Executive Summary

The purpose of the *Technology Master Plan* is to provide a roadmap for Hartnell Community College to apply technology and achieve its strategic plan goals. The *Technology Master Plan* considers technology trends and outlines how the district will leverage technology to meet students' technology needs and enable them to successfully transfer and earn degrees and/or certificates. As technology changes, the district needs to be able to maintain secure and reliable core services while proactively introducing new technical solutions to support the district's strategic goals.

Some of the key technology needs addressed in this plan include providing ongoing support for and upgrading of the student information system (SIS); implementing a technology refreshment plan; enhancing campus Wi-Fi; enhancing core network infrastructure, staffing, and security; and developing a disaster preparedness/recovery and cybersecurity response plan.

The Hartnell College *Technology Master Plan* is a living document that will be reviewed periodically by the Technology Development Council and updated as necessary. Major revisions of this document will be made based on updates to associated documents, such as institutional goals, strategic initiatives, and/or the college's mission. Ongoing meetings with individuals, shared governance committees, functional area groups, and campus-wide surveys will be used to continue gathering data.

During the planning process, objectives were identified and milestones set for a range of projects, including administrative system enhancements, classroom technology improvemeel2MCID 11o/F000091 72.02s(ch)11ETCEMC /P AMCID

NAME/TITLE/COUNCIL POSITION	REPRESENTING

e) Enhance the help desk

Equip the help desk with call routing/queuing (hunt group) to enable callers to leave messages or hold for an available help desk support technician.

f) Conduct staff/resource evaluation

Balance staff workloads to accord with Gartner industry standards.

Lead: ITR

Indicators of success

- *Items 1a, 1b, and 1c* will be measured using an IT satisfaction survey.
- *Item 1e* will be measured based on Gartner and community college workload comparison(s).

Technology and Professional Development

Accreditation Standards:

will b

b)

Develop a comprehensive security breach plan that includes communication, analysis, mitigation, recovery, and improvement.

Develop security policies that incorporate information protection processes and procedures.

Develop standard operating procedures that include the security maintenance of software and hardware, including the detection and monitoring of systems.

Conduct tests, training, and exercises to

Current state
The technology at each site varies in age and function. Some programs have expanded and require upgraded technology solutions, and industries are moving toward digitization, automation, and robotics. However, the technology infrastructure at the sites is currently inadequate for supporting the changing/growing demands.

Desired state
Future-focused technology infrastructure at all district locations. Technology will support the programs offered at each location and will be reviewed annually.

Plan
a) Establish baseline technology and identify gaps
Establish inventory and baseline technology based on identified gaps to support all programs offered.

b) *Develop technology planning*
Establish a workgroup to ensure that technology meets program and future employment needs.

Lead(s): ITR, AA

Indicators of success: IT survey

Section 4: Website

Accreditation Standards: III.C.1, III.C.3, III.C.4, III.C.5

Current state
The district's current website houses information for potential students, students, faculty, staff, and the community. The website includes items that must be made publicly available. The district is in the process of evaluating and redesigning the website based on the Chancellor's Office Vision for Success and the Guided Pathways initiative.

Desired state
A refreshed district website will focus on prospective students and the community, with portals for current students and employees.

Plan

Establish a cross-functional workgroup charged with oversight of and accountability for the new website.

Appendix A: Accreditation III C—Technology Standard

Standard III.C.1: Technology Resources

1. Technology services, professional support, facilities, hardware, and software are appropriate and adequate for supporting the institution's management and operational functions, academic programs, teaching and learning, and support services.

POSSIBLE SOURCES OF EVIDENCE: technology plans or program reviews that evaluate and plan for reliability, disaster recovery, privacy, and security; technology inventories; technology infrastructure blueprints; disaster recovery procedures or plans.

Review criteria and possible sources of evidence for the DE/CE technology plan and/or other documents that demonstrate the institution is aligned with

2. The institution continuously plans for, updates, and replaces technology to ensure its technological infrastructure, quality, and capacity are adequate for

The institution provides an appropriate system for reliability and emergency backup.

Standard III.C.4: Technology Resources

4. The institution provides appropriate instruction and support for faculty, administrative staff, and students in the effective use of technology and technology systems related to its programs, services, and institutional operations.

POSSIBLE SOURCES OF EVIDENCE: technology training schedules for staff and faculty; presentations or agendas on technology professional development opportunities; evaluations of training, and documentation of improvements to subsequent training for staff and faculty; technology training schedules for students; curricula for training students on technology usage; resources, such as manuals or online instructions, that support students, administrative staff, and faculty in their use of technology; and/or other documents that demonstrate this institution is aligned with the institution.

