

01.02.001 – Technology Master Plan Policy		
1.0	Purpose:	The purpose of this policy is to establish a framework for the creation, implementation, and maintenance of a Technology Master Plan (TMP) at Quinsigamond Community College (QCC) . The TMP ensures that the College’s technology infrastructure, systems, and resources align with its mission, strategic goals, and long-term academic and operational needs.
2.0	Revision History:	New Policy. Approved by the Board of Trustees: 6/11/2025
3.0	Persons Affected:	This policy applies to: <ul style="list-style-type: none"> • The Board of Trustees • The President and Executive Leadership • Information Technology (IT) Department • Faculty, Staff, and Students • External technology vendors and consultants
4.0	Policy:	<p>QCC shall develop, implement, and maintain a Technology Master Plan to guide the planning, acquisition, maintenance, and development of technology resources. The TMP will be reviewed and updated periodically to accommodate advancements in technology, cybersecurity best practices, evolving institutional priorities, student learning needs and legislative and other changes.</p> <p>The TMP shall:</p> <ol style="list-style-type: none"> 1. Align with the College’s Strategic Plan and academic priorities. 2. Support accessibility, cybersecurity, data privacy and governance, and operational efficiency. 3. Comply with local, state, and federal regulations regarding technology and data security. 4. Ensure that technology investments are planned in a fiscally responsible and sustainable manner.

5.0	Definitions:	<ul style="list-style-type: none"> • Technology Master Plan (TMP): A strategic document outlining short-term and long-term goals for the College's technology infrastructure, software, hardware, and digital resources. • Cybersecurity Standards: Policies and practices to protect the College's digital assets, networks, and data. • Enterprise Systems: Institution-wide software applications such as Learning Management Systems (LMS), Student Information Systems (SIS), and Enterprise Resource Planning (ERP) systems. • Technology Refresh Cycle: A planned schedule for updating or replacing hardware and software to maintain efficiency and security.
6.0	Responsibilities:	<p>Board of Trustees</p> <ul style="list-style-type: none"> • Approves the Technology Master Plan and any major revisions. • Provides oversight to ensure alignment with institutional goals and budget constraints. <p>President and Executive Leadership</p> <ul style="list-style-type: none"> • Oversees the development and execution of the TMP. • Ensures alignment with the College's strategic objectives and academic needs. <p>Information Technology (IT) Department</p> <ul style="list-style-type: none"> • Develops, maintains, and implements the TMP in coordination with relevant stakeholders. • Ensures cybersecurity, data privacy, and compliance with technology regulations. • Conducts regular assessments of technology needs and infrastructure. <p>Faculty, Staff, and Students</p> <ul style="list-style-type: none"> • Provide input on technology needs and priorities. • Follow cybersecurity guidelines and responsible technology use policies. <p>External Technology Vendors and Consultants</p> <ul style="list-style-type: none"> • Adhere to the TMP's security, data privacy, and technology standards.

7.0	Procedures:	<p>Development & Review</p> <ul style="list-style-type: none"> • The TMP shall be developed and reviewed every 5 years. • The review process shall include consultation with faculty, staff, students, and external stakeholders. • The IT Department will establish a process to collect feedback on a proposed final draft from the campus community before submitting a final draft to the President. • If a Technology Master Plan does not currently exist, or if it is out of date, QCC will create/update the TMP within 2 years. <p>Approval Process</p> <ul style="list-style-type: none"> • The IT Department drafts the TMP and presents it to the President. • The President submits the TMP to the Board of Trustees for approval. <p>Implementation & Maintenance</p> <ul style="list-style-type: none"> • Approved technology projects and initiatives are integrated into annual budgeting and planning. • The IT Department ensures ongoing cybersecurity, system updates, and infrastructure maintenance. • Annual progress reports are prepared and submitted to the President and Board.
8.0	Sanctions:	<p>Failure to adhere to this policy may result in:</p> <ul style="list-style-type: none"> • Suspension or delay of technology projects. • Financial or administrative penalties for non-compliance with cybersecurity or data privacy regulations. • Disciplinary action for employees who fail to comply with technology security and usage policies. • Contractual penalties for external vendors who fail to meet TMP guidelines.