



San Bernardino Community College District
 POLICIES & PROCEDURES ADVISORY
 COMMITTEE (PPAC)
 October 17, 2024
 3:00 pm-4:30 pm Pacific Time

MEETING AGENDA

Via Zoom: <https://cccconfer.zoom.us/j/91470895848>
 Or Dial-In: 669-900-6833 | Meeting ID: 914 7089 5848

A. Welcome & Introductions

Kristina Hannon and Jose Torres, Co-Chairs

B. Approval of Meeting Minutes

1. Confirmation of Quorum
2. 09/19/2024

C. Review of Final Input from Academic Senate - Level 3

These items were anticipated to appear on the 5/15/2024 Academic Senate agendas for Final Review. They are scheduled to appear on the 11/14/2024 BOT agenda for first read.

1. 5075 Course Adds, Drops, and Withdrawals

D. Review of Feedback from Constituents and Initial Input from Academic Senate - Level 3

These items are anticipated to appear on the 11/121/2024 PPAC Agenda for first final Academic Senate input.

1. 4300 Field Trips and Excursions

E. Feedback from Constituents and Academic Senate - Level 2

These items are anticipated on the 11/14/2024 BOT agenda for first read.

1. Family of IT P&Ps
 - i. 3725 Information and Communications Technology Accessibility
 - ii. 3726 Information Security Data Classification
 - iii. 3727 Information Security Access Control
 - iv. 3728 Information Security Physical Security
 - v. 3729 Information Security Logging and Monitoring
 - vi. 3730 Information Security Remote Access

- vii. 3731 Information Security Internally Developed Systems Change Control
 - viii. 3732 Information Security Security Incident Response
 - ix. 3733 Information Security Secure Operations
 - x. 3734 Information Security_Network Security
 - xi. 3735 Information Security Disaster Recovery
 - xii. 3736 Information Security Cloud Storage
 - xiii. 3737 Information Security_Payment Card Industry Requirements
- 2. 5030 Fees with Minor Chapter Lead Feedback (note slight change in language shown in green)
 - 3. 6925 Refreshments or Meals

F. New Chapter Lead Recommendations

- 1. Level 1 (information only)
 - None
- 2. Level 2 (minor review)
 - i. 3250 Institutional Planning
- 3. Level 3 (extensive review)
 - i. 4010 Academic Calendar
 - ii. 4020 Program, Curriculum, and Course Development
 - iii. 4100 Graduation Requirements
 - iv. 4230 Grading and Academic Record Symbols
 - v. 5012 International Students
 - vi. 5035 Withholding of Student Records
 - vii. 5055 Enrollment Priorities
 - viii. 5530 Student Rights and Grievances

G. On the October 10, 2024 BOT Agenda

- 1. BOT 1st Read
 - 2015 Student Trustees
 - 2355 Decorum
 - 2430 Delegation of Authority to the Chancellor
 - 2715 Code of Ethics/Standards of Practice
 - 2731 Trustee Emeritus
 - 5500 Standards of Student Conduct
- 2. BOT Final Approval
 - None

H. Adjournment & Next Meeting

The next PPAC meeting is scheduled for Thursday, 11/21/2024
at 2:30 p.m.



Policies & Procedures Advisory Committee
Meeting Minutes – September 19, 2024, 3:00 p.m.
 Via Zoom: <https://cccconfer.zoom.us/j/91470895848>
 Or Dial-In: 669-900-6833 | Meeting ID: 914 7089 5848

A. Welcome & Introductions

Jose Torres started the meeting shortly after 3:00 p.m. Those that were new to the committee made self-introductions.

B. Approval of Minutes

1. Confirmation of Quorum

Quorum was confirmed.

2. 05/13/2024
3. 08/15/2024

Ray Carlos made a motion to approve both sets of minutes which Karen Peterson seconded. The minutes were approved by a majority vote with Carmen Rodriguez, Chris Olivera, and Jessy Lemieux abstaining.

C. 2024-25 Annual Review List

Members discussed the Annual Review List with 120 items. It was stated that the list is a “living” document which will update throughout the year to reflect the committee’s work. This item will go before the Board in October. Kelly Goodrich made a motion to approve the list which Carmen Rodriguez seconded. The motion was approved by a unanimous vote.

Jeff Demsky joined.

1. 7250 Educational Administrators and 7340 Leaves – Remove 10+1 Designation 2024-25 Annual Review List

Kristina Hannon addressed the committee regarding the proposed removal of 10+1 designation from 7250 Educational Administrators and 7340 Leaves. She maintained that the 10+1 designation does align with two policies.

- *7340 speaks to Leaves, which are mandated by different regulations and negotiations. We can’t just decide to include or not.*
- *As far as the hiring process is concerned, we definitely want to continue to include the Senate voice, faculty voice, and honor the shared role of participating in the process. However, 7250 is beyond the hiring process, and speaks to personnel items like retreat rights. HR is tasked with making sure everyone’s personnel rights are observed in alignment with all regulations.*

- It was commented that a large portion of 7250 has to do with the hiring of the administrators which makes it seem like, although there are other elements, it is related to 10+1.
- Ray commented that 7250 sounds to him like it is very specific about hiring managers. The retreat rights are just to identify the rights, not necessarily the process for that, which is the big difference here.
- Andrea Hecht asked about the fact that educational administrators are overseeing faculty and felt that this may indicate 10+1.
- Kristina advised that the faculty voice is part of the process but the hiring process is not part of the AP. The process does need to be a collaborative effort, but it is not necessarily part of 7250.
- Committee members also discussed the fact that any changes to 7250 would still undergo a Level 2 review and that members of PPAC would see the changes and share with constituent groups.



Kristina made a motion that 7250 and 7340 be changed from Level 3 review to Level 2 review (thereby removing the 10+1 designation). Carmen Rodriguez seconded the motion which passed by a majority vote with Jessy abstaining.

D. Review of Final Input from Academic Senate - Level 3

1. 5500 Standards of Student Conduct

For the benefit of new members, Jose highlighted the date lists on the recommendations and the colors of the different changes, i.e. blue for legal, red for staff, etc. Since this item was on the 8/15/2024 agenda, but the PPAC didn't reach quorum, the dates were off by one month.

Ray had concerns about moving 5500 through the system since it contained a lot of changes, and the academic year is already underway. Chapter Lead Nohemy Ornelas felt that it was important to move the currently revised 5500 through the system as it had completed the process except for PPAC hearing any final input from the Academic Senate. She offered support to the campuses in getting the word out and posting to websites. It was confirmed that 5500 would become effective upon final approval by the Board of Trustees. After some discussion, Kristina made a motion to move 5500 through the process since there was no further feedback from Academic Senate. Jessy seconded the motion, which was approved by a majority vote with Ray voting no.

E. New Chapter Lead Recommendations

1. Level 1 (information only)
 - i. 2015 Student Trustees
 - ii. 2355 Decorum
 - iii. 2430 Delegation of Authority to the Chancellor
 - iv. 2715 Code of Ethics-Standards of Practice
 - v. 2731 Trustee Emeritus-Emerita-Emeriti

Committee members reviewed each item on this list. Carmen made a motion to approve the Level 1 review, which Kristina seconded. The motion passed with a unanimous vote.

2. Level 2 (minor review)
 - i. 5030 Fees
 - ii. 6925 Refreshments or Meals Served at Meetings and District Events
 - iii. Family of IT P&Ps
 - a. 3725 Information and Communications Technology Accessibility
 - b. 3726 Information Security: Data Classification
 - c. 3727 Information Security: Access Control
 - d. 3728 Information Security: Physical Security
 - e. 3729 Information Security: Logging and Monitoring
 - f. 3730 Information Security: Remote Access
 - g. 3731 Information Security: Internally Developed Systems Change Control
 - h. 3732 Information Security: Incident Response
 - i. 3733 Information Security: Secure Operations
 - j. 3734 Information Security: Network Security
 - k. 3735 Information Security: Disaster Recovery
 - l. 3736 Information Security: Cloud Storage
 - m. 3737 Information Security: Payment Card Industry Requirements

Committee members reviewed each item on this list. Luke Bixler spoke about the new family of IT security items. Kelly made a motion to approve the Level 2 review, which Carmen seconded. The motion passed with a unanimous vote.

3. Level 3 (extensive review)

i. 4300 Field Trips & Excursions

Kristina made a motion to approve 4300 for a Level 3 review, which Carmen seconded. The motion passed with a unanimous vote.

F. Adjournment & Next Meeting

Some members mentioned issues with accessing Govenda and advised they had not been added in Teams. Kelly will make sure that everyone has the access they need. For Govenda, no information was lost, as it is the same material distributed via email prior to the meeting.

The next PPAC meeting is scheduled for Thursday, October 17, 2024, at 2:30 p.m. The meeting adjourned at around 4:25 p.m.

QUORUM: Definition of Quorum is established by Chancellor's Council. Committees cannot vote or make decisions unless they have met quorum, but in order to encourage participation, committee members can provide a designee or a proxy if they are not able to attend.

yes	1) 50% + one of appointed voting members (not 50% of members plus vacancies).		
yes	2) One faculty member from each campus		
yes	3) Two persons from each site (CHC, SBVC, DSO)		
yes	4) Three of four constituent groups represented (faculty, classified, student, management)		
1	Latino Faculty, Staff, & Administrators Association	Carmen Rodriguez	<i>present</i>
2	CSEA (appointed by CSEA President)	Ernest Guillen	<i>present</i>
3	Faculty, CHC (appointed by Academic Senate President)	Chis Olivera	<i>present</i>
4	Management Association	Christopher Crew	
5	ASG President or designee, SBVC	Dyami Ruiz-Martinez	
6	Police Officer's Association	James Quigley	
7	CTA (appointed by CTA)	Jeff Demsky	
8	Faculty, SBVC (appointed by Academic Senate President)	Jessy Lemieux	<i>present</i>
9	Executive Vice Chancellor, Co-Chair	Jose Torres	<i>present</i>
10	Classified, CHC (appointed by Classified Senate President)	Karen Peterson	<i>present</i>
11	Management, CHC (appointed by college president)	Keith Wurtz	
12	Confidential Group	Kelly Goodrich	<i>present</i>
13	Vice Chancellor, Human Resources & Police Services	Kristina Hannon	<i>present</i>
14	Classified, SBVC (appointed by Classified Senate President)	Nathan Yearyeen	<i>present</i>
15	Management, SBVC (appointed by college president)	Ray Carlos	<i>present</i>
16	Asian Pacific Islanders Association	Rejoice Chavira	
17	ASG President or designee, CHC	Vacant	
18	Black Faculty & Staff Association	Veada Benjamin	<i>present</i>

BP 5075 Course Adds, Drops, and Withdrawals



10+1 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

- > Per discussion at 5/13/2024 PPAC requesting Chapter Lead clarification of "Intervention Program" and the impact of the "FW" grade.
- > Minor Clerical Edit

Level 3 Review Schedule

- 03/18/2024 ♦ Recommendation Received
- 04/08/2024 ♦ PPAC Approves Review Level
- 04/09/2024 ♦ Level 2 to Constituents and AS for Feedback
- 04/17/2024 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input
- 05/13/2024 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3
- 05/15/2024 ♦ AS Reviews Level 3 for Final Input
- 10/17/2024 ♦ PPAC Reviews Final AS Input
- 11/14/2024 ♦ BOT 1st Read
- 12/13/2024 ♦ BOT Final Approval

Begin Recommendation for BP 5075 Course Adds, Drops, and Withdrawals

(Replaces current SBCCD-BP-5080)

Students may add or drop courses in accordance with the procedures recommended by the Chancellor.

References:

Title 5 Sections 55024, [and 58004](#) [and 58509](#)

End Recommendation for BP 5075 Course Adds, Drops, and Withdrawals

AP

5075 Course Adds, Drops, and Withdrawals



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

- > Per discussion at 5/13/2024 PPAC requesting Chapter Lead clarification of "Intervention Program" and the impact of the "FW" grade.
- > Legal Update 42: The Service updated this procedure to align with updated Title 5 regulations.

Begin Recommendation for AP 5075 Course Adds, Drops, and Withdrawals

(Replaces current SBCCD AP 5080)

The District may allow students to add and drop courses pursuant to policy.

Adding Courses

- A. Students may add courses during the first two weeks for a full-term course, or the first 10% of a ~~short-term~~ short-term course, only with the instructor's permission, contingent upon:
 1. the course still having available space
 2. the instructor's judgment regarding pedagogical and safety issues
- B. After the add period concludes,
 1. ~~students~~ Students may add a course only with the instructor's permission and through a petition approved by the Director of Admissions & Records or designee.
 2. ~~students~~ Students not officially registered in a course shall not be permitted to attend that course.

Withdrawal/Military Withdrawal

- A. **Withdrawal Prior to Census (20% of instruction)**
Students who withdraw or are withdrawn from weekly census sections prior to census (or 20% of the instructional time frame for all other section accounting methods) shall have no notation made to the permanent record.
- B. **Withdrawal 20% - 60% of Instruction**
Students who withdraw or are withdrawn from weekly census sections on or after census (or 20% of the instructional time frame for all other section accounting methods) and through the end of the eleventh week (or 60% of the instructional time frame) shall have a "W" posted to the permanent record.
- C. **Withdrawal After 60% of Instruction**
The permanent record of students who remain in class beyond the eleventh week of the term in a weekly census section (or 60% of the instructional time frame for all other section accounting methods) must reflect a grade symbol other than "W".
- D. **Extenuating Circumstances**
Students who withdraw from weekly census sections after the eleventh week of the term (or 60% of the instructional time frame for all other sections accounting methods) may, in the case of extenuating circumstances, be assigned the "W". Such cases will require verification and will be handled by the appropriate college official in consultation with the instructor(s). Extenuating circumstances are defined as illness, accident, unforeseen job shift change, job assignment outside of the attendance area and extreme weather conditions.
- E. **Military Withdrawal**
An "MW" (Military Withdrawal) shall be assigned for students who are members of an active or reserve United States military service who receive orders compelling a withdrawal from courses. Upon verification of such orders, the symbol may be assigned at any time. The "MW" shall not be counted in progress probation and dismissal calculations.

