Policy No.: 8073
Board Approved: February 20, 2024
Revised:

Information Technology Security Policy

Where applicable, this policy applies to any device or software that access or stores HCC data, regardless of the ownership. This policy applies to all HCC employees.

Physical Security
All users are expected to lock their office area when unoccupied and to lock offices when away for an extended period of time (*such as leaving for lunch or a class session*). Mobile and portable devices are to be behind a lock, and if reasonable, kept out of sight when not in use. Users must lock their screen when leaving direct line of sight of their device.

Remote Access
Additional security precautions will be enforced if users are connecting remotely. This applies to devices owned by HCC and personally owned devices. Any device used to access or store HCC data must be password protected and have remote-wipe enabled in the device settings, if applicable. Users must follow HCC Telework Policy (*Policy No.: 5056*) regarding VPN access.

Cybersecurity
All users are expected to take reasonable precautions to keep devices secure. Reasonable security precautions include keeping devices updated and having security software enabled. This includes personal devices used to access HCC data or networks.

Software
All software used on HCC networks, or that represents HCC, must be vetted and approved by the IT department. This includes but is not limited to downloaded software, cloud-based software, web-based products, and products that Email on behalf of HCC. This applies to all software (including free, paid, trial, demo, subscription, etc.).

Software requests must include justification and approval from the director, dean or equivalent position of the requesting department. Requests should include multiple vendors. The IT department is not responsible for procurement of a product after approval.

Hardware
Hardware added to HCC networks is to be vetted and approved by the IT department. No device is to be added to the network without prior authorization of the IT department. The IT department may remove network access of any device on HCC networks without prior notice to the user.

HCC Email
Users are expected to protect their Email accounts and the content of Email messages. Devices used to access HCC Email must be password protected; mobile devices must have a secured lock screen enabled. Shared mobile devices may not be used for HCC Email. Personal devices used to access HCC Email may be wiped remotely.

Lost or Stolen Devices

Stolen devices must be reported immediately to the IT Help Desk (Email: *HCCIT@hagerstowncc.edu | Call/ Text: 240-329-4489)*. Lost and missing devices should be reported no later than 24 hours after the last known position of the device. After the initial report of a missing device, a detailed report should be given to the IT department explaining what the device was used for, and what data was stored on the device. This applies to both HCC devices and personally owned devices that are used to access HCC data or HCC Email.