

## A. Technology Resources

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

### Evidence of Meeting the Standard

Technology in the District is a critical component of multiple aspects of teaching, learning, and student support, as well as the foundation and infrastructure for all administrative and business operations throughout the District. As a multi-College District serving multiple campuses and locations throughout the City of San Diego, there are aspects of technology centralized to the District Office's Information Technology Services department and others decentralized to the Colleges' Information Technology areas. Technology-related services, hardware, and software are regularly evaluated, upgraded, and maintained through both District-wide process and efforts are being made at the individual campus level in order to provide appropriate and adequate technology support and services to the entire District's management and operational functions.

District services operate under the umbrella of the District Information Technology (IT) Director, and campus technology services operate under the College's School of Planning, Research, Institutional Effectiveness, and Library (PRIEL). The two departments are broadly categorized as "Administrative Computing Support" and "Instructional Computing Support", respectively.

### Analysis and Evaluation

The Colleges support the teaching and learning technology service-related needs of the academic programs at each institution, with the District's IT department providing Districtwide network infrastructure, hardware and software, telephone operations, data center, and "helpdesk" services to all four Colleges in addition to being responsible for the District Office's various locations. The District IT department is also responsible for the Districtwide library system and web servers, the administrative ERP (Enterprise Resource Planning) system's hardware and software configuration, installation and maintenance, and the standards for all technology software and hardware used throughout the District. The current District Technology Replacement Plan's priority is server upgrades, which require a comprehensive evaluation of the various physical and virtual servers within the District.

The District provides district wide software licensing for many essential and commonly used software packages such as the Adobe suite and Microsoft Office, as well as other essential Enterprise products such as Antivirus tools.

The District assures a robust and secure technical infrastructure for distance education (DE) classes through cloud-managed hosting with Canvas. Canvas uses redundant Amazon Web Services to provide highly available, robust services. The technical infrastructure is evaluated and maintained by Canvas. Reliability and support of the resources are monitored and provided

through a 24/7 Canvas Help Desk phone, email, and chat services. District students, faculty, and classified professionals have access to support services. Canvas also schedules security maintenance adhering to ISO 27001 (Evidence: IIIC2<sup>12</sup>). In addition, other technological resources are subscribed to, and the vendor sites maintain the services. A list of district wide technology available to the Colleges and terms of subscription are posted publicly. (Evidence: IIIC2<sup>13</sup>)

SDCCD Online Learning Pathways archives courses for three academic years. Archives are kept on backup Amazon Web Servers with redundancy across the United States and are accessible by written request by authorized personnel. Student information is restricted according to Family Educational Rights and Privacy Act (FERPA), and only selected data is uploaded to the server. Student information is not archived.

All student records are secured by multiple technologies, including firewalls installed on local servers. The student and course data are refreshed on a four-hour cycle throughout the semester. Both students and faculty have secure logins to the Canvas system. In addition, the District IT department and the College IT areas ensure all campus computers can connect to the Canvas data centers with reliable networking equipment, reliable and sufficient speeds of WAN bandwidth, and high-speed internet access. All the systems are monitored daily for reliability and bandwidth capacity.

The District does not provide “Personally Identifiable Information (PII)” data for students to the Canvas system. Only the student-assigned District ID is provided and matched along with course reference number information to build Canvas course rosters. The instructor of record manages the coursework in Canvas and is responsible for inputting attendance and grade information into the District’s administrative Enterprise Resource Planning (ERP) system.

The District IT department maintains a complete inventory of all the equipment it is responsible for supporting. It is funded by a general maintenance budget to maintain and refresh technology every five years. (Evidence: IIIC2<sup>14</sup>)

District IT utilizes various network management tools to monitor the quality and capacity of network segments, wide area network circuits (WAN), file server response times, disk capacities, and Internet bandwidth. This data is shared with the Colleges and District planning groups to ensure resources are efficiently and effectively expended. District IT also maintains and operates an IT Helpdesk where all support calls are logged, tracked, and reviewed monthly to determine trends in equipment failures and support service challenges.

Several Districtwide advisory committees ensure compliance with standards related to technology and acquisition, particularly regarding technology equipment, applications, and support services bid documents through Requests for Proposals (RFPs). The advisory committees serve as a resource to the District’s Director of Information Technology Services to solicit input from the Colleges regarding network and technology infrastructure capacity to ensure the District can support the academic and administrative program needs of the

College's IT services. The advisory committees also serve as an informal information-sharing opportunity with regard to information technology to ensure standards are established and adhered to district wide. RFPs communicate the District's equipment and construction standards to which vendors need to bid on or be in compliance with their bids, solution designs, and installations. The construction standards related to technology are addressed in construction-related RFPs for new and existing buildings to ensure compliance with standards.

Examples of District IT department-supported systems are:

- Administrative Enterprise Resource Planning (ERP) Systems (Student System including Financial Aid, Finance, PCTS, and Payroll)
- Campus-based local area networks (LAN)
- Internet and Intranet Security Systems
- Communications Infrastructure (Internet, Intranet, District phone system, Voice Mail, and emergency communication systems)
- District Web Services (Campus websites and portals)
- Remote Access Services
- Student, Course, and Instructor data for the Canvas learning management system
- Building Communications and Audio-Visual Infrastructure

These systems are all covered by the District IT department's technology maintenance and refresh budget. Major system replacements are capital budget project requests, funded through the District Office's Districtwide budget prioritization process.

The District takes steps to provide for Disaster recovery through multiple means, such as providing for redundant power (e.g., the District Data Center provides both UPS and Diesel generator power backups), and District data is regularly backed up to tape and stored both on-site and off-site.

At the college level, planning begins with the annual Program Review process, where departments identify upcoming technology needs [whereas available resources can address priorities](#) (EVIDENCE: Sample resource request). There are provisions for reliability, disaster recovery, privacy, and security, when considering the College's technology needs. Provisions for disaster recovery/security are discussed in section III.C.3.

The College [strives to meet](#) technology needs through both governance and operational processes. Needs are assessed across campus during the annual Program Review process, where each instructional or service department identifies needs which are compiled as "Requests for Funding (RFFs)". This information is vetted through the Budget & Resource Development Subcommittee (BRDS), which recommends the allocation of various funds based upon the Program Review process (EVIDENCE: Sample BRDS Minutes with RFF review). The college's Instructional Computing Support Supervisor is a defined member of the BRDS committee to ensure technology needs can be assessed with a comprehensive viewpoint.

Additionally, BRDS vets all technology requests from Program Review through the campus Technology Committee for review (EVIDENCE: Technology Committee Agenda). Moving forward, the college will make efforts to strengthen communication of resource requests (e.g., technology) and their status. To ensure better integration with District IT, the College's Technology Committee has defined a position for the District IT director (or designee).

These departmental needs are consolidated and prioritized for each school/operational area. The requests are sent to BRDS, followed by the Technology Committee for further review and prioritization. Generally, the Technology Committee does not reprioritize most requests. However, it looks for areas that can be handled with existing equipment/services, consolidates requests to avoid making many small purchases, and ensures standards are being adhered to where possible. This updated prioritization is then formally proposed as a recommendation to the BRDS committee. Both the Audiovisual and Instructional Computing Support departments provide input into the prioritization.

In addition to the formal processes outlined above, BRDS maintains an emergency fund to handle unplanned events. Not all funds go through the BRDS process. Individual departments and schools have their own discretionary budgets which may be used as deemed necessary by the department/school administrator without utilizing the BRDS process. Campus-wide technology support departments routinely plan for technology upgrades via both internal and BRDS processes (EVIDENCE: AV Priority list, Campus Computer replacement list). Other examples of funds that can be used independently of the BRDS process would be grant funds which are already very specific to a purpose, and the emergency funds provided during COVID which needed to be utilized in a timely manner to ensure students were provided the support needed. For instance, during COVID, federal funds were utilized to provide students access to laptops allowing them the opportunity to succeed in a remote-only situation.