Intervention Program



5075 Course Adds, Drops, and Withdrawals



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

A student will be permitted to withdraw from a class and receive a "W" no more than three times. In the case of multiple withdrawals, the District offers the following intervention program:

- A. Students may be permitted to enroll in a class after having received the maximum authorized number of "W" symbols as long as the students will receive a grade or a non-evaluative symbol other than a "W" upon completion of the course, if the District policy permits additional withdrawals for which it does not receive apportionment and the official designated in the District's policy approves such withdrawal after a review of a petition submitted by the student.
- B. An excused withdrawal ("EW") will not be counted toward the permitted number of withdrawals or counted as an enrollment attempt, nor will it be counted in progress probation and dismissal calculations. An excused withdrawal occurs when a student withdraws from a course due to an extraordinary condition under Title 5 Section 58509. In no case shall an excused withdrawal result in a student being assigned an "FW" grade,

Instructor Initiated Drops Prior to Census

- A. For purpose of census collection, instructors shall drop students due to inactive enrollment not later than the end of the last business day before the census day for all students who have:
1. Been identified as a no show
 2. Students who are no longer attending the course

Instructors shall clear their rolls of inactive students no later than the day prior to census.

"Inactive students" include:

- Students identified as no-shows,
- Students who officially withdraw,
- Students who are no longer participating in the courses ~~and~~ are therefore dropped by the instructor.

Course Repetition

The District will comply with Title 5 regulations regarding course repetition and withdrawals.

References:

Title 5 Sections 55024, [and 58004](#), [and 58509](#)

End Recommendation for AP 5075 Course Adds, Drops, and Withdrawals



4300 Field Trips and Excursions



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

- > Legal Update 43: The Service updated this policy to remove the out-of-state travel ban pursuant to changes in the Government Code.
- > 3/11/2024 PPAC requested additional review.

Level 3 Review Schedule

- 05/13/2024 ♦ Recommendation Received
- 09/19/2024 ♦ PPAC Approves Review Level
- 09/20/2024 ♦ Level 2 to Constituents and AS for Feedback
- 10/02/2024 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input
- 10/17/2024 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3
- 11/06/2024 ♦ AS Reviews Level 3 for Final Input
- 11/21/2024 ♦ PPAC Reviews Final AS Input
- 12/13/2024 ♦ BOT 1st Read
- 01/09/2025 ♦ BOT Final Approval

Begin Recommendation for BP 4300 Field Trips and Excursions

(Replaces current SBCCD BP 4300)

The Chancellor shall establish procedures that regulate the use of District funds for student travel and attendance at conferences and other activities that are performed as a class assignment or co-curricular activity.

The District may pay for expenses of students participating in a field trip or excursion with auxiliary, grant or categorical program funds if the funds are used consistently with the funding source. The expenses of instructors, chaperones, and other personnel traveling with students may be paid from District funds.

Students and staff shall at all times adhere to the standards of conduct applicable to conduct on campus.

Reference:

Government Code Section 11139.8; Title 5 Section 55220

End Recommendation for BP 4300 Field Trips and Excursions

AP 4300 Field Trips and Excursions



10+1 ♦ CCLC | Legally Advised ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

> Legal Update 43: The Service updated this policy to remove the out-of-state travel ban pursuant to changes in the Government Code.

> 3/11/2024 PPAC requested additional review.

Begin Recommendation for AP 4300 Field Trips and Excursions

(Replaces current SBCCD AP 4300)

The District may ~~conduct~~ provide field trips and excursions in connection with courses of instruction or college-related social, educational, cultural, athletic or musical activities to and from places in California, or any other state, the District of Columbia, or a foreign country for students.

Field trips or excursions must be approved in advance by the appropriate administrator and be supervised by an approved faculty member or other district employee. A field trip or excursion generally falls into one of the following categories:

- Required trips are local and are designed as an integral part of the class and listed in the syllabus. Trips scheduled during class time are considered part of normal class attendance. For example, an administration of justice class may visit a local police department; an art class may meet at a gallery exhibit.
- Required trips or excursions take place outside of class time and are described in the syllabus and catalog description, for example, a field laboratory experience in biology or geology.
- Optional field trips or excursions are not required. Students who cannot attend the field trip/excursion incur no academic penalty and are provided alternative assignments. These are trips which take place outside of class when the dates and times are agreed to by consent of students enrolled and the instructor.
- Other field trips or excursions as approved and deemed beneficial to students by providing educational/cultural enrichment.

~~The District shall engage instructors, supervisors, and other personnel, except classified employees, as may be necessary for such excursions or field trips who desire to contribute their services over and above the normal period for which they are employed by the District.~~

~~The District shall, at the discretion of the Chancellor or designee, transport students, instructors, supervisors or other personnel by use of District equipment, contract to provide transportation, or arrange transportation by the use of other equipment.~~

~~When District equipment is used, the District shall obtain liability insurance, and if travel is to and from a foreign country, the liability insurance shall be secured from a carrier licensed to transact insurance business in the foreign country.~~

The District may provide supervision of students involved in field trips or excursions by academic employees of the district.

- Authorization

Any curricular activity, field trip, or excursion involving student participation at an off-campus location other than the usual meeting location of the class requires authorization by the appropriate administrator prior to the commencement of the activity. ~~Any overnight trip, in excess of \$500 total cost, or any trip involving cost for student meals must be approved by the College President.~~

- Expenditure of Funds

Travel requests shall be made in accordance with the District's travel request and approval processes. Please reference AP 7400 regarding those processes.

The approval request shall include any anticipated expenditure of funds for lodging, food, transportation, or activity fees. The District may pay expenses of instructors, chaperones, and other personnel participating in a field trip or excursion. Payment shall be by way of itemized reimbursement in a form prescribed by the Chancellor or designee. The District may pay for expenses of students participating

AP 4300 Field Trips and Excursions



10+1 ♦ CCLC | Legally Advised ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

in a field trip or excursion with auxiliary, grant, or categorical program funds if the funds are used consistently with the funding source. Usual and customary travel expenses for authorized District personnel may be provided. Expenditures shall be approved only after an approved trip request is submitted with a Purchase Requisition, ~~and if that amount has been budgeted and sufficient funds remain in the account to cover the claim.~~

No student shall be prevented from making a field trip or excursion ~~which is integral to the completion of a course~~ because of lack of sufficient funds. ~~The District shall coordinate efforts of community services groups to provide funds for students in need of them.~~

- Accountability

When transportation is provided, the individual responsible for the field trip shall leave a list of all participants, including students and employees who are on the trip, where it can easily be found in case of an emergency.

- Transportation

1. Students shall be transported in commercially procured transportation whenever possible. Van size is limited to no larger than the 10-passenger size as defined in California Vehicle Code. Commercial bus lines must have on file a certificate of insurance with the Office of Risk Management prior to the commencement of the trip naming the District as "additional insured." Transportation requiring rental of van(s) or bus(s) must have a contract. The contract must be signed by a Board approved authorized signer fourteen (14) calendar days prior to the day of travel. (See AP 6340 titled Contracts)
2. If rented vans or automobiles are used, each driver must be a District employee, be registered on the Approved Drivers' List and have the appropriate class of driver's license to operate the intended vehicle. No student is authorized to drive any vehicle on District business. District insurance provides primary liability coverage for rented vehicles and secondary coverage for property damage coverage.
3. If funds are not available for transportation, students may provide their own transportation. In such cases students should be asked to meet at the site at a specified time. Car caravans are not appropriate.
4. No employee shall transport any student in ~~his/her~~ their private vehicle on college business.

- Liability

When District equipment is used, the District shall obtain liability insurance, and if travel is to and from a foreign country, the liability insurance shall be secured from a carrier licensed to transact insurance business in the foreign country. All persons making a field trip or excursion shall be deemed to have waived all claims against the District for injury, accident, illness, or death occurring during or by reason of the field trip or excursion. All adults taking such trips and all parents or guardians of minor students shall sign a statement waiving such claims.

Reference:

[Government Code Section 11139.8](#) - Title 5 Section 55220

End Recommendation for AP 4300 Field Trips and Excursions

BP**3725 Information and Communications
Technology Accessibility & ~~Acceptable Use~~**

Non 10+1 ♦ CCLC | Good Practice/Optional ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

- > Chapter Lead review of IT security
- > Legal Update 38: The Service updated this policy to add optional language to highlight diversity, equity, and inclusion issues. (2022-23 carryover)
- > Moving language from below legal reference into the body of the AP.

Level 2 Review Schedule

- 08/30/2024 ♦ Recommendation Received
- 09/19/2024 ♦ PPAC Approves Review Level
- 09/20/2024 ♦ Level 2 to Constituents and AS for Feedback
- 10/02/2024 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input
- 10/17/2024 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3
- 11/14/2024 ♦ BOT 1st Read
- 12/13/2024 ♦ BOT Final Approval

Begin Recommendation for BP 3725 Information and Communications Technology Accessibility & Acceptable Use

The governing board shall ensure equal access to instructional materials and information and communication technology (ICT) for all and particularly for individuals with disabilities, in a timely manner.

As it relates to equally effective alternative access to instructional materials and ICT, timely manner means that the individual with a disability receives access to the instructional materials or ICT at the same time as an individual without a disability.

The Chancellor shall establish administrative procedures to comply with the requirements specified in Section 508 of the Rehabilitation Act and its implementing regulations. The Chancellor shall also establish administrative procedures to enable the District to lawfully manage its use of third-party social media platforms and communication to the general public via third-party social media platforms.

Also see BP/AP 3410 Nondiscrimination, BP/AP 3720 Computer and Network Use, AP 3725 Accessibility and Acceptable Use, BP/AP 5140 Student Accessibility Services, and AP 6365 Contracts – Accessibility of Information Technology.

References:

Government Code Sections 7405, 11135, and 11546.7;
Section 504, Rehabilitation Act of 1973 (29 U.S. Code Section 701);
Section 508, Rehabilitation Act of 1973 (Federal Electronic and Information Technology) (29 U.S. Code Section 794d);
36 Code of Federal Regulations Parts 1194.1 et seq. Also see BP/AP 3410 Nondiscrimination, BP/AP 3720 Computer and Network Use, AP 3725 Accessibility and Acceptable Use, BP/AP 5140 Disabled Student Programs and Services, and AP 6365 Contracts – Accessibility of Information Technology.

End Recommendation for BP 3725 Information and Communications Technology Accessibility & Acceptable Use

AP

3725 Information and Communications Technology Accessibility & ~~Acceptable Use~~



Non 10+1 ♦ CCLC | Good Practice/Optional ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

- > Chapter Lead review of IT security
- > Legal Update 42: The Service updated this procedure to align with updated Title 5 regulations.
- > Legal Update 38: The Service updated this procedure to add optional language to highlight diversity, equity, and inclusion issues. (2022-23 carryover)

Begin Recommendation for AP 3725 Information and Communications Technology Accessibility & Acceptable Use

DEFINITIONS

The following definitions apply to this procedure:

Accessible: An individual with a disability is afforded the opportunity to acquire the same information, engage in the same interactions, and enjoy the same services as a person without a disability in an equally effective and equally integrated manner, with substantially equivalent ease of use. [The person with a disability must be able to obtain the information as fully, equally, and independently as a person without a disability. Although this might not result in identical ease of use compared to that of persons without disabilities, it still must ensure equal opportunity to the educational benefits and opportunities afforded by the technology and equal treatment in the use of such technology.](#)

Equally Effective: Alternative access for individuals with disabilities to instructional materials and information and communication technology that (1) is timely, (2) is accurate in translation, (3) is delivered in a manner and medium appropriate to the disability of the individual, and (4) affords the individual with a disability the opportunity to obtain the information as fully, equally and independently as a person without a disability with substantially equivalent ease of use. Note, such alternative(s) are not required to produce the identical result or level of achievement, but must afford individuals with disabilities equal opportunity to obtain the same result, to gain the same benefit, or to reach the same level of achievement in the most integrated setting appropriate to the person's needs.

Individual with a Disability: An individual who has one or more physical or mental impairments that substantially limit one or more major life activities.

Information and Communication Technology (ICT): Encompasses electronic and information technology covered by Section 508 of the Rehabilitation Act of 1973, as well as telecommunications products, interconnected Voice over Internet Protocol (VoIP) products, and Customer Premises Equipment (CPE) covered by Section 255. Examples of ICT include computers, information kiosks and transaction machines, telecommunications equipment, multifunction office machines, software, Web sites, and electronic documents.

Web Page Standards: The San Bernardino Community College District (District) is committed to providing information via the Internet and Web pages that is reasonably accessible to all students and interested parties regardless of physical ability. The District will establish and maintain Web Page Accessibility Standards. A Web Standards committee will be established and be responsible for establishing and documenting the Web Page Accessibility Standards ("**Standards**") for the district and the colleges. The approved Standards will be available electronically on the district and college web sites. The information will be available in alternative formats as needed. Web Page Accessibility Standards compliance is inclusive of all web pages for colleges, departments, and the District. It is encouraged, but not required, to have individual faculty, staff and student web pages comply with the accessibility standards. Mandatory compliance, however, is required for any faculty, staff or student web page that contains information necessary for students to complete required course work; these pages must comply with the accessibility standards or be made available to students in an alternative format when requested, consistent with ADA regulations concerning reasonable accommodation.

AP

3725 Information and Communications Technology Accessibility & ~~Acceptable Use~~



Non 10+1 ♦ CCLC | Good Practice/Optional ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Instructional Materials: Includes electronic instructional materials, such as, syllabi, textbooks, presentations and handouts delivered within CCC's learning management system, via email or via another electronic means for face-to-face classes as well as e-learning courses. It also includes electronic instructional activities such as instructional videos, online collaborative writing, Web conferencing, blogging, and any other instructional materials as technology evolves.

Timely: As it relates to equally effective alternative access to instructional materials and ICT, timely means that the individual with a disability receives access to the instructional materials or ICT at the same time as an individual without a disability.

ICT AND INSTRUCTIONAL MATERIAL ACCESSIBILITY STANDARD STATEMENT

The District is committed to ensuring equal access to instructional materials and ICT for all, and particularly for individuals with disabilities in a timely manner. In accordance with Government Code Sections 7405, 11135, and 11546.7, and best practices, the District will comply with the accessibility requirements of Section 508 of the Federal Rehabilitation Act of 1973 by:

- Developing, purchasing or acquiring, to the extent feasible, instructional materials and ICT products that are accessible to individuals with disabilities;
- Using and maintaining instructional materials and ICT that is consistent with this Standard; and
- Promoting awareness of this Standard to all relevant parties, particularly those in roles that are responsible for creating, selecting, or maintaining electronic content and applications.

Ensuring equal access to equally effective instructional materials and ICT is the responsibility of all District administrators, faculty, and staff.

References:

Government Code Sections 7405, 11135, and 11546.7;

Section 504, Rehabilitation Act of 1973 (29 U.S. Code Section 701);

Section 508, Rehabilitation Act of 1973 (Federal Electronic and Information Technology) (29 U.S. Code Section 794d);

36 Code of Federal Regulations Parts 1194.1 et seq.

End Recommendation for AP 3725 Information and Communications Technology Accessibility & Acceptable Use



3726 Information Security Data Classification



Non 10+2 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Reasons for Review

> New AP resulting from Chapter Lead review of IT security

Level 2 Review Schedule

08/31/24 ♦ Estimated Receipt of Recommendation

09/19/24 ♦ PPAC Approves Review Level

09/20/24 ♦ Level 2 to Constituents and AS for Feedback

10/02/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

10/17/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

11/14/24 ♦ BOT 1st Read

12/13/24 ♦ BOT Final Approval

Begin Recommendation for AP 3726 Information Security Data Classification

1. PURPOSE AND SCOPE

The purpose of this Administrative Procedure is to provide information security requirements for the ownership, classification, and protection of the San Bernardino Community College District (SBCCD) information assets.

An information asset is a definable piece of information, regardless of format, that is recognized as valuable to the organization. Classifying information is at the core of an information security program because it specifies how information, based on its sensitivity and value, will be protected from unauthorized disclosure, use, modification or deletion.

This is one of a series of Information Security Administrative Procedures maintained by the District's Technology & Educational Support Services department designed to protect SBCCD information systems.

2. RESPONSIBILITIES

The following roles and responsibilities are established for carrying out this data regulation:

- a. **Executive sponsors** are senior college officials who have planning responsibility and accountability for major administrative data systems (e.g. student, human resources, financial, research, etc.) within their functional areas. By understanding the planning needs of the institution, they are able to anticipate how data will be used to meet institutional needs.
- b. **Data stewards** are appointed by the executive sponsors to implement established data policies and general administrative data security policies for their functional areas. Data stewards are responsible for safeguarding the data from unauthorized access and abuse through established security and authorization procedures and educational programs. They authorize the use of data within their functional areas and monitor this use to verify appropriate data access. They support access by providing appropriate documentation and training to support data users. Identified data stewards, ~~having served informally at the institution, will be identified and~~ will serve on existing change management committees and the District and/or Campus information security team as appropriate.
- c. **Data owners** are employees who most often report to data stewards, whose duties provide them with an intricate understanding of the data in their area. They work with the data stewards to establish procedures for the responsible management of data, including data entry, auditing, and reporting. Some data owners may work in a



3726 Information Security Data Classification



Non 10+2 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

technology unit outside of the functional unit but have responsibilities such as security and access as decided by the stewards. Technical data owners may also be responsible for implementing backup and retention plans or ensuring proper performance of database software and hardware. Identified data owners ~~administrators, having served informally at the institution,~~ will be identified and called upon for their subject matter expertise.

3. DATA CLASSIFICATION

Users of SBCCD systems need to understand the importance of securely handling the information they are able to access and the standards that have been created to ensure data protection. For the purposes of this Administrative Procedure, data includes both electronic and paper.

Specific protection requirements are mandated for certain types of data, such as credit card information, personally identifiable information, or financial data. Where information is entrusted to us by our students, employees, or business partners, their expectations for secure handling must be met. Consistent use of this Administrative Procedure will help to ensure that we maintain adequate data protection.

a. Classification of Data Assets

SBCCD classifies information regardless of the medium (electronic or paper) according to its sensitivity and the potential impact of disclosure.

In general, information is disclosed to employees or others when there is a business need to know. The information must be consistently handled according to its requirements for confidentiality and disclosure.

Data Owners, defined below, are responsible for determining the appropriate classification level for data for which they are responsible or for the same information maintained on paper documents.

If the classification level is set too high, the cost of protection will be excessive in relation to the value or sensitivity of the data. If it is set too low, the risk of compromise could be increased. Downgrading to a lower classification at a future date is appropriate should conditions warrant.

b. Data Ownership

Every business application must have one or more designated Data Owners. The Data Owner is the person responsible for (or dependent upon) the business process associated with an information asset. The Data Owner is knowledgeable about how the information is acquired, transmitted, stored, deleted, or otherwise processed and is, therefore, best suited to make decisions about the information on behalf of the organization.

The Data Owner is ultimately responsible for security decisions regarding the data. The Data Owner will work with the appropriate college Technology Departments or District Information Technology (IT) department to ensure that minimum-security standards are met. The District IT and college Technology departments will provide appropriate security technology solutions (such as system or application security controls or encryption methods) based on classification level.

If the Data Owner has chosen to outsource the processing or storage of information at a location outside of SBCCD's control, such as on a cloud-based service, the Data Owner retains full accountability for the security of the



3726 Information Security Data Classification



Non 10+2 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

information. Security controls that are required to be performed by the third-party service provider must be detailed in the contract with that provider and monitored by the Data Owner.

The Data Owner's responsibilities include:

- i. Classifying data for which they are responsible. This includes determining the level of confidentiality that should be assigned to information, which will dictate its level of protection;
- ii. Working with IT to select security controls that are appropriate to the level of sensitivity, value or confidentiality of the application or data it processes;
- iii. Ensuring that third parties to whom data has been entrusted meet SBCCD security requirements;
- iv. Establishing and maintaining response plans that identify actions to be taken for their area of control, such as Security Incident Response processes and defined Business Continuity Plans; and
- v. Depending on location, provide District and/or College IT management with administrative access in order to maintain continuity of access to systems and services.

c. Data Classification Categories

Information that is owned, used, created or maintained by SBCCD must be classified into one of three categories:

- i. **Public**
Data classified as Public is suitable for routine public disclosure and use. Security at this level is the minimum required by SBCCD to protect the integrity and availability of this data. Examples of this type of data include, but are not limited to, data routinely distributed to the public, such as publicly accessible web pages, marketing materials, and press statements.
- ii. **Internal**
Internal data is information about SBCCD or internal processes that must be guarded due to proprietary or business considerations, but which is not personally identifiable or otherwise considered confidential. This classification may apply even if there are no regulatory or contractual requirements for its protection.

Data in this category is generally available to employees, contractors, students, or business associates but is not routinely distributed outside SBCCD. Some Internal data may be limited to individuals who have a legitimate business purpose for accessing the data, and not be available to everyone. Examples of Internal data may include:
 - SBCCD procedures and manuals
 - Organization charts
 - Data that is on the internal Intranet (SharePoint), but has not been approved for external communication
 - Software application lists or project reports
 - Building or facility floor plans or equipment locations
- iii. **Restricted**
 - Restricted data is information that is sensitive in nature and may be proprietary, personally identifiable, or otherwise sensitive. Unauthorized compromise or disclosure of the information would likely cause serious financial, legal, or reputation damage to SBCCD or result in embarrassment or difficulty for SBCCD, its employees, or students. Restricted data may be protected by statutes, regulations, or contractual requirements. Disclosure is limited to those within SBCCD on a "need-to-know" basis only.



3726 Information Security Data Classification



Non 10+2 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Disclosure to parties outside of SBCCD must be authorized by appropriate management and covered by a binding confidentiality or non-disclosure agreement. Examples of Restricted data include personally identifiable (as defined below) information of our employees, contractors, or students.

- Human Resources, employee, or payroll records.
- Student data.
- Specialized audit reports or results.
- System and network configuration details, including diagrams, passwords, programs, or other IT-specific documentation.
- Intellectual property.
- Health records.
- Legal documents.

For purposes of this Administrative Procedure, the term “personally identifiable information” means an individual’s first name and last name or first initial and last name in combination with any one or more items of personal information, such as social security number or other identity verification number, driver’s license number or state-issued identification card number, student and/or employee ID numbers, financial account number, credit or debit card number, date or place of birth, and gender or gender identity; provided, however, that “personally identifiable information” shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

d. Minimum Classification

All information should be assumed Internal unless classified otherwise.

e. Classification Flow Chart

The Classification Flow Chart is intended to assist a Data Owner, document creator, or user to assist in quickly determining the classification of a data element or document.

f. Information Access

The Data Owner makes access decisions regarding information they are responsible for and must be consulted when access decisions are to be made, extended, or modified.

g. Periodic Review

The Data Owner, at least every two years, or when necessary, based on business need, must review information asset classifications. Review records must be maintained by Data Owners documenting the review processes that took place.

References:

Civil Code 1798.29

Family Education Rights and Privacy Act (FERPA)

Social Security Number Policy

Health Insurance Portability and Accountability Act (HIPAA)

End Recommendation for AP 3726 Information Security Data Classification



3727 Information Security Access Control



Non 10+3 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Reasons for Review

> New AP resulting from Chapter Lead review of IT security

Level 2 Review Schedule

08/31/24 ♦ Estimated Receipt of Recommendation

09/19/24 ♦ PPAC Approves Review Level

09/20/24 ♦ Level 2 to Constituents and AS for Feedback

10/02/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

10/17/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

11/14/24 ♦ BOT 1st Read

12/13/24 ♦ BOT Final Approval

Begin Recommendation for AP 3727 Information Security Access Control

1. PURPOSE AND SCOPE

The objective of this Administrative Procedure is to provide internal controls for access to the San Bernardino Community College District (SBCCD) sites, information, and applications. This administrative procedure (AP) is part of a series of APs governing the secure use and access of Information Technology Systems and Services.

Access controls may be physical (such as locks and badges), administrative (such as the AP to safeguard passwords), or technical (protections enforced by software settings or privileges). These controls are designed to allow or restrict the ability to view, update, or delete information within the SBCCD networks and systems or paper documents.

a. Applicability of Assets

The scope of this AP includes all electronic assets owned or leased by SBCCD. Assets may include but are not limited to:

- i. Desktop and Laptop computers
- ii. Mobile Devices
- iii. Servers
- iv. Network Infrastructure
- v. Electronic Media
- vi. Mobile Computing Devices

b. Applicability

This AP applies to all SBCCD employees, including consultants, contractors, temporary employees, and volunteers.

c. Applicability to External Parties

This AP applies to all external parties, including but not limited to SBCCD business partners, vendors, suppliers, outsourced service providers, and other third-party entities with access to SBCCD networks and system resources.



3727 Information Security Access Control



Non 10+3 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

2. ACCESS CONTROL

a. Access Control Principles

There are three basic access control principles at the SBCCD:

- i. All information is made available only to those with a legitimate “need-to know”. Access is provided on this basis, guided by job requirements and data classification.
- ii. Access controls for SBCCD systems will be provided in a manner that promotes individual accountability. Audit trails and monitoring of access establishes accountability and allows for follow-up of access violations and security breaches.
- iii. Users with the highest levels of privilege on a computer system will be restricted to the least privileges necessary to perform the job.

b. Authentication to District Systems

Authentication is the verification of a user's identity. All individuals require identification (ID) prior to gaining access to secured SBCCD facilities or systems such as server rooms, cash handling rooms and other areas where security is in the interest of the District.

Internal (SBCCD personnel) and external (non-personnel) users must provide a valid and unique user ID in order to authenticate to the network. In addition to a unique ID, the authentication method must include at least one of the following:

- i. A password or passphrase;
- ii. Token device or smart card; or
- iii. Biometric.

If the new user is a contractor or non-employee, the user ID will be identifiable as such by its naming convention.

Group, shared, or generic accounts do not provide accountability and are not to be used for network or application authentication. Some exceptions may apply to this requirement, such as a system account that is required for server or network processing or an account that is to be used by departments that would be used as an official communications account.

Physical access to secured facilities requires that SBCCD users possess appropriate access badges or credentials in order to enter all sites. Some areas, such as computer rooms, may require additional access levels, cards or keys. Refer to the AP-3728: Information Security - Physical Security for specific information.

c. Authorization to Applications

Addition, modification, and deletion of user IDs and other credentials must be controlled. Data Owners (or their designees) have the responsibility for making security decisions about applications that process data for which they are responsible.

Assuming the role of the Data Owner may require:

- i. Approving and re-certifying access by users to systems or data they control, or
- ii. Classifying data belonging to the application system they manage (determining the level of confidentiality or classification that should be assigned to an application's data, which will dictate its level of protection).

Access to certain functions may be provisioned automatically based on job position. Otherwise, the appropriate IT department, as authorized by Data Owners, must approve all new accounts. Each request for access must contain written and/or electronic evidence of approval by the Data Owner, District IT, or college Technology Services. Extension authorizations for contractor accounts must be applied by District IT or college Technology Services to provide an audit trail.



3727 Information Security Access Control



Non 10+3 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Access requests must specify access either explicitly or via a “role” that has been mapped to the required access. Outside of initial standard network access provided based on the job position of the users, access to additional applications or capabilities is discretionary and must be both requested and approved by the Data Owner. For additional access, users should submit an access request.

Departmental security administrators, as defined below, may set up access for some applications. District IT will pass the request on to the relevant team to set up access.

Remote access is not automatically provided to all users and must be requested and approved. Refer to the AP-3730: Remote Access for additional information.

The District IT or college Technology Services departments will maintain for a minimum of six (6) years logs or other documentation of all access request approvals, user account creations, modifications, and deletions.

3. SECURITY ADMINISTRATORS

The appropriate District IT or college Technology Services department is responsible for administering overall system access within SBCCD, and so may request information from appropriate managers or administrators, such as who has access to their applications, and the procedures that they have put in place to provision them.

Some users (in District IT, college Technology departments, or business departments) may have a higher level of access privilege in order to administer systems or applications. They may have the ability to add, modify, or delete other users for the applications they control. To maintain system access to District-owned or developed software, District IT or the college Technology departments shall be provided an Administrative Account that will be used for recovery and auditing elevated access periodically.

Systems administrators and network technicians, under management supervision, have a responsibility to maintain appropriate access controls for the applications they maintain in order to protect information from unauthorized access. The number of administrators should be tightly controlled and limited to as few as necessary.

Security administrators should have their accounts set up with the proper access and log in with their accounts to conduct any privileged access. A log should be kept to review any privilege access and changes, and a report should be delivered and reviewed periodically each year by the Security Director and college Technology Directors. Security administrators should only use their privileged accounts to carry out administrative tasks that require privileged access. A non-privileged account should be used to perform routine tasks.

4. PASSWORDS

Users of the SBCCD computer systems will be provided with one or more unique accounts and associated passwords.

Users are accountable for work performed with the account(s) issued to them and are responsible for the confidentiality of their passwords. Passwords must be difficult to guess and kept private, and users must not disclose their passwords to anyone.

The following rules apply to password composition:

- i. Must not be left blank when a new account is created. New passwords must not be the same for all users;
- ii. Must have a minimum length of eight (8) characters;
- iii. Must contain both numeric, special, and alphabetic characters /be alphanumeric and contain one upper case letter;
- iv. New passwords must be changed immediately upon first use;



3727 Information Security Access Control



Non 10+3 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

- v. New passwords must not be the same as the four previously used passwords or used within a one-year period, and Passwords must be changed at least every 90 days (some passwords within IT are exempt from this requirement).

If a user requests a password reset via phone, email, web, or other non-face-to-face method,

Administrators who can reset passwords must verify the user's identity, such as by providing personal information, before changing the password.

5. ACCOUNT LOCKOUT

Accounts will be locked after six (6) invalid login attempts. Once an account is locked, an authorized District IT or college Technology department staff, automated recovery system or authorized student services representative is required to reset the account after the user's identity has been verified. The lockout duration will be set to a minimum of 30 minutes or until an administrator enables the account.

Faculty classroom/lab workstations have a session idle time of 30 minutes after which the session will be locked. With the exception of some system accounts, all other user accounts have a session idle time of 15 minutes, after which the session will be locked.

6. EMERGENCY ACCOUNTS

An Emergency Account / User ID will be established when access is needed to diagnose or correct a problem. The request to create the Emergency ID must be made through the appropriate college Technology Director, District IT manager, or administrator. The ID will be enabled only for a 24-hour period unless a specific time period is requested.

Upon completion of the work, the requestor must inform the appropriate college Technology Director or District IT manager so that the ID can be disabled.

7. TERMINATION OF ACCESS PRIVILEGES

Supervisors are responsible for notifying Human Resources if personnel will be leaving SBCCD or, in some cases, those who are placed on administrative or extended leave. HR will contact District IT and other Security Administrators as required so that access may be removed. Access must be disabled immediately upon notification or at the end of the last day of work.

8. REVIEW OF ACCESS

A bi-annual audit of computer resource authorizations to confirm that access privileges remain appropriate will be conducted by appropriate IT staff. After an additional sixty (60) days, inactive accounts will be purged. These requirements may not apply to certain specialized accounts (e.g., Windows Administrator, root). Student accounts maybe be exempt and regulated by the District established provisioning process.

District IT and/or college Technology departments, working with HR, may periodically validate employment and may immediately suspend users who are on leave of absence or extended disability. At least annually, IT will request that Data Owners verify continued access by users with access to their applications. District IT, college Technology departments, and/or external auditors will periodically review security administration procedures for specific applications and may employ monitoring tools to audit and verify access controls.

9. PAYMENT CARD INDUSTRY REQUIREMENTS

Refer to AP 3737 Information Security - Payment Card Industry Requirements (PCI).



3727 Information Security Access Control



Non 10+3 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

References:

PCI DSS Requirements and Security Assessment Procedures:

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

PCI DSS Quick Reference Guide

Version3.0: https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3.pdf

NIST SP 800-53 Rev. 4 AC-2, IA Family

HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)

End Recommendation for AP 3727 Information Security Access Control



3728 Information Security Physical Security



Non 10+4 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Reasons for Review

> New AP resulting from Chapter Lead review of IT security

Level 2 Review Schedule

08/31/24 ♦ Estimated Receipt of Recommendation

09/19/24 ♦ PPAC Approves Review Level

09/20/24 ♦ Level 2 to Constituents and AS for Feedback

10/02/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

10/17/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

11/14/24 ♦ BOT 1st Read

12/13/24 ♦ BOT Final Approval

Begin Recommendation for AP 3728 Information Security Physical Security

1. PURPOSE AND SCOPE

All San Bernardino Community College District (SBCCD) information systems must be properly protected from potential physical and environmental threats to ensure the confidentiality, integrity, and availability of the data contained within. This Administrative Procedure describes physical access methods, visitors, data center security, and media disposal.

This is one of a series of information security Administrative Procedures maintained by the District Information Technology (IT) department designed to protect SBCCD information systems.

Please refer to AP-3725–Information Security Program Overview for information on the assets' applicability and application to employees and external parties.

2. PHYSICAL SECURITY

All SBCCD technology locations will employ security control measures to prevent unauthorized physical access, damage, or interference to the premises and information.

a. Physical Security Responsibilities

- i. The Campus Police departments manage perimeter security for the colleges and District offices. This group has physical keys to buildings and a master badge allowing access to all facilities.
- ii. District IT is responsible for the data center at each location. District IT approves access to the District IT- data centers.

b. Access Cards and Visitors to SBCCD Data Centers

District IT offices and secure areas are protected by entry controls designed to allow only authorized personnel to obtain building access. Authorized individuals may be issued an Employee, Temporary, or Visitor badge that enables electronic access to exterior doors and authorized internal doors. Additional authorization may be required for access to some doors.



3728 Information Security Physical Security



Non 10+4 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Employees and visitors to SBCCD District IT facilities must clearly display ID badges at all times. Employees must be alert for unknown persons without badges, or employees not displaying badges.

District IT visitors must be provided with a badge or keycard that expires and identifies the person as a non-employee. SBCCD personnel must escort visitors. Visitors may be required to surrender badges after leaving the facility or at the date of expiration.

c. Data Center Access

The District IT and College data centers are critical processing facilities that must be protected by defined security perimeters with appropriate security access controls.

All persons who do not have a badge that requires access to the data center must be escorted by an employee whose badge is authorized to access the data center. Approval is required from the District IT and/or college management prior to any access to this area.

An authorized District IT employee is responsible for making sure that visitors entering a SBCCD data center are properly logged. It is mandatory that all visitors check in with District IT reception or college Technology departments, and visitors to a SBCCD data center must sign in and sign out with District IT and/or college Technology Department reception so that the entry and purpose of the visit can be tracked for auditing and security purposes.

For data center visitors, the reception log must note the name, date, company, purpose of visit, any escorting employee, and both sign-in and sign-out times. Spot checks of the log may be performed by District IT and/or college Technology departments and matched against the audit trail of door accesses from the keycard badging system. Reception area visitor logs must be retained for three months.

For audit and compliance purposes, the District IT management and/or college Technology department management will review those authorized to access an SBCCD data center at least quarterly to ensure that the privileges of employees or vendors who no longer need access to the data center have been removed. Records of these reviews will be maintained for audit purposes.

d. Equipment Maintenance and Environmental

District IT and college Technology departments must ensure that all utilities (e.g. UPS, generator) and other equipment is monitored in accordance with manufacturer specifications and correctly maintained to ensure the availability, integrity and confidentiality of information contained within it.

The typical data center should have dry pipe water fire suppression, HVAC units, environmental protection, redundant UPS systems, and an exterior backup diesel generator.

Only authorized maintenance personnel are allowed to perform repairs. All repairs or service work must be documented. Documentation records must be maintained by District IT and/or college Technology departments.

Computer room personnel must be trained in the use of any automatic fire suppression systems, the use of portable fire extinguishers and in the proper response to smoke and fire alarms.

Smoking, drinking, and eating in computer processing rooms is prohibited.

e. Media Disposal and Destruction

District IT and/or College Technology Departments must ensure that electronic information storage devices (e.g., hard drives (spinning, ssd, m.2, etc.), tapes, USB sticks, removable hard disks, floppy disks, CD's and DVD's) are disposed of in a manner commensurate with their information classification.



3728 Information Security Physical Security



Non 10+4 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

All electronic storage devices must be wiped by a process such that data on the storage device cannot be recovered by individuals and/or technology.

External firms responsible for disposing of any type of SBCCD information must be held to any standards specified by contract. This includes confidentiality agreements and adequate security controls.

All Data Owners must ensure that media containing Restricted data is destroyed when it is no longer needed for business or legal reasons.

Employees must use proper destruction methods when disposing of SBCCD information. Paper copies of sensitive information must be shredded or incinerated. Users of the information are responsible for disposing of it in secure disposal containers or using another proper destruction method.

f. Payment Card Industry (PCI) Requirements

Refer to AP 3737 Information Security - Payment Card Industry Requirements (PCI).

g. Policy Enforcement

Any person found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action, up to and including loss of access rights or termination of employment.

References:

NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20

HIPAA Security Rule 45 C.F.R. §§ 164.310(a)(2)(ii), 164.310(a)(2)(iii)

PCI DSS Requirements and Security Assessment

Procedures: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

PCI DSS Quick Reference Guide Version

3.0 https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3.pdf

End Recommendation for AP 3728 Information Security Physical Security

AP**3729 Information Security Logging & Monitoring**

Non 10+5 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Reasons for Review

> New AP resulting from Chapter Lead review of IT security

Level 2 Review Schedule

08/31/24 ♦ Estimated Receipt of Recommendation

09/19/24 ♦ PPAC Approves Review Level

09/20/24 ♦ Level 2 to Constituents and AS for Feedback

10/02/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

10/17/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

11/14/24 ♦ BOT 1st Read

12/13/24 ♦ BOT Final Approval

Begin Recommendation for AP 3729 Information Security Logging & Monitoring**1. PURPOSE AND SCOPE**

The objective of this Administrative Procedure is to document the requirements for logging and monitoring at the San Bernardino Community College District (SBCCD). SBCCD monitors its information technology (IT) infrastructure so that potential security incidents can be detected early and dealt with effectively.

This is one of a series of information security Administrative Procedures maintained by the District IT department designed to protect the SBCCD information systems.

Please refer to AP-3725–Information Security Program Overview applicability of assets, application to staff, and external parties.

2. LOGGING AND MONITORING

Monitoring helps speed the resolution of system problems and aids in the identification of access control policy violations. The monitoring program also verifies correct operation and the overall success or failure of network, server, and application security controls.

a. Logging Responsibilities and Tools

The District IT infrastructure must provide district-wide network logging and monitoring services. Appropriate college Technology department managers and staff will have access to these services. Centralized log analysis and event correlation of operating system event logs is performed continuously.

b. Basic Logging Requirements

Automated audit trails should reconstruct the following events for all firewalls, routers, database servers, and critical servers including:

- 1) Alarms generated by network management devices or access control systems;
- 2) All actions taken by any individual with administrative privileges;

AP

3729 Information Security Logging & Monitoring



Non 10+5 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

- 3) Changes to the configuration of major operating systems/network services/utilities/security software;
- 4) Anti-virus software alerts;
- 5) Access to all audit trails or log records; and
- 6) Failed or rejected attempts to access Restricted data or resources.

These events should be tracked by:

- 1) User identification (User ID/account name).
- 2) Type of event.
- 3) Date and time stamp.
- 4) Success or failure indication.
- 5) Name of affected data, system component, or resource.

c. Log Access and Retention

Access to audit files must be limited to authorized administrators, District IT management, and college Technology department management. Only individuals with a job-related need should be able to view, initialize or create audit files. Audit files must be kept secure so that they cannot be altered in any way, through file permissions or other means. Precautions must also be taken to prevent files or media containing logs from being overwritten and that sufficient storage capacity is present for logs.

Logs must be kept for the minimum period specified by any business or legal requirements. If no specific requirements exist, logs should be retained for at least one year.

d. Protection of Logs

Audit records are protected against modification and deletion to prevent unauthorized use.

Audit records for external-facing technologies (e.g., wireless, firewalls, DNS, etc.) are stored on a server located on the internal network.

e. Log Monitoring, Review, Analysis & Reporting

SBCCD reviews and analyzes audit records for evidence of suspicious, unusual, and inappropriate activity. SBCCD reports anomalous auditable events and related security incidents to the Vice Chancellor of Technology and Learning Services, who is responsible for reporting security issues to the Executive Leadership Team as appropriate. SBCCD adjusts the level of audit review, analysis, and reporting within systems when there is a change in risk to operations, assets, individuals, and other organizations based on law enforcement information, intelligence information, or other credible sources of information.

SBCCD establishes procedures for monitoring the use of systems and facilities to test the effectiveness of access control and security mechanisms. The results of the monitoring activities are reviewed on a regular basis. Monitoring activities include execution of privileged operations, authorized access, unauthorized access attempts, and system alerts or failures.

SBCCD meets all applicable legal requirements related to monitoring authorized access and unauthorized access attempts.

AP

3729 Information Security Logging & Monitoring



Non 10+5 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

SBCCD System Administrator activities are logged and reviewed on a regular basis.

f. Log Review Schedule like the sample below.

IT Security Event	Frequency	Responsibility
Alarms generated by network management devices or access control systems	Daily	District IT or college Technology department staff
All actions taken by any individual with administrative privileges	Daily	District IT or college Technology department staff
Anti-virus software alerts	Daily	District IT or college Technology department staff
Access to all audit trails	Daily	District IT or college Technology department staff
Failed or rejected attempts to access <i>Restricted</i> data or resources	Daily	District IT or college Technology department staff
Changes to the configuration of major operating system network services / utilities / security software	Weekly or as required	District IT or college Technology department staff
Application logs (e.g., SIS)	As required	District IT or college Technology department staff

g. Payment Card Industry (PCI Requirements)

Refer to AP 3737 Information Security - Payment Card Industry Requirements (PCI).

References:

NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, CM-8, SC-5, PE-3, PE-6, PE-20, SC-7, SI-4
 HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C),
 164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c),
 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.312(e)(2)(i), 164.314(b)(2)(i)

End Recommendation for AP 3729 Information Security Logging & Monitoring

AP 3730 Information Security Remote Access



Non 10+6 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Reasons for Review

> New AP resulting from Chapter Lead review of IT security

Level 2 Review Schedule

08/31/24 ♦ Estimated Receipt of Recommendation

09/19/24 ♦ PPAC Approves Review Level

09/20/24 ♦ Level 2 to Constituents and AS for Feedback

10/02/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

10/17/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

11/14/24 ♦ BOT 1st Read

12/13/24 ♦ BOT Final Approval

Begin Recommendation for AP 3730 Information Security Remote Access

1. PURPOSE AND SCOPE

The objective of this Administrative Procedure is to control access to the San Bernardino Community College District (SBCCD) information and systems when connections are made to those systems from a remote location.

This is one of a series of information security Administrative Procedures maintained by the Technology and Educational Support Services department designed to protect SBCCD information systems.

Please refer to AP-3725-Information Security Overview for applicability of assets application to staff, and external parties.

2. REMOTE ACCESS

All connections into and out of the internal network must be documented and managed by District IT and/or college Technology departments. Remote access is not automatically provided to all personnel and must be requested and approved as described below. The exception to this is access to the Student Information System (SIS) through the Colleague Self-Service and WebAdvisor using an Internet browser. Access to these systems is authorized for both employees and students, based on their job function and role, using assigned credentials and passwords.

Users must use established remote access mechanisms or gateways to District systems. Aside from the Colleague Self-Service and WebAdvisor, SSL VPN is used to gain access to SBCCD systems.

Remote access to District financial systems requires two-factor authentication and is granted based on the employee's job function and role, using assigned credentials and passwords.

Remote access is prohibited from any public or shared computer or Internet kiosk. This would include public computers provided for open use in a library, hotel, conference center, or any location that provides open access to a computer.

Users may not establish new remote access systems or methods unless approval has been granted, as noted below.

All remote access will be audited annually by District IT management and/or college Technology department management.



3730 Information Security Remote Access



Non 10+6 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

a. Request for Remote Access

Users create service desk tickets to request remote access. Refer to the AP-3727 Information Security - Access Control for further information.

b. Approvals for Remote Access

General remote access: For college employees, remote access must be approved by the college President or designee. For District Services employees, remote access must be approved by the Chief Technology Officer and Technology and Educational Support Services or designee.

New remote access methods: District IT must approve any new remote access method or system.

c. Access Controls for Remote Connections

Remote access sessions will be automatically disconnected after 30 minutes of inactivity. Personal firewall software must be installed on all SBCCD or employee-owned computers with direct connectivity to the Internet that are used to access a District network. Anti-virus software must also be installed and must include the most recent software updates and virus profiles.

Any remote access connection that has been established for a vendor, business partner, or other third party for purposes of support must be immediately deactivated once no longer in use by the appropriate IT staff.

d. Transmission Over Networks

If SBCCD Restricted data is to be transmitted over any communications network, it must be sent only in encrypted form. Networks include SBCCD email mail systems, connections using the Internet, and supplied SBCCD remote access systems. All such transmissions must use software encryption approved by the District IT department. For further information, refer to the AP-3726 Information Security—Data Classification.

e. Payment Card Industry Considerations

SBCCD adheres to the requirements of the Payment Card Industry Data Security Standard (PCI). Where cardholder data is present, remote access to those systems must incorporate two-factor authentication. This refers to network-level access originating from outside the SBCCD network to the SBCCD network by employees and third parties.

Personnel accessing cardholder data via remote-access technologies are prohibited from copying, moving, and storing cardholder data onto local hard drives and removable electronic media unless explicitly authorized by the Vice Chancellor of Technology and Learning Services for a legitimate business need.

3. REGULATION COMPLIANCE

The SBCCD IT team will verify compliance with this policy through various methods, including but not limited to periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate asset owner.

a. Exceptions

Any exception to this regulation must be approved in advance by the college president or designee for college employees or the Chief Technology Officer for the District employees.



3730 Information Security Remote Access



Non 10+6 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

b. Non-Compliance

c.

An employee found to have violated this regulation may be subject to disciplinary action, up to and including termination of employment.

4. RELATED STANDARDS, POLICIES, AND PROCESSES

Please review the following regulations and guidelines for details of protecting information when accessing the network via remote access methods and acceptable use of SBCCD's network:

- Administrative Procedure 3720 Electronic Communications

Reference:

NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20

HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)

End Recommendation for AP 3730 Information Security Remote Access

AP

3731 Information Security Internally Developed Systems Change Control



Non 10+7 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Reasons for Review

> New AP resulting from Chapter Lead review of IT security

Level 2 Review Schedule

08/31/24 ♦ Estimated Receipt of Recommendation

09/19/24 ♦ PPAC Approves Review Level

09/20/24 ♦ Level 2 to Constituents and AS for Feedback

10/02/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

10/17/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

11/14/24 ♦ BOT 1st Read

12/13/24 ♦ BOT Final Approval

Begin Recommendation for AP 3731 Information Security Internally Developed Systems Change Control

1. PURPOSE AND SCOPE

The objective of this Administrative Procedure is to ensure a standardized method for handling changes to District internally developed systems. Change control promotes the stability of the environment, which is essential to its security and integrity.

This is one of a series of information security Administrative Procedures designed to protect District information systems. The District Information Technology (IT) department has a district-wide fiduciary responsibility to set, maintain, and ensure the provisions of this regulation. District IT accomplishes this through collaborative engagement with the campus Technology Services departments.

a. Applicability

This Administrative Procedure applies to all full-time and part-time regular academic and classified employees, such as short-term (temporary) staff, substitutes, professional experts, Federal Work Study students, and student help who are employed by and volunteers who assist the District for the purpose of meeting the needs of students.

b. Applicability to External Parties

This Administrative Procedure applies to all external parties, including but not limited to District business partners, vendors, suppliers, service providers, and other third-party entities with access to District networks and system resources.

c. References and Related Procedures

Please refer to the Information Security Administrative Procedures for additional information, references, and definitions:

2. CHANGE CONTROL

A change is any modification or enhancement to an existing production system. Modifications can be updates to existing data, functionality, or system processes. The District IT department shall adhere to industry best practices in the development and maintenance of all internally developed systems.

a. Change Roles

The following roles have been established to guide the Change Management process for internally developed applications:

- Release Manager: Oversees the change being released into production.

AP**3731 Information Security Internally Developed Systems Change Control**

Non 10+7 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

- User: the individual or entity initiating a change, which may be either an internal District employee or contractor or an external organization.
- Product Owner: the role that qualifies and prioritizes customer Change Requests. The Product Owner may represent interests within a specific organizational entity.
- Prioritization Committee: one or more organizational bodies that review and prioritize Change Requests submitted by Product Owners or the user community.
- Quality Assurance Team: the internal department to test developed changes prior to introducing them into production. This group must be independent of the development group.
- Release Team: Internal team designed to schedule and implement changes into production.
- Development Team: the internal District group responsible for implementing and/or delivering the Change Requests.

b. Process Tools

The primary tools used to manage Change Requests are the District-wide Service Desk system for project management and an Application Lifecycle Management tool for logging, backup, and integrity monitoring.

c. Change Requirements

The basic requirements for Change Management are:

Changes that are part of the production environment must follow defined procedures by submitting a Change Request through the service desk system.

- 1) The User submits the Request.
- 2) The Request is reviewed by District IT, the relevant Product Owner, and further reviewed and prioritized by the Prioritization Committee.
- 3) Once approved by the Prioritization Committee, the development team schedules and implements the change.
- 4) All changes must be authorized by the appropriate management.
- 5) All changes to production software must be completely and comprehensively tested.
- 6) All required documentation associated with the changes must be included with the software delivery.
- 7) Program source code must be protected by restricting access to those within the Development team who have a need-to-know. Segregation of duties must be maintained.
- 8) Version controls for source code must be in place to maintain application integrity.
- 9) All change requests must be accompanied by back-out procedures to be used in the event of unexpected error conditions.
- 10) Roll-back execution conditions will be defined during the Project Release plan creation.
- 11) Production data should not be used for testing data unless it has been scrubbed. Where sensitive data must be used, the development and test environments will remain isolated from external communication.

d. Application Security Knowledge Transfer

Changes related to new or significant implementation efforts should include a knowledge transfer of relevant security information from the Development team to the Network and Security staff and other interested parties.

e. Payment Card Industry Considerations

Refer to AP 3737 Information Security - Payment Card Industry Requirements (PCI).

End Recommendation for AP 3731 Information Security Internally Developed Systems Change Control

AP**3732 Information Security Security Incident Response**

Non 10+8 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Reasons for Review

> New AP resulting from Chapter Lead review of IT security

Level 2 Review Schedule

08/31/24 ♦ Estimated Receipt of Recommendation

09/19/24 ♦ PPAC Approves Review Level

09/20/24 ♦ Level 2 to Constituents and AS for Feedback

10/02/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

10/17/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

11/14/24 ♦ BOT 1st Read

12/13/24 ♦ BOT Final Approval

Begin Recommendation for AP 3732 Information Security Security Incident Response**1. PURPOSE AND SCOPE**

The purpose of the Security Incident Response Administrative Procedure is to ensure a standardized method for handling changes to District internally developed systems. Change control promotes the stability of the environment, which is essential to its security and integrity. This is one of a series of information security Administrative Procedures designed to protect District information systems. The District Information Technology (IT) department has district-wide fiduciary responsibility to set, maintain, and ensure the regulations' provisions. District IT accomplishes this through collaborative engagement with the college Technology Services departments.

This Administrative Procedure has been written to align with the best practices as outlined in the NIST SP 800-61 Guidance.

- a. **Applicability**
This Administrative Procedure applies to all full-time and part-time regular academic and classified employees, such as, short-term (temporary) staff, substitutes, professional experts, Federal Work Study students, and student help who are employed by, and volunteers who assist, the District for the purpose of meeting the needs of students.
- b. **Applicability to External Parties**
This Administrative Procedure applies to all external parties, including but not limited to District business partners, vendors, suppliers, service providers, and other third-party entities with access to District networks and system resources.
- c. **References and Related Administrative Procedures**
Please refer to Information Security Administrative Procedures for additional information, references, and definitions.

2. INFORMATION SECURITY INCIDENT RESPONSE

Information in this regulation may be supplemented with other District information external to this document. Such information may include other business continuity plans, processes, procedures, technical standards, runbooks, etc.

In addition to providing a standardized process flow, this regulation:

- Identifies the incident response (IR) stakeholders and establishes their roles and responsibilities;
- describes incident triggering sources, incident types, and incident severity levels; and



3732 Information Security Security Incident Response



Non 10+8 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

- includes requirements for maintenance. This Administrative Procedure aligns with best practices as outlined in NIST SP 800-61.

a. Glossary/Definitions

Business Services Response Teams	Business Services Response Teams can be activated to enhance District response to incidents that affect specific business services areas. These teams have established designated contacts for handling incidents or security breaches and enhancing collaboration between diverse groups.
Computer Incident Response Team (CIRT)	The CIRT will act as the core incident coordination team for severe security incidents or breaches and is represented by individuals from District IT, College Technology Services departments, and business areas. The composition of the CIRT will vary based on incident requirements.
Incident	An Incident is defined as an event that presents the potential of unauthorized and/or unintended exposure, modification, restriction from access, or deletion of information assets, both physical and electronic, under the care of the District.
Incident Response Coordinator (IRC)	The IRC serves as the primary point of contact for response activities and maintains records of all incidents. This role has overall responsibility and ownership of the Incident Response process. The Director, Security and User Services is assigned this role by default, but other positions may act as IRC where appropriate.
Security Breach	Unauthorized release or exposure of information that is confidential, sensitive, or personally identifiable. The definition of a breach and the actions that must be taken can vary based on regulatory or contractual requirements.
Security Incident	A security incident is any adverse event that compromises the confidentiality, availability, or integrity of information. An incident may be noticed or recorded on any system and or network controlled by the District or by a service provider acting on behalf of the District.
Security Violation	An act that bypasses or contravenes District security Administrative Procedures, practices, or procedures. A security violation may result in a security incident or breach.
External Entities	In consultation with the CIRT, external entities may conduct hands-on IR activities, such as investigative response activities, or may provide guidance. External entities include vendors, service providers, or law enforcement, such as: <ul style="list-style-type: none"> Multi-State Information Sharing and Analysis Center (MS-ISAC) Federal Bureau of Investigation (FBI) Attorneys (e.g., "Cyber Coaches") and Forensics Consultants Service Providers such as Internet and Security Data Holder Vendors

b. Incident Reporting

Unplanned information security events must be reported to the appropriate manager and the district-wide IT Service Desk as quickly as possible. Suspected data breaches must be reported to the IT Service Desk within eight (8) hours of identification.



3732 Information Security Security Incident Response



Non 10+8 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Any directives issued by a member of the CIRT during a response may supersede this document.

c. Maintenance

This Administrative Procedure will be reviewed and updated minimally every five years or as relevant personnel, locations, threats, or regulatory/contractual requirements change.

The Incident Response plan and procedures should be tested at least annually.

d. Incident Response Process

The following section describes the procedures that are common to all types of security incidents and the recommended steps for each phase of a security incident.

i. Documentation and Preservation of Evidence

Evidence of a computer security incident may be required for civil or criminal prosecution or to document the event for insurance reasons. In order to preserve evidence, all relevant information collected during the incident must be protected. To maintain the usefulness of possible evidence, District staff must be able to identify each note or piece of evidence and be prepared to explain its meaning and content.

The chain of custody for all evidence must be preserved. Documentation will be required that indicates the date, time, storage location, and sequence of individuals who handled the evidence. There must not be any lapses in time or date. The hand-off of evidence to authorities must also be documented.

Documentation of the incident must minimally include:

- Date/time the incident was reported
- Type of Incident
- Reporting source of incident
- Summary of the incident
- Current status of the incident
- All actions taken concerning the incident
- Contact information for all involved parties
- Evidence gathered during the incident investigation
- Relevant comments from IR team members
- Proposed next steps to be taken

ii. Security Incident Categories

District Security incident categories can be found in the district-wide IT Service Desk.

iii. Security Incident Severity Levels

Incident Severity Level	Description	Action Required
	Significant risk of negative financial or public relations impact	Management team members

<p>HIGH</p>	<ul style="list-style-type: none"> • Hacking or denial of service attack attempted with limited impact on operations • Widespread instances of a new computer virus not handled by anti-virus software • Possible breach of student information or PII • Some risk of negative financial or public relations impact 	<ol style="list-style-type: none"> 1. Log incident in IT Service Desk 2. Notify IRC or designee 3. IRC will notify CIRT team members as needed
<p>MEDIUM</p>	<ul style="list-style-type: none"> • Hacking or denial of service attacks attempted with no impact on operations • Widespread computer viruses are easily handled by anti-virus software • Lost laptop/smartphone, but no data compromised 	<ol style="list-style-type: none"> 1. Log incident in IT Service Desk 2. IRC will review and notify CIRT team members as needed.
<p>LOW</p>	<ul style="list-style-type: none"> • Password compromises – single user • Unauthorized access attempts • Account sharing • Account lockouts 	<ol style="list-style-type: none"> 1. Log the incident in the IT Service Desk where appropriate. 2. IRC will review and coordinate remediation as needed.

iv. Escalation

If it is discovered that the scope or severity of an incident has changed, it is important to communicate this change to the CIRT.

If an incident involves a breach of Payment Card Industry (PCI) data, the acquirer and related payment brands must be notified of the incident as soon as possible.

Include the appropriate IR stakeholders in identifying the reporting procedures for each payment brand and acquirer involved in the incident. (PCI DSS 12.10.1)

If an incident potentially involves a breach of student personally identifiable information (PII) or financial aid data, the IRC must be notified immediately. The IRC will then communicate to appropriate CIRT team members (e.g., Financial Aid Directors). It is their responsibility to follow the U.S. Department of Education Privacy laws specified in the Family Educational Rights and Privacy Act (FERPA).

For all other incidents, the Vice Chancellor of Educational and Technology Services or designee(s) must be consulted prior to discussion with any person outside of the District.

End Recommendation for AP 3732 Information Security Security Incident Response

AP**3733 Information Security Security Secure Operations**

Non 10+9 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Reasons for Review

> New AP resulting from Chapter Lead review of IT security

Level 2 Review Schedule

08/31/24 ♦ Estimated Receipt of Recommendation

09/19/24 ♦ PPAC Approves Review Level

09/20/24 ♦ Level 2 to Constituents and AS for Feedback

10/02/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

10/17/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

11/14/24 ♦ BOT 1st Read

12/13/24 ♦ BOT Final Approval

Begin Recommendation for AP 3733 Information Security Security Secure Operations**1. PURPOSE AND SCOPE**

The objective of this Administrative Procedure is to describe policies for secure operations of District information and systems. The following topics are covered:

- Operations Processing
- Application Development
- Virus Management
- Patches and Updates
- Backup AR
- Third Party Management

This is one of a series of information security Administrative Procedures designed to protect the District's information systems. The District Information Technology (IT) department has district-wide fiduciary responsibility to set, maintain, and ensure the provisions of this regulation. District IT accomplishes this through collaborative engagement with the campus Technology Services departments.

- a. **Applicability**
This Administrative Procedure applies to all full-time and part-time regular academic and classified employees, such as, short-term (temporary) staff, substitutes, professional experts, Federal Work Study students, and student help who are employed by, and volunteers who assist, the District for the purpose of meeting the needs of students.
- b. **Applicability to External Parties**
This Administrative Procedure applies to all external parties, including but not limited to District business partners, vendors, suppliers, service providers, and other third-party entities with access to District networks and system resources.
- c. **References and Related Documents**
Please refer to the Information Security Administrative Procedures for additional information and references, and definitions.

AP

3733 Information Security Security Secure Operations



Non 10+9 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

2. SECURE OPERATIONS

a. Operations Processing

All system scheduling, jobs, and dependencies must be documented. This documentation must include job start times, latest job completion times, delay procedures, and handling procedures in case of failure or error.

Operating system and application processing, restart, and shutdown procedures must be documented.

Application back out, restart, and shutdown procedures with emergency contact information must be provided by the Applications Development team and made available to District IT operations personnel.

Refer to AR 3728: Information Security – Physical Security for data center access and other physical security controls.

b. Virus Management

All applicable systems must be configured with District IT-approved anti-virus software. The software must be configured to scan for viruses in real time. Anti-virus programs must be capable of detecting, removing, and protecting against all known types of malicious software.

All systems with anti-virus software must be configured to update virus signatures daily.

End users must not be able to configure or disable the software.

c. All anti-virus mechanisms must generate audit logs to aid District IT and college Technology Departments in detecting and responding to virus outbreaks.

d. District IT or college Technology Services departments may install approved anti-virus software on any District assets or allow users to install it themselves.

e. Patches and Updates

The District must ensure that all system components and software are protected from known vulnerabilities by installing the latest vendor-supplied firmware, security patches, hot fixes, and service packs found to be applicable to District computing resources.

District IT and college Technology Services network administrators must keep up with vendor changes and enhancements. New or modified non-urgent security patches must be scheduled and installed within one month of release. College Technology Services departments may elect not to install system updates that are unrelated to District business and that do not affect security. Urgent patches that address security vulnerabilities must be installed as soon as feasible without introducing instability or impacting service availability.

Where feasible, patches must be tested in a test environment prior to production deployment. Testing must ensure that systems function correctly.

Changes to servers and networks should be tested prior to implementation and follow normal change control management procedures.

District IT and campus technology departments must be alerted to identifying new security vulnerabilities by monitoring available vendor or industry security sources. Hardening and configuration standards must be updated as soon as practical after new vulnerabilities are found.

f. Software and Asset Management

AP**3733 Information Security Security Secure Operations**

Non 10+9 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

The AP 3720: Electronic Communications sets forth usage policies for critical technologies that include e-mail usage and Internet usage and defines proper use of these technologies. District IT and college Technology Services departments may also issue mobile devices (such as laptops or removable storage devices) and will maintain a list of issued devices and personnel with access to assist in determining the owner, contact information, and purpose.

District IT and campus technology departments will maintain a list of company-approved products and software.

g. Backup and Media

Users must store all critical files on the local area network so that they can be properly backed up. If an end-user chooses to store essential data elsewhere, it must be approved by District IT management or college Technology Services management, and the user is responsible for ensuring the data can be recovered.

Any media containing backup data that is stored onsite must be classified so that operations personnel can determine the sensitivity of the data stored on tape or other formats. Refer to the AP 3726: Information Security - Data Classification for classification and handling information.

Any backup media that must be transferred that contains Restricted information must be sent by secured courier or other delivery method that can be accurately tracked. Management must approve any and all media that is moved from a secured area, especially when media is distributed to individuals.

Strict control must be maintained over the storage and accessibility of backup media. Inventory logs of all media must be maintained and reviewed at least annually.

Media must be destroyed when it is no longer needed for business or legal reasons. Data retention requirements must be documented.

h. Third Party Management

A third-party user is a non-District employee or entity that is authorized to access District systems and networks. Examples of third-party users include consultants, contractors, project specialists, vendors, business partners, service providers, and suppliers of products, services, or information.

A process for engaging service providers must include proper due diligence prior to beginning the engagement. A list of all third-party providers must be maintained.

Network connections between the District's environment and third parties must follow agreed-upon security procedures and/or confidentiality requirements. Such connections and other third-party access to the District's systems must be governed by formal written agreements or contracts. The third party must agree to adhere to the District Information Security Administrative Procedure.

These agreements may require signed Confidentiality and Non-Disclosure statements restricting the subsequent usage and dissemination of District information.

Vendors or other third parties with access to District-owned or leased equipment or systems housed in the District's data center are restricted to only the specific equipment and systems they are authorized to maintain or monitor.

1) G.1 HIPAA Third Party Agreements

- HIPAA regulations specify that formal written agreements must be established with each party (often considered a "business associate") who will access protected health information (PHI). The parties must agree to protect the integrity and confidentiality of the information being exchanged, and the agreement would clearly define responsibilities of both parties as follows:
- District security policies and security mandates, including any fines and penalties that may be incurred for HIPAA or PCI non-compliance for lack of compliance with the regulations.

AP**3733 Information Security Security Secure Operations**

Non 10+9 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

- Ownership and acceptable uses of PHI and other classified information.
- Requirements for business continuity by the third party, in the event of a major disruption, disaster, or failure.
- Audit provisions for District or District-approved entities in the event of a data compromise. Provisions to ensure that District, or a District approved auditor, will be provided with full cooperation and access to conduct a thorough security review after a security intrusion. The review will validate compliance with District standards and HIPAA regulators for protecting PHI and other District information.
- Security of PHI and District information during third-party contract terminations or data transfers.

2) G.2 PCI Third-Party Requirements

The District maintains a program to monitor its Payment Card Industry Data Security Standard (PCI DSS) service providers' compliance status at least annually.

PCI DSS requires that shared hosting providers protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A of the PCI DSS.

A written agreement that includes an acknowledgment from any PCI service provider must be maintained to ensure that the third party accepts responsibility for the security of cardholder data the service provider possesses.

All service providers providing PCI services must be monitored at least annually to ensure their continued compliance with PCI DSS.

Refer to AP 3737 Information Security - Payment Card Industry Requirements (PCI).

End Recommendation for AP 3733 Information Security Security Secure Operations

AP**3734 Information Security Security Network Security**

Non 10+10 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Reasons for Review

> New AP resulting from Chapter Lead review of IT security

Level 2 Review Schedule

08/31/24 ♦ Estimated Receipt of Recommendation

09/19/24 ♦ PPAC Approves Review Level

09/20/24 ♦ Level 2 to Constituents and AS for Feedback

10/02/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

10/17/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

11/14/24 ♦ BOT 1st Read

12/13/24 ♦ BOT Final Approval

Begin Recommendation for AP 3734 Information Security Security Network Security**1. PURPOSE AND SCOPE**

The objective of this Administrative Procedure is to describe controls required to protect District information and systems. Network infrastructure must be configured securely in order to protect District systems and maintain network integrity and availability. Effective network security will reduce potential vulnerabilities and help to enforce secure access to District information and technology.

This is one of a series of information security Administrative Procedures designed to protect District information systems. The District Information Technology (IT) department has a district-wide fiduciary responsibility to set, maintain, and ensure the provisions of this regulation. District IT accomplishes this through collaborative engagement with the campus Technology Services departments.

a. Applicability of Assets

This Administrative Procedure applies to all electronic assets that are owned or leased by the District, including but not limited to:

- Servers
- Network Infrastructure
- Mobile Devices
- Infrastructure as a Service or IaaS

b. Applicability

This Administrative Procedure applies to all full-time and part-time regular academic and classified employees, , such as short-term (temporary) staff, substitutes, professional experts, Federal Work Study students, and student help, who are employed by, and volunteers who assist the District for meeting the needs of students.

c. Applicability and Related Documents

This Administrative Procedure applies to all external parties, including but not limited to District business partners, vendors, suppliers, service providers, and other third-party entities with access to District networks and system resources.

AP

3734 Information Security Security Network Security



Non 10+10 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

d. References and Related Documents

Please refer to the Information Security Administrative Procedures for additional information references, and definitions.

2. NETWORK SECURITY

District IT has primary responsibility for District network and security. District IT in collaboration with the college technology departments manages and administers campus infrastructure and network components. Senior Technology Support Specialists, supervised by the District Director Technology Services are the operational managers of district and campus firewalls and network equipment.

a. General Network Controls

System configuration standards are in place for critical network and server components that are managed by District IT and campus technology departments. Standards must address known security vulnerabilities and industry best practices and provide specifications for "hardening" the native operating system or platform from known security weaknesses.

District IT must maintain appropriate network documentation, including a high-level network diagram specifically noting inbound and outbound network connections. This must include wireless network components and show connections to all networks, any cardholder data Payment Card Industry (PCI) locations, and wireless networks.

Network diagrams and configuration details must not be disclosed to unauthorized parties unless identifying IP addresses and names have been removed. The data classification level for sanitized (IP addresses, server names, and other identifying elements removed) diagrams is Internal. Unsanitized network diagrams have a data classification of Restricted. Refer to the Administrative Procedure 3726: Information Security - Data Classification for classification requirements.

Only necessary and secure services, protocols, services/daemons, etc., should be enabled as required for the function of the system. For any required services, protocols, or services/daemons that are insecure, appropriate security features must be enabled. For example, secure technologies such as SSH, S-FTP, SSL, or IPsec VPN should be used to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.

Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure must be maintained by District IT or college Technology Services. Vendor-supplied defaults must be changed before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.

System security parameters must be configured to prevent misuse. All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers, must be removed.

Publicly accessible network jacks should be restricted to authorized systems.

b. External Connections and Firewalls

District IT management or campus technology management must approve all new external connections, inbound or outbound, to the District's internal network. All connections into and out of the internal network must be documented, managed, and internally coordinated. Firewalls must be deployed to restrict inbound and outbound connections to the District's network.

New network connections requested to be allowed through District firewalls must be approved by District IT management or college Technology Department management and require a business case justification.



3734 Information Security Security Network Security



Non 10+10 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Ad-hoc modification of firewall rules can jeopardize the security of the District's network. Established change control procedures must be followed for all firewall changes.

Where technically possible, firewall rules should be tested prior to implementation.

A review of all firewalls and routers must be completed every six (6) months. This activity must include a review of the specific ports/services/protocols allowed into the environment and proper documentation of the review.

For specific processes and procedures, refer to AR 3731: Internally Developed Systems- Change Control and Firewall Security Departmental Procedures.

c. Wireless Security

Wireless connectivity is provided as a convenience for staff and students utilizing wireless implementation at SBCCD colleges and sites. Either a student or staff SSID must be entered to gain access. Refer to Wireless Security Departmental Procedures for additional information on using wireless services.

Any other permanent wireless network implementations must be approved by District IT.

Wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings, must be changed prior to implementation.

District IT and college Technology Departments will test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.

1) Wireless Environments and PCI

Whenever possible, cellular networks must be used for wireless transmission of cardholder data.

Firewalls are installed between wireless networks and the cardholder data environment and configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

For wireless environments connected to the cardholder data environment or transmitting cardholder data, vendor defaults must be changed. This includes but is not limited to default wireless encryption keys, passwords, and SNMP community strings.

d. Encryption

Encryption scrambles sensitive information that is stored or transmitted electronically. Cryptographic solutions must adhere to international export laws or any applicable legal or regulatory controls. Encryption must be used at the District in the following situations.

1) Passwords

All passwords must be encrypted and unreadable. This includes password files for users, firewalls, routers, operating systems, applications, databases, and web servers. Password or credential files stored on third-party platforms must also be encrypted.

2) Restricted Data

AP 3726: Information Security-Data Classification describes how data is categorized based on its sensitivity, need for confidentiality, or value to the District. Data classified as Restricted is the most sensitive category. Its unauthorized disclosure may violate regulations or standards, such as PCI, or contractual agreements with third parties or service providers.

Restricted data may exist in applications, databases, or files. Various access controls protect data when in its original location, but



3734 Information Security Security Network Security



Non 10+10 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

when copied, reproduced, or transmitted, the original protections are lost. However, the classification and level of protection for a data element must travel with it regardless of its location or format.

Storing Restricted data on unencrypted removable devices, personal drives, or various types of USB storage may expose sensitive or confidential data to unauthorized disclosure and is against District regulations. If transporting or storing restricted data, it must be on a removable device; users must work with District IT or campus IT to ensure the data is secure.

If Restricted data is copied from its original location (e.g., to other files, removable devices, or on backup media), it must be encrypted. If sent via e-mail or other transmission means on public networks, it must be encrypted. Refer to the Encryption Departmental Procedures for specific encryption methods and procedures.

3) Remote Administrator Access

Remote access by security, system, or firewall administrators to perform maintenance or troubleshoot problems presents a greater security risk due to the elevated privileges these individuals possess. System Administrators must connect securely using the SSL VPN to ensure that communications with District networks from a remote location are over an encrypted channel. This includes any non-console administrative access. Two-factor authentication is required where technically feasible.

4) Key Management

Key management procedures must be documented for all processes and procedures involving encryption keys, especially if used for cardholder data. PCI DSS requirements mandate strong keys, secure key distribution and storage, periodic key changes, and other requirements. Please refer to the Encryption Departmental Procedures for detailed information.

e. Scanning and Vulnerability Management

District IT and college Technology Departments must be informed of information security issues and vulnerabilities applicable to District computing systems. When security issues are identified, District IT is responsible for notifying appropriate personnel, including system and network administrators/technicians and college Technology Directors.

The primary method for identifying new threats as they arise will be through vendor and security Internet mailing lists. The District will identify and assign a risk ranking to newly discovered security vulnerabilities. As appropriate, platform hardening standards must be updated to reflect measures required for protection from any newly discovered vulnerability.

The District performs quarterly external vulnerability scans on critical systems and networks in scope for PCI compliance. External vulnerability scans are performed by an Approved Scanning Vendor (ASV) as designated by the Payment Card Industry Security Standards Council (PCI SSC).

The District performs internal vulnerability scans on a periodic (at least semi-annual) basis or after any significant network changes. Penetration tests must be performed at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include both network-layer and application-layer tests.

An annual process is in place to identify threats and vulnerabilities that result in a formal risk assessment.

f. Network Time Protocol (NTP)

All critical system clocks and times must be configured to acquire, distribute, and store a consistent time. All District production systems must be configured to use one of the internal NTP servers to maintain time synchronization with other systems in the environment. Internal NTP servers will be configured to request time updates from the Internet site <http://time.nist.gov>. Client systems able to retrieve time settings from the NTP server will be limited through Access Control Lists (ACL). The NTP system will always run the latest available version of the software.

AP

3734 Information Security Security Network Security



Non 10+10 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

- g. Payment Card Industry (PCI) Requirements
Refer to AP 3737 Information Security - Payment Card Industry Requirements (PCI).

End Recommendation for AP 3734 Information Security Security Network Security



3735 Information Security Disaster Recovery



Non 10+11 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Reasons for Review

> New AP resulting from Chapter Lead review of IT security

Level 2 Review Schedule

08/31/24 ♦ Estimated Receipt of Recommendation

09/19/24 ♦ PPAC Approves Review Level

09/20/24 ♦ Level 2 to Constituents and AS for Feedback

10/02/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

10/17/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

11/14/24 ♦ BOT 1st Read

12/13/24 ♦ BOT Final Approval

Begin Recommendation for AP 3735 Information Security Disaster Recovery

1. PURPOSE AND SCOPE

The objective of this Administrative Procedure is to outline the strategy and basic procedures to enable the District to withstand the prolonged unavailability of critical information and systems and provide for the recovery of District Information Technology (IT) services in the event of a disaster.

This is one of a series of information security Administrative Procedures designed to protect District information systems. The District Information Technology (IT) department has a district-wide fiduciary responsibility to set, maintain, and ensure the provisions of this regulation. District IT accomplishes this through collaborative engagement with the campus Technology Services departments.

a. Applicability

This Administrative Procedure applies to all full-time and part-time regular academic and classified employees, such as short-term (temporary) staff, substitutes, professional experts, Federal Work Study students, and student help, who are employed by, and volunteers who assist the District for the purpose of meeting the needs of students.

b. Applicability to External Parties

This Administrative Procedure applies to all external parties, including but not limited to District business partners, vendors, suppliers, service providers, and other third-party entities with access to District networks and system resources.

c. References and Related Documents

Please refer to the Information Security Administrative Procedures for additional information, references, and definitions.

2. DISASTER RECOVERY

Disaster Recovery (DR) is best described as the plans and activities designed to recover technical infrastructure and restore critical business applications to an acceptable condition. DR is a component of Business Continuity Planning, which is the process of ensuring that essential business functions continue to operate during and after a disaster.



3735 Information Security Disaster Recovery



Non 10+11 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

a. Disaster Recovery Strategy and Components

This plan is structured around teams, with each team having a set of specific responsibilities. The District Disaster Recovery strategy is based on the following elements:

- IT infrastructure designed with redundancy and application availability in mind.
- The ability to leverage cloud-based or alternate site locations and facilities.
- Documented and tested IT Disaster Recovery procedures for each Tier 1 application.
- Business Continuity plans as developed by associated business areas.

This Administrative Procedure describes:

- Disaster declaration.
- A priority list of critical applications and services to be recovered.
- Key tasks that include responsibilities and assignments for each task.
- Departments and individuals who are part of the recovery process.

Each critical application that has been identified in this Administrative Procedure has its own Disaster Recovery Plan that can be found in Departmental Procedures.

Paper copies of this Administrative Procedure and Appendices must be stored at secure and readily accessible off-site locations.

b. Business Continuity Plans

The Disaster Recovery Plan for a critical application is a complementary subset of departmental Business Continuity Plans (BCPs). These plans describe the actions to be taken within business areas that rely upon and use those applications.

Copies of BCPs will be documented and maintained by District business units as led and developed by management. The IT Disaster Recovery Coordinator will retain master copies of all District BCPs (see Section II.C.2 for the description of roles).

Copies of all BCPs must be kept off-site. All plans must be reviewed at least annually and updated for any significant changes.

All relevant District employees must be made aware of the Business Continuity Plan and their own respective roles. Training must be provided to staff with operational business and /or recovery plan execution responsibilities.

Business Continuity Plans must be developed with requirements based on the specific risks associated with the process or system. Business Continuity Plans must include, but are not limited to, the following information:

- 1) Executive Summary
- 2) Key Assumptions
- 3) Identified Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- 4) Long-term vs. Short-term Outage Considerations
- 5) Disaster Declaration / Plan Activation Procedures (e.g., communication plan, mobilization plan)
- 6) Key Contacts / Calling Tree(s)
- 7) Roles / Responsibilities (e.g., Recovery Teams)
- 8) Alternate Site / Lodging
- 9) Asset Inventory
- 10) Detailed Recovery Procedures, including the priority order of system recovery
- 11) Relevant Disaster Recovery Plan
- 12) Event and recovery status reporting to District management, appropriate employees, third parties, and business partners.

Sufficient detail must be included so that procedures can be carried out by individuals who do not normally perform these responsibilities.



3735 Information Security Disaster Recovery



Non 10+11 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

c. Roles and Responsibilities

1) Disaster Management Team

The Disaster Management Team is responsible for providing overall direction of the data center recovery operations. It ascertains the extent of the damage and activates the recovery organization. Its prime role is to monitor and direct the recovery effort. It has a dual structure in that its members include Team Leaders of other teams. Responsibilities of the Disaster Management Team include:

- Evaluating the extent of the problem and potential consequences and initiating disaster recovery procedures.
- Monitoring recovery operations; managing the Recovery teams and liaising with District management and users as appropriate; notifying senior management of the disaster, recovery progress, and problems.
- Controlling and recording emergency costs and expenditures; expediting authorization of expenditures by other teams.
- Approving the results of audit tests on the applications which are processed at the standby facility shortly after they have been produced.
- Declaring that the Disaster Recovery Plan is no longer in effect when critical business systems and application processing are restored at the primary site.

The Disaster Management Team Leader is responsible for deciding whether or not the situation warrants the introduction of disaster recovery procedures. If they decide that it does, then the organization defined in this section comes into force and, for the duration of the disaster, supersedes any current management structures.

The Disaster Management Team will operate from a Command Center or, if that is not possible, at a secondary location to be determined. The team members are:

- Vice Chancellor of Educational & Student Support Services
- Chief of Technology
- Director of Technical Services

2) Recovery Coordinators

There are two coordination roles who will report to the Disaster Management Team:

- A Disaster Recovery Coordinator (to be appointed) is the communications focal point for the Disaster Management Team and other teams, and will coordinate disaster notification, damage control, and problem correction services. The Disaster Recovery Coordinator also maintains the IT Disaster Recovery Plans and offsite copies, and retains master copies of Business Recovery Plans.
- Business Recovery Coordinators (to be appointed) will develop and maintain Business Recovery Plans and coordinate recovery efforts and notification in their business areas.

3) Operations Team

The Operations Team is responsible for the computer environment (Data Center and other vital computer locations) and for performing tasks within those environments. This team is responsible for restoring computer processing and for performing Data Center activities, including:

- Installing the computer hardware and setting up the latest version of the operating system at the standby facility.
- Arranging for acquisition and/or availability of necessary computer equipment and supplies.
- Establishing processing schedule and informing user contacts.
- Obtaining all appropriate historical/current data from the offsite storage vendor.
- Restoring the most current application systems, software libraries, and database environments.



3735 Information Security Disaster Recovery



Non 10+11 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

- Coordinating the user groups to aid the recovery of any non-recoverable (i.e., not available on the latest backup) data.
- Providing the appropriate management and staffing for the standby data center, help desk, and backup library in order to meet the defined level of user requirements.
- Performing backup activities at the standby site.
- Providing ongoing technical support at the standby site.
- Working with the Network Team to restore local and wide area data communications services to meet the minimum processing requirements.
- Ensuring that all documentation for standards, operations, vital records maintenance, application programs etc. are stored in a secure/safe environment and reassembled at the standby facilities, as appropriate.

4) Network Team

The Network Team is responsible for all computer networking and communications, to include:

- Evaluating the extent of damage to the voice and data network.
- Discussing alternate communications arrangements with telecom service providers, and ordering the voice/data communications services and equipment as required.
- Arranging new local and wide area data communications facilities and a communications network that links the standby facility to the critical users.
- Establishing the network at the standby site, and installing a minimum voice network to enable identified critical telephone users to link to the public network.
- Defining the priorities for restoring the network in the user areas.
- Supervising the line and equipment installation for the new network.
- Providing necessary network documentation.
- Providing ongoing support of the networks at the standby facility.
- Re-establishing networks at the primary site when the post-disaster restoration is complete.

5) Facilities Team

The Facilities Team is responsible for the general environment, including buildings, services, and environmental issues outside of the Data Center. This team has responsibility for security, health and safety, and for replacement of building facilities, including:

- In conjunction with the Disaster Management Team, evaluate the damage and identify equipment that can be salvaged.
- Arranging all transport to the standby facility.
- Arranging for all necessary office support services.
- Controlling security at the standby facility and the damaged site (physical security may need to be increased).
- Working with the Network Team to have lines ready for rapid activation.
- As soon as the standby site is occupied, clean up the disaster site and secure that site to prevent further damage.
- Administering the reconstruction of the original site for recovery and operation.
- Supplying information for initiating insurance claims and ensuring that insurance arrangements are appropriate for the circumstances (i.e., any replacement equipment is immediately covered, etc.).
- Maintaining current configuration schematics of the Data Center (stored off-site). This should include:
 - air conditioning
 - power distribution
 - electrical supplies and connections
 - specifications and floor layouts
- Dealing with staff safety and welfare.
- Working with Campus Police, who will contact local law enforcement if needed.

6) Communications Team



3735 Information Security Disaster Recovery



Non 10+11 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

The Communications Team is responsible for obtaining communications directives from the Disaster Management Team and communicating information during the disaster and restoration phases to employees, suppliers, third parties, and students. All information that is to be released must be handled through the Public Information Officer (PIO).

The Communications Team is made up of the PIO and individuals from colleges, marketing, legal, HR, and business area organizations, as appropriate. This team has the responsibility for:

- Liaising with the PIO, Disaster Recovery Coordinator and/or Business Recovery Coordinators to obtain directives on the messages to communicate.
- Making statements to local, national, and international media.
- Informing suppliers and students of any potential delays.
- Informing employees of the recovery progress of the schedules using available communication methods.
- Ensuring that there is no miscommunications that could damage the image of the District.
- Any other public relations requirements.

d. Update, Testing and Maintenance

This Disaster Recovery plan must be kept up to date. It is the responsibility of the Disaster Recovery Coordinator to ensure that procedures are in place to keep this plan up to date. If, while using this plan, any information is found to be incorrect, missing or unclear, please inform the Disaster Recovery Coordinator so that it may be corrected. It is important that everyone understands their role as described in this plan.

