

AGENDA
COMBINED HYBRID MEETING OF THE
BUSINESS AFFAIRS AND EXECUTIVE
COMMITTEES OF THE BOARD OF TRUSTEES
Community College of Philadelphia
Wednesday, July 16, 2025 – 9:00 A.M.

TO: Business Affairs and Executive Committees of the Board of Trustees
FROM: Jacob Eapen
DATE: July 10, 2025
SUBJECT: Combined/Hybrid Meeting of the Business Affairs and Executive Committees of the Board of Trustees

A combined/hybrid Business Affairs and Executive Committees of the Board of Trustees meeting is scheduled for July 16, 2025 at 9:00 A.M. Participants and attendees may attend in person in the Isadore A. Shrager Boardroom M2-1 or *via* Zoom. The Zoom information for the Public Session is as follows:

Topic: 07/16/2025 Combined/Hybrid Business Affairs
and Executive Committees of the Board of Trustees
Public Session

<https://ccp.zoom.us/j/98850175538?pwd=JjRNelaU6FjomNEGbzGnWuUcTybFIA.1>

Meeting ID: 988 5017 5538

Passcode: 8029

AGENDA
BUSINESS AFFAIRS COMMITTEE
PUBLIC SESSION

Please note that Attachment A contains a spreadsheet that lists the vendor/consultant, the amount, and the source of funding (i.e., Capital Budget, Operating Budget, Grants, or Bond Proceeds) which College Administration is seeking approval.

(1) Maintenance Agreement and Annual Lease with Crown Castle Fiber LLC
(Action Item)

The College requests renewal of the annual lease and maintenance contract with Crown Castle Fiber LLC for dedicated dark fiber optic connectivity between all college-owned and leased facilities.

This network infrastructure is composed on nine (9) distinct fiber circuits, supports the College's critical IT services, including internet access, enterprise systems, Voice over IP (VoIP), video conferencing, security systems, academic technology platforms, and business community/disaster recovery operations.

Strategic & Technical Benefits:

- Dark Fiber allows the College to independently manage bandwidth, quality of service, and future upgrades – unlike carrier services.
- The network is built on a ring topology providing:
 - Redundancy: Auto rerouting in case of circuit failure.
 - Resilience: Enhanced uptime for instructional systems, ERP, VoIP, and video security.
- Critical for:
 - Academic continuity
 - Secure transmission of sensitive data
 - 24/7 Banner ERP services

Updated Financial Impact Summary – 3-Year Term

ITEM	DETAILS	MONTHLY COST (MRC)	ANNUAL COST	3-YEAR TOTAL
Total Number of Circuits	9 Point-to-Point Dark Fiber Circuits	-----	-----	-----
New Monthly Rate (MRC)	Negotiated 3-Year Rate	\$10,945	\$131,340	\$394,020
Previous Annual Rate	1-Year Renewal Baseline	\$12,569	\$150,830	\$452,491 (3-year)
Net 3-Year Savings	Total cost avoided with multi-year term	-----	-----	\$58,471

This renewal supports the uninterrupted delivery of digital services across all college campuses and administrative buildings. This expenditure is pre-budgeted annually under the ITS operating budget for Network Infrastructure Services. The dark fiber backbone is foundational to the College's data infrastructure and is a mission-critical asset for academic delivery, administrative services, cybersecurity resilience, and institutional compliance.

Approving this 3-year dark fiber renewal secures both technical stability and financial efficiency. It delivers \$58,472 in savings over a typical 3-year renewal cycle and maintains uninterrupted delivery of high-priority digital services across all College sites.

Staff is requesting that the Business Affairs Committee recommend to the Executive Committee of the Board of Trustees the approval of a 3-year agreement with Crown Castle Fiber LLC in the total amount of \$394,020 (\$131,340 annually). These funds will be coming from operating budget.

(2) Renewal Contract with Dell – APEX Backup (Action Item)

The staff requests approval to renew the College's enterprise backup solution - Dell Druva/Apex backup service totals \$110,899 as part of its continued investment in cyber resilience, disaster recovery, and data protection. The updated agreement includes expanded ransomware protection and cyber recovery functionality, critical enhancements in the current threat landscape.