## **2. The institution continuously plans for, updates and replaces technology to ensure its technological infrastructure, quality and capacity are adequate to support its mission, operations, programs, and services.**

### **Evidence of Meeting the Standard**

The Colleges and District IT departments ensure that various technology needs are identified, updated, and replaced through multiple planning and administrative processes to ensure technological infrastructure, quality, and capacity are adequate to support its mission, operations, programs, and services. This occurs through several methods whereby the District IT department and Colleges collaborate on technology-related issues. Each College has an Information Technology Committee with constituency representation serving on the committee to provide input for planning, budgets, and timelines to address technology issues at each institution.

At the college level, existing technology such as classroom/lab computers and projection systems are identified and prioritized for maintenance or replacement as resources are available. New or specialized technology needs are planned for via the campus-wide program

review process. Resource requests are then funneled to the appropriate technology department that work with the requestors to ensure standards are met, reduce duplication, and provide input on prioritization of requests to the BRDS Committee. The campus is currently planning to expend a significant amount of PPIS funding to update existing computer infrastructure as well as audiovisual installations (Evidence: PPIS document).

### **Analysis and Evaluation**

To ensure coordination of Districtwide technology needs, the District's Information Technology Services Director attends the various College IT committee meetings to share planning information related to Districtwide operational technology projects. In addition, the District recently added a Districtwide Technology Committee that consists of individuals possessing technical and functional technology skills and knowledge representing the District offices with the four Colleges. The Technology Committee was formed to ensure a venue by which broad-based communications related to Districtwide technology support and services may be addressed.

The District maintains a redundant leased fiber connection currently providing 10Gbit Internet connectivity to the District and ensures all Colleges have sufficient Internet bandwidth to meet the needs of students and staff. (Evidence: IIC2<sup>1</sup>)

In addition to working with the Districtwide technology advisory groups, the District IT department works closely with the Purchasing and Contract Services department in developing all RFPs related to technology acquisitions and the development of technology standards Districtwide. Each major technology vendor utilizes the District's "Track-IT" IT Help Desk software, enabling automatic tracking, status, and dispatch of support staff for problems or work request tickets. This process enables the District to identify problem equipment to assist in modifying computer, printer, and audiovisual standards as necessary, as well as vendor support issues.

The District makes decisions about the use and distribution of its technology resources at the District level with input from each College through the Districtwide Distance Education Steering Committee (DDESC) and Educational Services Software Workgroup (ESSW). DDESC and ESSW facilitate discussions about district wide evaluation, adoption, and review. DDESC members participated in a Canvas Learning Management System (LMS) pilot, and in the summer of 2019, the District fully transitioned into Canvas LMS. (Evidence: IIC2<sup>9</sup>)

Additionally, ESSW reviews Districtwide technological resources and makes recommendations to acquire those resources. Recently, the district's plagiarism solution was reviewed in fall 2021 by the committee via an evaluation group comprised of faculty at each College and the Online Learning Pathways department. After evaluating various solutions, the ESSW voted to acquire TurnItIn to replace the current Unicheck plagiarism system. (Evidence: IIC2<sup>10</sup>) ESSW also annually reviews software (accessibility, plagiarism, student communication, online tutoring) offered to Colleges at a discount through the California Community College Foundation's Systemwide Technology Access Collaborative (Evidence: IIC2<sup>11</sup>)

SDCCD Online Learning Pathways coordinates a student satisfaction survey with the District Institutional Research and Effectiveness department bi-annually to review and assess students' needs. The survey results are shared with the DDESC, which makes recommendations accordingly. For example, survey results from a 2020 student need survey showed a desire for faculty to complete the online certification program to improve teaching abilities. **IIIC2<sup>5</sup>**. Based on the survey results and upon recommendation and support of the DDESC, the Online Faculty Certification Program capacity was increased to support. (Evidence: **IIIC2<sup>14</sup> IIIC2<sup>15</sup>**). SDCCD Online Learning Pathways staff monitors and evaluates the inquiries to the Help Desk. For example, the staff reviewed the inquiries and found that students' most frequent problem was password information for logging into Canvas. To help solve the issue, automatic emails are sent to all registered online students one week before their class, starting with information on how to log in to Canvas before the start of each semester session. In addition, login instructions are included in the online class section of the printed class schedule and posted directly on the Canvas login page. (Evidence: **IIIC2<sup>16</sup> IIIC2<sup>17</sup>**)

The District provides various services, including technical and hardware support, infrastructure, Internet and telecommunications, and instructional platforms. In collaboration with the College's IT staff, the District has a process for identifying and prioritizing technology needs and works with College IT to ensure those needs are met.

