURES:** Administrative Procedure 0700 – Information Technology Services - Acceptable Usage Guidelines.
- VIII. **MAINTENANCE AND UPDATE OF THIS ADMINISTRATIVE PROCEDURE:** This administrative procedure originates with the Division of Information Technology and will be updated as needed.
- IX. **CANCELLATIONS AND SUPERSEDURES:** This administrative procedure cancels and supersedes the version dated July 1, 2019.
- X. **EFFECTIVE DATE:** October 3, 2024

Attachments: