Computer Use and Security Guidelines

Chris Gorrell - 2023-02-10 - Policies

General Security and Remote Access Guidelines

Use of Personal Computers

- No personally owned computer may be connected to the PMI Corporate network at any PMI campus.
- Employees working remotely should use PMI-owned computers as much as possible. The use of personally owned computers for work-related purposes is discouraged.
- Any computer, personally-owned or otherwise, which is used to connect to PMI's network via VPN should have anti-virus software installed and working. The IT Department can provide recommendations for such software.

Guidelines for Use of PMI Computers

- All computers owned by PMI will have the following software installed:
    - Rapid7 Agent (Security Monitoring Software)
    - Antivirus Software (As provided by IT)
- No software should be installed on any PMI-owned computer unless approved by the IT Department
- Unless otherwise authorized by the IT Department, the following software is prohibited.
    - Hacking or penetration testing tools such as Metasploit
    - Whole-disk or file encryption software not expressly approved by the IT Department
    - Packet sniffing or network monitoring tools, such as Wireshark
    - File sharing programs such as Bittorrent
    - Third-party screen savers such as Web Shots
    - Any unlicensed software
- Computers owned by PMI may be used by PMI employees only. They should not be shared with family members or any other person.

Passwords

Employees are assigned at least two accounts for individual use, the PMI Network Account, and a Google account used for email. Employees who require access to CampusNexus are assigned an account for it, as well.

- Initial passwords, assigned by IT, should be changed as soon as the user logs into the account.
- Passwords for individual-use accounts are not to be shared for any reason.
- No employee may ask another for individual-use account passwords. This includes that supervisors may not ask subordinates for their passwords.
- Passwords should never be included in any email communication, including emails to the IT Department.
- No person may log on to a computer or other system using another person's account.

Remote Access

Two Factor Authentication (2FA) is required for remote access to the PMI Corporate Network, Citrix Gateway, and Cream.

- Cream uses a built-in 2FA system which relies on SMS to send a secondary password to the user's cell phone. The user's cell phone number must be on file in Cream.
- GlobalProtect VPN provides remote access to the corporate network. Citrix Gateway provides direct access to CampusNexus. Both use the same 2FA system. This system relies on a smartphone app to provide a One Time Password which is required after the normal username and password. Instructions to set this up are available from the IT Department

General Guidelines and Tips

- For all of the above, more detailed guidelines can be found in the employee handbook.
- IT Department contact info can be found in our Phone Directory website.
- The IT Department does not know, and cannot retrieve, the password for any person's account.
- Passwords should not be written down, and should never be saved in an unencrypted file, such as a text file or Word document.
- Email should not be considered a secure means of communication. Do not include any sensitive information in an email unless other precautions are taken.
- Email addresses are very easy to forge. In particular, the "From" address of an email can easily be faked and should not be relied upon to determine the source of a message.
- Suspicious emails, especially emails with unexpected attachments, should be deleted.
- To securely send files by email, encryption should be used. The site https://filesender.pmi.edu can be used for this purpose. The encryption password should be communicated to the recipient separately, at the very least in a separate email.
- Any person who uses 2FA should notify the IT Department immediately if their phone is lost or stolen, so they can invalidate the OTP Token.