The College is currently soliciting participation in the Districtwide Technology Planning Process to help strengthen collaboration. IT needs are The College's ability to plan for multi-year technology projects is limited due to the fluctuation of available funding in a given fiscal year. All funds used for campus technology must generally be expended in that year, and there is no guarantee that funding will continue to be available for larger projects.

### **3. The institution assures that technology resources at all locations where it offers courses, programs, and services are implemented and maintained to assure reliable access, safety, and security.**

#### **Evidence of Meeting the Standard**

The District IT department is primarily responsible for technology security, as all enterprise systems reside at the District level. For instance, District IT is responsible for such Enterprise services as student records, email servers, PeopleSoft, Canvas, etc. However, the College website is the responsibility of the College. The College ensures its labs and classrooms are maintained and updated regularly via annual allocations of PPIS funding (EVIDENCE: **Sample BRDS Minutes with RFF review**). All campus instructional systems are deployed with suitable antivirus tools and use DeepFreeze to ensure reliability.

District IT systems are operational seven days a week, 24 hours a day. Each server is backed up nightly to a system that duplicates the data for onsite and offsite storage. Backups are copied to tape, placed into a safe weekly, and transported offsite to a secure location in case

of a disaster.

The District IT department is responsible for a maintenance budget that covers all the hardware and software it supports and is responsible for throughout the District. The District maintains various maintenance and support contracts depending on the systems' critical nature and the downtime impact. Critical systems such as the Administrative Enterprise Resource Planning hosts (PCTS/Payroll, Finance, Student, and Financial Aid) have seven days a week, 24 hours a day on-site maintenance agreements. Other less critical systems have five days a week, 8:00 am to 5:00 pm on-site service agreements with spare-in-the-air service (manufacturer sends replacement parts before receiving the failed part). Spare-in-the-air support agreements are always preferred because the supplier is responsible for sending the replacement part upon contact rather than waiting to receive and verify the failed part, which may often take days to receive a new replacement part.

In addition, the District maintains a stock of critical spare parts for the IT staff to use for replacement purposes, which is usually quicker service than vendors can provide. Examples of such parts are network switches and blades, servers, and raid array hard disks.

The District IT department also utilizes various network management tools to monitor the quality and capacity of network segments, wide area network circuits (WAN), file server response times, disk capacities, and Internet bandwidth. All District computer equipment is behind multiple firewalls using network address translation (NAT) technology, which translates the names of District computers visible to the public to internal TCP/IP addresses of the servers to prevent hackers from seeing or having direct access to District servers.

Regarding security, all Active Directory servers authenticate user accounts and passwords. Web servers utilize Secure Socket Layer (SSL) encryption for data security, preventing hackers from seeing or stealing employee login IDs and passwords.

The District IT department provides and supports the network infrastructure, including cloud and file servers, and ensures the core data and telecom services are available at all District locations. These include telephone service with local four-digit dialing for internal District calls and voice mail, local microcomputer and network service, internet services, email service, and access to core administrative services such as the Student Campus Solutions, Financial Aid, and People, Culture, and Technology Services departments.

### **Analysis and Evaluation**

The College ensures reliability and security of its systems through multiple means. Antivirus software (Avast, ESET or Defender) is installed on all systems, and all instructional computers also employ DeepFreeze, which ensures systems are always rebooted in a clean state. Production servers are all virtualized and regularly backed up via Veeam and additionally, critical files are backed up separately, such as the Pay-4-Print and website databases. Administratively, faculty and staff [have access to network drives](#) share to store work and important files, which is backed up by District IT. All enterprise services provided by the District are backed up regularly



and copies are kept off-line and off-site as well. This includes email, student records, financials, etc. Internet connectivity to the District is provided by redundant 10 Gigabit links, and all servers are protected by the District firewall. Physical security is maintained by separately-keyed telecom rooms and coded access to the data-center which is also staffed 24 hours per day. Expensive equipment such as projection systems are physically secured as well.

