HLC Accreditation Evidence

- Technology Infrastructure

URL:

Office of Origin:

- Information

Contact(s):

- Chief Information Officer

Technology Infrastructure

Information Services supports the following instructional sites:

- Barton Community College, Great Bend
- Fort Leavenworth Military Base
- Fort Riley Military Base
- Grand View Plaza located in Junction City, Kansas
- Adult Ed, RSVP, EOC – Downtown Great Bend, Kansas
- Barton/Pratt Nursing – Pratt Community College, Pratt, Kansas

Current Technology Assets at Barton:

- Cloud Infrastructure
    - AWS – (Amazon Web Services)
        - 9 Microsoft Servers
        - 2 Linux Servers
    - GCP – (Google Cloud Platform)
        - 2 Load Balancers in front of a container system to run the websites
        - 1 server for redirects
    - KanREN
        - Firewall Management hosting and on prem
        - DNS host
        - Provides connectivity services between all remote campuses
- On premise network infrastructure
    - 115 Switches split between Main Campus, Downtown, Fort Riley, Grandview Plaza, and Fort Leavenworth
    - 196 Access Points
    - 298 Security Cameras
    - 339 Phones
    - 50 Microsoft Servers
    - 1 Barracuda Spam Filter Appliance
    - 2 Barracuda Backup Appliances
- End User Technology
    - Workstations – employee and student labs
    - Printers
    - Laptops
    - Tablets, iPads and Remarkable Tablets
    - iMacs
    - MacBooks
    - Ladibug Document Cameras
    - Projectors

- Anatomage Classroom
- Active Learning Classrooms (2)
- Classrooms with Zoom technology (79)
- Canvas Learning Management System
- Apporto Virtual Desktop

Major Projects:

- Moved students and employees to O365 cloud – Spring 2020
    - Removed on-prem Exchange servers from environment

- Moved Ellucian Systems to Cloud – Spring 2020
    - Removed on-prem Banner servers.
      Evidence: 2019.03.12 Barton Community College Ellucian Cloud
      Evidence: Customer Snapshot

- Updated Classrooms and labs to accommodate Zoom teaching Spring 2020 & Summer 2020

- Pulled and configured lab machines to accommodate remote workers through 2020 pandemic.

    - During the first months of 2020, Information Services pulled lab machines and re-configured them for employee remote working. This was a massive undertaking involving the entire Information Services Department. Beginning to end process during this time was to configure the pc, troubleshooting with remote workers, track/document equipment, physically sanitize, and then return equipment into the labs. During Summer 2021, remote workers started returning and bringing equipment back. By Fall semester 2021, computers were returned to labs, sanitized, reconfigured and ready for student use.

Security, Cybersecurity and MFA

- College pcs, laptops, classroom instructor and student pcs use Microsoft Defender desktop protection. Information Services uses PDQ and Microsoft WSUS for desktop updates and monitoring.
- College Apple Macs have Avast for protection.

Annually, beginning in March of every year, employees are allowed 30 days to complete Cybersecurity training. This training does vary from one year to the next. The annual training does include:

- Security Awareness
- Internet Security
- Phishing Awareness

August 2022, OKTA MFA was implemented for employees and students. Staying compliant with Cybersecurity Insurance.

- Employees have a choice of four different options of authentication
- Students have a choice of five different options of authentication