Barton Community College Strategic Plan Project Charter

Purpose (The why of the project/current state):
This initiative sustains effective cyber and physical security practices to mitigate risks and vulnerabilities across the institution, supporting Barton's goal to align processes in ways that increase efficiency, strengthen institutional effectiveness, and uphold responsible stewardship of the resources entrusted to the College. In addition to addressing institution-wide security needs, this initiative mitigates human--factor risks such as phishing, baiting, and other social--engineering- threats. These efforts complement the systems-level- risk reductions achieved through Initiative 5.3, which resolves vulnerabilities created by legacy technologies and authentication processes. Initiative 5.4 operates independently of Initiative 5.3's implementation schedule. No deliverables from 5.3 are required for 5.4 to proceed. By strengthening employee awareness and response to malicious activity, this initiative reduces behavior-based vulnerabilities and advances a complete, people-centered security posture for the institution. Addressing both the system and human dimensions is essential to lowering Barton's exposure to preventable security incidents.

Artifacts: (The evidence being used):
- Mandatory cybersecurity training records and completion reports.
- Quarterly phishing simulation reports provided by Tandem Cyber.
- Cybersecurity insurance documentation and training content approvals.
- Chief Information Officer (CIO) Cybersecurity evaluations and HR training management materials.
- Incident response logs, acceptable use policy, and security awareness communications.
- Physical security assessments (access control audit results, camera coverage review notes, incident drill reports).
- Email-security platform outcomes (e.g., phishing detection counts, quarantine totals) used to calculate report-rate and report-to-click metrics.

Overview (Summary of what will be done):
College employees complete annual mandatory cybersecurity training provided through the College's cybersecurity insurance, with Human Resources managing assignment and tracking and the CIO reviewing and approving all training content prior to deployment. In

addition, the College's cybersecurity partner, Tandem Cyber, conducts quarterly simulated phishing campaigns, tracking employee responses and supplying detailed reports to the CIO to support continuous improvement and targeted just-in-time training. These cybersecurity efforts are complemented by strengthened physical-security practices, including scheduled access-control audits, basic camera coverage reviews completed in coordination with Facilities and Campus Safety, and tabletop incident readiness drills (practice conversations) that reinforce institutional preparedness.

This initiative reinforces the human-readiness side of institutional security by strengthening employee cybersecurity behaviors and institutional preparedness. It focuses on people, practices, and readiness, complementing systems-level efforts without reliance on them.

Project Addresses Strategic Initiative:
5.4 Sustain effective cyber and physical security practices to mitigate risks and vulnerabilities.

Goal (Desired result/the data point you want to move):

- Maintain 100% employee completion of annual cybersecurity training within a six-week launch window, ensuring training remains current and responsive to emerging threats.
- Establish a simulated-phishing click-rate baseline using FY2026 data and reduce this rate over the plan cycle, achieving ≤5% by the end of FY2027.
- Increase the proportion of suspected phishing messages that are reported through Report Phish or helpdesk channels, relative to the total suspected messages identified by employees or security tools.
- Complete a baseline physical-security assessment (access controls and basic camera coverage) and implement prioritized remediation actions.
- Conduct annual incident-readiness tabletop drills focused on cyber and physical-security scenarios to strengthen institutional preparedness and ensure consistent response practices across departments.

Project Description or Scope of Work:

Starting Date:
Annually starting in October for cybersecurity training. Physical security assessment activities begin Spring 2026 and recur annually thereafter.

Milestone Dates:

- Fall 2026: Confirm annual cybersecurity training content; schedule quarterly phishing simulations; plan physical-security baseline assessment.
- Fall 2026: (annually in October): Launch cybersecurity training; six-week completion window opens.
- Quarterly (ongoing): Conduct phishing simulations and publish CIO reports with trends and recommendations.
- Summer (annually): Complete physical security assessment and finalize remediation plan for the upcoming fiscal year.

Impact (How the goal is reflected in a defined population):
All employees develop the skills to recognize phishing, baiting, spam, and scamming emails, strengthening Barton's ability to protect institutional data and employee accounts. Strengthened physical-security practices further reduce exposure to access-control failures and improve incident readiness lowering institutional risk, reducing preventable disruptions, and supporting efficient, reliable operations. These efforts advance Barton's commitment to operational efficiency, responsible stewardship of institutional resources, and a strengthened cybersecurity posture. By elevating employee readiness and institutional preparedness, the College reduces preventable disruptions, decreases helpdesk dependency, and safeguards institutional data assets—improving the reliability, security, and effectiveness of Barton's core operations. This initiative ensures that employees can engage with Barton's systems and environments safely and reliably and supports consistent, dependable operations through improved cybersecurity behaviors and physical-security practices. These efforts reduce preventable disruptions and support consistent, reliable operations by strengthening both employee cybersecurity readiness and institutional physical-security posture.

RACI (Responsible, Accountable, Consulted, Informed) Chart:

- See RACI Chart Spreadsheet

Plan for Sustainability (Where will project "live" after implementation):
Cybersecurity insurance is maintained by the College and includes access to annual training content; annual training remains a required activity for all employees. Quarterly phishing simulations continue through the College's cybersecurity partner, with results reviewed by the CIO and communicated institution-wide. Physical-security assessments

are embedded into Facilities/Campus Safety annual workplans. Policies and practices are reviewed on a routine schedule to ensure continued relevance.

Additional Relevant Information:

Identified Institutional Values: (For 5.4 SPI, what institutional values are demonstrated by this initiative? (Honesty, Fairness, Respect, Courage, Trust, Responsibility)
Courage, Trust, & Responsibility