The campus website is backed up daily, as both a full virtual machine backup (via Veeam) and as a set of file backups of the website database and file-system. Further, the website utilizes standard open-source tools such as Composer and Git, which allow a complete server rebuild to be nearly fully automated.

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

##### **Evidence of Meeting the Standard**

Instruction and support of staff and administrators at the District Office related to the use of technology and technology systems are primarily done on an as-needed basis via requests made through the District Help Desk. As new technology applications or equipment comes on board at the District Office, the District IT department offers training opportunities, e.g., staff and administrators attended training sessions when the new Microsoft Office version was implemented. In addition, in coordination with the District's People, Culture, and Technology Services department, the District IT department funds a 50 concurrent-user license account subscription with the State Chancellor's Vision Resource Center for self-paced, professional development service for all employees to remain current on over 100 products, including Microsoft Windows, Microsoft Office Suite, programming languages, techniques and tools, Adobe products, Microsoft Certified Network Engineer training, SharePoint, SQL Server, AutoCAD, Java, Apple IOS, Final Cut, and many more.

##### **Analysis and Evaluation**

With regard to faculty, staff, and administrators' training related to the use of technology and technology systems related to teaching and learning, the District, in partnership with the Colleges, provides training and support for faculty, staff, students, and administrators, in the effective use of technology and technology systems related to its programs, services, and institutional operations using several methods to obtain feedback to include the following:

- An Online Student Satisfaction Survey is administered bi-annually.
- At the end of each technology training workshop, a short questionnaire is submitted by participants regarding other technological training needed.
- Faculty mentors serve on the Districtwide Distance Education Steering Committee from the campuses and report to the Dean, Online and Distributed Learning about any training requested.
- Also, the Flex Coordinator at each campus solicits suggestions for faculty training.
- The Colleges also rely heavily on the District's Online Learning Pathways to provide



technology training for distance education teaching. Online Learning Pathways regularly offers the Online Faculty Certification Program. The rigorous certification activity, facilitated and graded by District instructional designers, is self-paced and requires an average of 20-30 hours to complete. Over 1,000 contracts and adjunct faculty have completed the course and received certification. The course is required for teaching distance education courses in the District.

The District's Online Learning Pathways (OLP) offers extensive training to faculty and staff in using the Canvas Course Management System, online pedagogy, and general educational technology applicable to online learning. Each semester, a series of general instructional technology workshops pertinent to both online and classroom instruction is offered by SDCCD Online Learning Pathways staff. These workshops may be face-to-face, online synchronous, or online asynchronous. Topics addressed include media production, regular and substantive interactions, accessibility, online learning, and many more. OLP also provides a Distance Education Handbook, which includes policy, procedure, technology resources, and best practices. At the end of each workshop, the participant receives evaluations via face-to-face, email, or an online questionnaire. (Evidence: I11C4<sup>9</sup>)

In addition, OLP has made available a Student Orientation available for all students taking an online class. The orientation covers time management, organizational skills, local resources, and navigating the LMS. OLP has a 24x7 Help Desk to support faculty and students with technology-related problems accessing Canvas.

The College offers training on the use of campus technology to staff primarily, through the Audiovisual and Instructional Computing Support departments. Training is provided either in-person (individual or group settings) and informational videos may be provided either as a supplement to or in place of in-person training (EVIDENCE: SDMC Website Video Tutorials.pdf). Additionally, selected faculty and staff are provided training as college website content editors on an individual and group basis (EVIDENCE: SDMC Website Content Editor Training Session.pdf )

Faculty and staff are required to go through a training session prior to being given access to use the instructional podiums. This training, provided by the Audiovisual Department, ensures the end-user knows how to properly use the standard equipment in classrooms. Instructional Computing Support/Web Services provides individual training to content authors who publish content for the College website. Self-help videos on the Web Services department page are also available, along with a style guide, FAQ and other information. Individual assistance is also available for various issues as needed from all technology departments; Audiovisual (AV) Department, Instructional Computing Support (ICS), and Web Design.