Background & Business Justification:

Since its original adoption during the pandemic, Dell's Druva/Apex backup solution has served as a foundational component of the College's enterprise data protection infrastructure. ITS initially selected the Dell ecosystem to align with our evolving strategy of secure, scalable cloud-first solutions, seamlessly integrating with existing virtualization and storage environments for business continuity and data recovery.

In early 2024, ITS initiated a comprehensive evaluation of emerging cybersecurity risks and business continuity standards, driven by the escalating frequency and sophistication of ransomware attacks targeting higher education institutions. As part of this assessment, the department rigorously compared Dell's expanded PowerProtect Cyber Recovery services with similar offerings from Rubrik. While Rubrik presented a robust security-focused architecture, its total cost was significantly higher, and implementation would have necessitated a disruptive transition.

The strategic decision to remain with Dell's enhanced Apex backup and Cyber Recovery offering, procured through SHI under existing purchasing agreements, was predicated on its superior cost-effectiveness, robust ransomware countermeasures, and streamlined deployment into our AWS environment. This enhanced solution introduces a logically air-gapped vault, automated anomaly detection through CyberSense analytics, and immutable backup snapshots with retention lock. These features collectively provide advanced forensic recovery capabilities and ensure rapid restoration of mission-critical data in the event of a cyber incident. This enhanced protection further strengthens the College's layered security approach, building upon our existing Fortinet Fabric investment and aligning with critical business recovery objectives.

Key Features and Benefits of Dell PowerProtect Cyber Recovery:

- **Logically Isolated Backup Vaults:** Ensures copies of critical systems and data are shielded from compromise through stringent network segmentation and controlled access policies, creating an impenetrable last line of defense.
- **AI/ML-driven CyberSense Analytics:** Leverages advanced artificial intelligence and machine learning to scan for ransomware signatures, data corruption, and anomalies with greater than 99% accuracy *before* systems are restored, preventing reinfection.
- **Automated Replication Policies:** Provides periodic, policy-driven synchronization of data from production to vault environments, coupled with compliance-grade immutability settings to guarantee data integrity.
- **Native AWS Integration:** Offers seamless orchestration via Dell Apex and CloudFormation templates, facilitating scalable deployment and optimized cost management within our public cloud infrastructure.
- **Business Continuity & Compliance:** Supports institutional Service Level Agreements (SLAs) and Service Level Objectives (SLOs) for data integrity, recovery assurance, and audit readiness, reinforcing our commitment to operational resilience.

Financial Impact:

The renewal quote from SHI (Quotation #: 25739236, Created On: 1/17/2025, Valid Until: 7/11/2025) for the enhanced Dell Druva/Apex backup service totals \$110,898. This represents an increase of \$64,898 over the previous contract term, reflecting the expanded feature set and enhanced security capabilities. However, this investment delivers significant added value by eliminating the need for a separate, costly third-party ransomware recovery platform and substantially reducing Recovery Time Objectives (RTO) in the event of a cyberattack.

ITS projects long-term savings compared to alternative offerings like Rubrik, which carried significantly higher upfront and operating costs.

Conclusion & Request:

In light of the current escalating threat landscape and the increasing prevalence of ransomware attacks targeting educational institutions, the staff strongly recommends renewing and upgrading the Dell Druva/Apex backup service to include the PowerProtect Cyber Recovery and CyberSense feature sets. This strategic investment aligns directly with the College's risk mitigation goals and critically positions our infrastructure to maintain operational continuity and data integrity in the face of evolving cyber threats.

Staff requests that the Business Affairs Committee recommend to the Executive Committee the approval to renew the contract with Dell – APEX Backup, totaling \$110,899, as an essential component of our ongoing cybersecurity and infrastructure resilience roadmap. These funds will come from operating budget.

(3) Renewal of Fortinet Security Solutions Contracts (Through June 30, 2026) (Action Item)

The staff is requesting approval to renew the Fortinet Security Solutions support agreements for critical components for the College's network security infrastructure. These systems form the core of our cybersecurity framework, delivering protection, detection, and centralized control across our enterprise.