REVIEW CRITERIA: The institution assesses the need for IT training for students and personnel.

The institution ali20cETOEMC /P AMCID 10>BDC q9(n)Tf1 -6q12nstitutionini231 0 0 1 1G[p
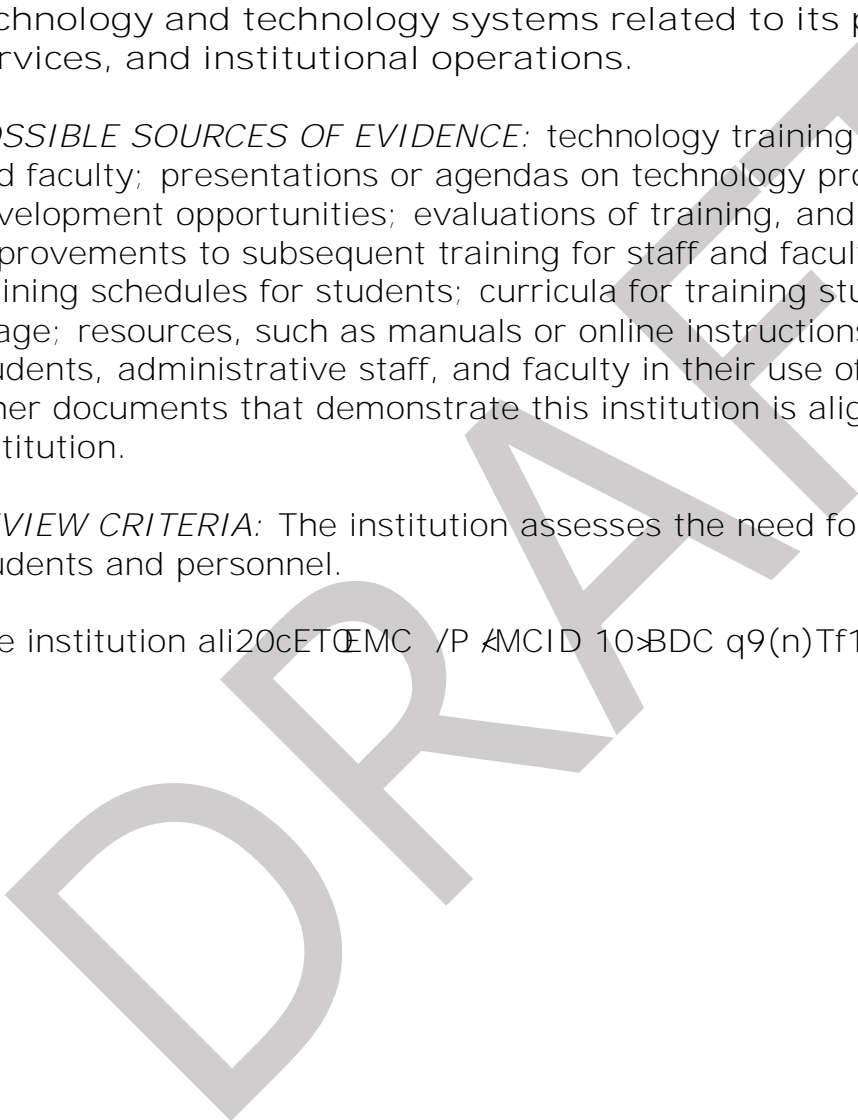
Appendix B: ITR Program Review

Department /Program	Priority within Category	Description of Request	Activity
ITR	1	1 FTE	Hire a director of information security & technology resources

ITR

functions. All functions will ultimately be continued as the campus returns to normal operations.

While developing the plan, departments should consider the following:

- operating at an alternate location
- continuing without the data network
- continuing with a reduced workforce
- how communications will work without email
- line of succession and delegation of authority
- continuing education (how will instruction continue?)
- special considerations

Operational checklists should also be developed. Checklists may be designed to list the responsibilities of a specific position or the steps required to complete a specific task. Sample operational checklists may include:

- phone trees
- key personnel rosters and critical functions checklists
- critical function recovery team checklists
- telecommute/alternate work location checklists
- emergency operating records and IT checklists
- emergency equipment checklists

Appendix F: Board Policies and Procedures

AP 3720 Computer, Electronic Communication, and Network Use