**5. The institution has policies and procedures that guide the appropriate use of technology in the teaching and learning processes.**

## Evidence of Meeting the Standard

### Distance Education:

The institution has policies and procedures that guide the appropriate use of technology in teaching and learning, as evidenced in AP 5105. According to AP 5105, the Vice Chancellor of Educational Services, or designee in collegial consultation via the District Governance Council, shall utilize one or more methods of secure credentialing/login and password, proctored examinations, or new or other technologies and practices that are effective in verifying student identification. In addition, guidelines for good practice are included in the Online Faculty Certification Program and SDCCD Online Learning Pathway's Distance Education Handbook.

On-campus, all computers are protected by an anti-virus product and, with few exceptions, instructional systems (e.g., computer labs) utilize DeepFreeze. This ensures that students are afforded a level of protection and that the systems remain consistent and stable from day-to-day. In order for ICS to provide effective service to so many systems, ICS ensures that, to the extent possible, all systems be grouped into large blocks of identical systems. This practice allows for the maintenance of a single hard-drive image, making it much easier for ICS to update an image to provide the latest software. The college wide practice is that most technology purchases go through the Audiovisual Department, Administrative Computing Support or Instructional Computing Support for signatures. This allows these departments to review and ensure all systems purchased are standard, or that there is a justification for deviating from the standard. Systems can then be replaced under a roll-down process (please see Standard III.C.2 for details), so that individual requests from departments Requests for Funding are aggregated into a single large block purchase of identical systems when possible. This block of computers can then replace computers in large labs, providing "roll-down" systems to handle the needs of smaller labs or various departmental requests.

### Analysis and Evaluation

As evidenced by the college-level and district wide processes that guide technology use, the College and the District follow established policies and procedures that outline the appropriate use of technology in the teaching and learning process

The District provides Board Policies (BP) and Administrative Procedures (AP), which determine the appropriate use of technology. The specific BP/AP's relating to this are: BP/AP 3720 (Computer and Network Use), AP 3721 (Electronic Mail and Digital Communication) and BP/AP 3310 (Records Retention and Destruction). These BPs and APs are then implemented and followed by the District and Campus technology departments. Additionally, the College provides its own procedures (staying within the BP/AP guidelines) for the use of technology where appropriate. For example, the College utilizes antivirus protection on all systems, ensures we remain within our licensing agreements by employing Sassafras Keyserver, and works collaboratively with District IT when implementing security procedures (**Evidence: Security Squirrel Emails**)

---

### **Conclusions on Standard III.C: Technology Resources**

As evidenced above, San Diego Miramar College meets this standard. The College works in collaboration with the District [in an effort to ensure](#) faculty, staff and students have access to current and effective technology for administrative and academic purposes. The College utilizes program review and the governance processes effectively in identifying technology needs and planning appropriate allocations of funding. Instructional classroom technology is regularly updated through this process, [based on available resources](#). College and District IT collaborate through multiple means. Formal processes such as the Districtwide Technology Committee bring together key stakeholders from across the District, and the District IT Director (or designee) is a member of the College Technology committee. College faculty and staff have access to training on campus technology regularly via planned events, online resources (video tutorials, Vision Resource Center, etc.) as well as individual appointments. Security of information systems is a shared responsibility between the College and the District. The District has the larger burden as they maintain the enterprise systems with critical and sensitive data, which is protected via multiple means including firewalls, encryption and other enterprise security tools and methods such as multi-factor authentication. The College collaborates effectively with the District to ensure systems are deployed with appropriate tools to protect the systems and end-users.

### **Improvement Plan(s)**

[Through the campus Technology Committee, the campus will be involved in identifying ways to improve training and communication processes to track measurable progress.](#) Specifically, improvement plans are identified for III.C.1 and III.C. 2.

III.C.1 [The College will make efforts to strengthen communication of resource requests and their status.](#) A feedback process will be developed in that all technology requests submitted by the campus Technology Committee during the program review process will include ongoing communication to the originator.

III.C.2 To strengthen collaboration, [the College will participate in the Districtwide Technology Planning Process in efforts to](#) improve the College's ability in planning for multi-year technology projects. The District and College respective plans will be integrated to include necessary [technology training, processes to communicate IT needs, resource allocation, milestones, measurable progress, and deliverables.](#)

### **Evidence List**

[List forthcoming](#)

---