Historical Context:

During the COVID-19 pandemic, the College strategically transitioned to the Fortinet Security Fabric as a unified cybersecurity platform, using Higher Education Emergency Relief Funds (HEERF) to strengthen our security posture in response to increased remote and online learning. The adoption of Fortinet's comprehensive product suite—including Smart next-gen firewalls, Forti Analyzer, endpoint detection and response (EDR), and Network Access Control (NAC)—was approved by the Board and implemented to enhance visibility, automate threat response, and establish end-to-end protection across all campus locations. This integrated approach provided scalable and centralized enforcement of security policies, dramatically improving our ability to detect, contain, and remediate threats in real time.

Assets Covered:

- FortiGate 1500D Appliances (2)
- FortiAnalyzer Virtual Machine (1)
- FortiEDR Managed Service (1)
- FortiGate 501E Appliances (2)
- FortiGate 2000E Appliances (4)

Renewal Scope:

- Vendor: Fortinet
- Support Type: Comprehensive hardware/software including firmware, advanced threat intelligence, and 24/7 global technical support
- Term: Co-termed support coverage through June 30, 2026
- Annual Cost: \$138,401

Business Justification:

- Operational Continuity: Ensures seamless support coverage for core cybersecurity infrastructure, mitigating potential service disruptions.
- Risk Reduction: Maintains timely access to critical threat updates, patches, and advanced defense mechanisms.
- Budget Optimization: Co-termed renewal streamlines contract administration and reduce renewal fragmentation across fiscal cycles.
- Regulatory Compliance; Sustains our posture for required cybersecurity and data protection standards.

Staff is requesting that the Business Affairs Committee recommend to the Executive Committee to renew Fortinet Support Contracts component totaling \$138,401. This will support out long-term IT security strategy and maintains robust protection of college systems and data assets through FY2026. These funds will come from the operating budget.

(4) Award to Positive Wiring for Electrical Work at CATC & WRC (Action Item)

Staff seeks approval for electrical construction for the renovation of CATC welding lab and WRC classroom space to support the NWI welding Program. The College is currently working with the Naval Welding Institute, LLC (NWI) for the development of advanced manufacturing classes, focusing on Naval shipbuilding for national defense. This program includes the installation of 20 new welding booths in CATC (NWI Grant) and the relocation of the existing welding booths to WRC to support the CCP existing program.

CCP received proposals for electrical work thru PA State COSTAR Cooperative Purchasing Program. The electrical work required is mainly to upgrade the electrical systems in both buildings to support the new equipment load.

Positive Wiring CATC work: \$142,400

Positive Wiring WRC work: \$139,200

Staff request that the Business Affairs Committee recommend to the full Board the award to Positive Wiring for Electrical Construction in the amount of \$281,600.

This purchase will be paid from grants and the Capital Budget.

**(5) Next Meeting – Business Affairs Committee of the Board of Trustees
(Information Item)**

The next meeting of the Business Affairs Committee is scheduled for August 20, 2025 at 9:00 am.

AGENDA
EXECUTIVE SESSTION
PUBLIC SESSION

(1) Based on the recommendations of the Business Affairs Committee, the Executive Committee of the Board of Trustees will motion on the following items:

- Maintenance Agreement and Annual Lease with Crown Castle Fiber LLC
- Contract Renewal with Dell – APEX Backup
- Contract Renewal with Fortinet
- Welding Electrical Construction – CATC
- Welding Electrical Construction - WPRC

EXECUTIVE SESSION

The Business Affairs and Executive Committees will go into Executive Session.

The zoom information for the Executive Session will be provided in a separate email for those who will be attendance

The Business Affairs and Executive Committees will return to Public Session

JE/tn

c: Ms. Mindy Posoff
Dr. Alycia Marshall
Mr. Gim Lim
Mr. Derrick Sawyer
Ms. Carolyn Flynn

ATTACHMENT A
FUNDING FOR ACTION ITEMS

**COMBINED MEETING OF THE BUSINESS
AFFAIRS COMMITTEE AND THE
BOARD OF TRUSTEES**

AGENDA: July 16, 2025

Agenda No.	Vendor/Consultant	Amount	Source
1	Crown Castle Fiber LLC	\$394,020 (\$131,340 annually)	Operating Budget
2	Dell – Apex Backup	\$110,899	Operating Budget
3	Fortinet Security Systems	\$138,401	Operating Budget
4	Positive Wiring – CATC	\$142,400	Capital Budget
4	Positive Wiring – WPRC	\$139,200	Capital Budget