Updated versions of the plan are distributed to the authorized recipients, listed in Section II.E.

The IT Disaster Recovery Plans, as documented in the Appendices, must be reviewed by IT and business management at least semi-annually and when significant application or infrastructure changes are made.

Plans must be tested periodically and at least annually, and include realistic simulations involving the business users and District IT staff. The results of DR tests must be documented, reviewed, and approved by appropriate management.

e. Distribution List

The Disaster Recovery Coordinator is responsible for distributing this plan. Each plan holder, listed in the table below, receives two copies of this plan. One copy is to be kept at the place of work and the other copy at home or other safe and secure offsite location. These copies have an official copy number.

Name	Copy Number	Location
Vice Chancellor, Educational and Student Support Services	DR001	Office
Chief Technology Officer	DR002	Office
District Director, Technology Services	DR003	Office
Director, Security and User Services	DR004	Office
Director, Administrative Applications	DR005	Office
Business Systems Administrator	DR006	Office
College Director, Technology Services (Crafton)	DR007	Office
College Director, Technology Services (Valley)	DR008	Office
Public Information Officer		

f. What to do in the Event of a Disaster



3735 Information Security Disaster Recovery



Non 10+11 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

The most critical and complex part of disaster response is mobilizing the required personnel in an efficient manner during the invocation of the plan. Because normal processes have been disrupted, individuals are taking on new roles and responsibilities and must adapt to changing circumstances quickly.

The key is for personnel to be well-rehearsed, familiar with the Disaster Recovery Plan, and be sure of their assignments.

1) Standard Emergency Plan The priority in a disaster situation is to ensure the safe evacuation of all personnel.

In the event of a major physical disruption, standard emergency procedures must be followed. This means immediately:

- Activating the standard alarm procedures for that section of the building to ensure that emergency authorities (fire, medical, law enforcement, etc.) are correctly alerted.
- If necessary, evacuating the premises following the established evacuation procedures and assembling outside at the designated location if it is safe to do so.

2) First Steps for the Recovery Teams

Action	Team
Evaluate the damage	Disaster Management, Facilities, Operations, Network
Identify the concerned applications	Disaster Management, Operations, Network
Request the appropriate resources for the Standby Facility	Disaster Management
Obtain the appropriate backups	Operations
Restart the appropriate applications at the Standby Facility	Operations
Inform users of the new procedures	Communications
Order replacement equipment to replace the damaged computers/networks	Operations, Network
Install replacement equipment and restart the applications	Operations, Network
Inform users of normal operations	Communications

3) The Next Steps

- The Disaster Management Team Leader decides whether to declare a disaster and activate the Disaster Recovery Plan and which recovery scenario will be followed.
- The Recovery Teams then follow the defined recovery activities and act within the responsibilities of each team, as defined in this Disaster Recovery Plan and those defined for the critical applications outlined in the District IT Business Continuity Departmental Procedures.

4) Critical Business Applications/Services

The following business applications are considered critical to the District's business:

- Tier 1 application (Student Information System)



3735 Information Security Disaster Recovery



Non 10+11 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

- Tier 1 application (Financial System)

District IT departmental procedures exist to address the DR procedures for these services.

g. Disaster Declaration

In the event of a serious system disruption, the Disaster Management Team will determine the level of response based on the disaster classification categories below. This determination will be made within four (4) hours of the occurrence.

The classification level should be reviewed every 12 hours, and re-classification of the disaster will be made as needed until recovery is complete.

Disasters at the District fall into one of the following four levels.

Disaster Classification	Description
Level 1 (Low)	<p>Sub-system Outage / Minor Damage</p> <p>Partial loss of a component of a critical application for a period of one day to one week. This type of outage does not result in the total loss of operation for that application; however, specific functionality is reduced or impaired.</p> <p>In this scenario, only a part of the computer processing environment is impacted, but the communication lines and network are still up and running. The building is still available, and the users can use normal office space to wait for the restart of the server or application processing. The goal of the recovery process, in this case, is to restore server or application functionality.</p>
Level 2 (Medium)	<p>Short Term Outage</p> <p>Complete loss of a critical application for a period of one day to one week. The ability to meet business functions and mission objectives may be impacted, usually by elongated processing cycles and missed deadlines, but not to a significant extent.</p> <p>In this scenario, a key computer processing application is unavailable. Communication lines or portions of the network may be down.</p> <p>The goal of the recovery process is to restore minimum critical application functionality, which may require moving affected applications to alternate equipment. An alternate site may need to be put on Standby.</p>



3735 Information Security Disaster Recovery



Non 10+11 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

<p>Level 3 (High)</p>	<p>Long Term Outage</p> <p>Complete loss of a critical application for a period greater than one week but less than two weeks.</p> <p>The ability to continue the business function and its mission is in jeopardy and may fail in some circumstances, such as missing critical milestones in the business cycle.</p> <p>In this scenario, key portions of the computer processing environment are unavailable. Communication lines or portions of the network may also be down.</p> <p>The goal of the recovery process is to restore minimum critical application functionality either at the primary facility or at the Standby facility.</p>
<p>Level 4 (Critical)</p>	<p>Total System Disaster</p> <p>Catastrophic loss of operation of critical system(s) for a period greater than two weeks. Also included in this class are disasters that may not produce outages greater than two weeks, but involve more than one critical application; or natural disasters such as fires, floods, or other catastrophic situations.</p> <p>In this scenario, the entire computer processing environment has experienced a catastrophic disaster and is generally unavailable. Communication lines and/or the network also may not be available.</p> <p>The goal of the recovery process is to restore minimum critical application functionality either at the primary or at the Standby facility as quickly as possible.</p>

End Recommendation for AP 3735 Information Security Disaster Recovery

AP 3736 Information Security Cloud Storage



Non 10+12 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Reasons for Review

> New AP resulting from Chapter Lead review of IT security

Level 2 Review Schedule

08/31/24 ♦ Estimated Receipt of Recommendation

09/19/24 ♦ PPAC Approves Review Level

09/20/24 ♦ Level 2 to Constituents and AS for Feedback

10/02/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

10/17/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

11/14/24 ♦ BOT 1st Read

12/13/24 ♦ BOT Final Approval

Begin Recommendation for AP 3736 Information Security Cloud Storage

1. PURPOSE AND SCOPE

The objective of this Administrative Procedure is to provide the framework within which San Bernardino Community College District (SBCCD) employees can create, store, share, and process data in “cloud storage” environments.

This is one of a series of information security Administrative Procedures maintained by the District Information Technology (IT) Department with collaboration and input from the colleges and designed to protect district information systems.

Please refer to AP 3725: Information Security Program Overview for applicability to staff and external parties and to AP 3726: Information Security—Data Classification for detailed information about the types of data.

2. CLOUD STORAGE

- a. Cloud Storage: A model of networked online storage where data is stored in virtualized storage pools not contained within the device through which the data is accessed. Such data storage is most often offsite and usually managed by independent vendors (e.g., Google Drive or G-Suite, Apple iCloud, Microsoft OneDrive). Cloud storage of data classified as Internal or Restricted can exist within the district-approved Learning Management System (such as Canvas), or district-approved cloud storage (such as Sharepoint or OneDrive).
- b. Data Types: Per AP 3725 and AP 3726, district data is classified in the following categories:
 - i. Public: information made for public distribution (such as press releases, public web pages, or publicly available data);
 - ii. Internal: data that must be protected due to proprietary or business reasons but is not personally identifiable or sensitive;
 - iii. Restricted: information that is sensitive in nature, may be protected by statute, regulation, or contractual requirements, and can include personally identifiable information like student data and grades, credit card data, human resources information, or health-care related information III.

3. APPROPRIATE USE OF CLOUD STORAGE

While recognized as a valuable teaching and productivity tool, cloud storage increases the risk of a data breach. As a result, users must adhere to the following requirements:



3736 Information Security Cloud Storage



Non 10+12 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

- a. SBCCD employees have a responsibility to protect the college and District data, particularly confidential data about individuals.
- b. Internal and Restricted district data may be stored by employees on cloud storage under the following conditions:
 - i. The cloud storage must be District-approved cloud storage.
 - ii. Access to the data in cloud storage is secure (e.g., requires password and/or dual factor authentication for access).
 - iii. Devices (including desktop, notebook or tablet computers and cellular phones) through which the cloud storage is accessed must have active password or equivalent protection.
 - iv. Networks (including home Ethernet or wireless networks) through which the cloud storage is accessed must be encrypted, and have active password protection.
 - v. Employees may not access cloud storage containing internal or restricted data through open, public or unencrypted networks (e.g., Starbucks Wi-Fi access) unless the data communication protocol is encrypted (e.g., sites beginning with https).
- c. District cloud storage will not normally be used for personal data (such as non-work documents, personal photos, or videos), although incidental and/or temporary use may be permitted. Users should be aware that any and all data transmitted or stored using District resources is subject to review by appropriate District personnel.
- d. When using cloud storage for collaboration with others, users shall grant access only to files or folders that are required for the collaboration to take place only for the duration of the collaboration, removing permissions in a timely manner when the collaboration has concluded.
- e. The Vice Chancellor of Educational & Student Support Services or designee is authorized to make exceptions to this Administrative Procedure. Users must contact District IT or college Technology Departments to make an exception request.

4. ADDITIONAL INFORMATION

- a. Employees may contact District IT or college Technology Departments for further guidance on:
 - i. Use of cloud storage consistent with the intent of this Administrative Procedure;
 - ii. Rights and permissions requested by a cloud storage application prior to installation to ensure they do not put SBCCD data or systems at risk of being compromised;
 - iii. Methods of secure access to cloud storage;
 - iv. Designation of data types, and appropriate ways to store that data.
- b. The district will provide opportunities for users to familiarize themselves with the security requirements of the data in their custody to make appropriate, informed decisions about data storage.
- c. District IT and college Technology Services provide technical support only for approved cloud storage (see appropriate technology website for a list of approved cloud storage), LMS, and cloud storage clients or apps, and not personal/public storage such as Dropbox and Box.com.

References: NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, CM-8, SC-5, PE-3, PE-6, PE-20, SC-7, SI-4; HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.312(e)(2)(i), 164.314(b)(2)(i)

End Recommendation for AP 3736 Information Security Cloud Storage

AP

3737 Information Security Payment Card Industry Requirements



Non 10+13 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

Reasons for Review

> New AP resulting from Chapter Lead review of IT security

Level 2 Review Schedule

08/31/24 ♦ Estimated Receipt of Recommendation

09/19/24 ♦ PPAC Approves Review Level

09/20/24 ♦ Level 2 to Constituents and AS for Feedback

10/02/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

10/17/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

11/14/24 ♦ BOT 1st Read

12/13/24 ♦ BOT Final Approval

Begin Recommendation for AP 3737 Information Security Payment Card Industry Requirements

1. PURPOSE AND SCOPE

SBCCD adheres to the requirements of the Payment Card Industry Data Security Standard (PCI). The following additional requirements are mandatory for systems that store, process, or transmit cardholder data. References to the relevant PCI section numbers are in parentheses after each requirement:

2. ACCESS CONTROL

- i. Implementation of an automated access control system (7.1.4).
- ii. The access control system must cover all (PCI) system components (7.2.1).
- iii. The access control system must assign privileges based on job classification and function (7.2.2).
- iv. The access control system must be set to a default “deny all” setting (7.2.3).
- v. Render all passwords unreadable during transmission and storage on all systems components using strong cryptography (8.4).
- vi. Set the lockout duration to a minimum of 30 minutes or until the administrator enables the user ID (8.5.14).
- vii. Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users (8.5.16).

3. PHYSICAL SECURITY

- i. Video cameras must be used to monitor individual physical access to areas where credit card data is stored, processed, or transmitted.
- ii. Physical access to publicly accessible network jacks must be restricted. Network ports for visitors should not be enabled unless network access is explicitly authorized by District IT or college Technology departments.
- iii. Physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines must be restricted to those authorized to work with cardholder data.
- iv. All media containing cardholder data must be physically secured. Media back-ups must be stored in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. These locations must be reviewed at least annually.
 - a. Internal or external distribution of any kind of media must be strictly controlled.
 - b. Media containing cardholder data must be classified so sensitivity of the data can be determined.
 - c. Secure couriers or other delivery methods that can be accurately tracked must be used.



3737 Information Security Payment Card Industry Requirements



Non 10+13 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

- d. Appropriate IT management must approve any and all media that is moved from a secured area (especially when media is distributed to individuals).
- v. Storage and accessibility of media must be strictly controlled. Inventory logs of media must be maintained and inventoried at least annually.
- vi. Media containing credit card data must be destroyed when it is no longer needed for business or legal reasons. a) Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.
- vii. Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.

4. LOGGING AND MONITORING

- i. Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).
- ii. Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting servers.
- iii. Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).

5. INTERNALLY DEVELOPED SYSTEMS CHANGE CONTROL

- Development/test and production environments must be separate.
- Separation of duties between development/test and production environments.
- Production data (live PANs) are not used for testing or development.
- Removal of test data and accounts before production systems become active.
- Change control procedures for the implementation of security patches and software modifications must include the following:
 - Description of the impact of the change.
 - Documented change approval by authorized parties.
 - Functionality testing to verify that the change does not adversely impact the security of the system.
 - Back-out procedures.

6. NETWORK SECURITY

- Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.
- Firewall and router configurations must restrict connections between untrusted networks and any system components in the cardholder data environment. An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.
- Prohibit direct public access between the Internet and any system component in the cardholder data environment. Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.
- Implement a demilitarized zone (DMZ) to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. Limit inbound Internet traffic to IP addresses within the DMZ.
- Install a firewall at each Internet connection and between any DMZ and the internal network zone.
- Do not allow internal addresses to pass from the Internet into the DMZ.
- Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.
- Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)
- Place system components that store cardholder data (such as a database) in an internal network zone.
- Where feasible, implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)
- Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises.
- Never send unprotected primary account numbers (PANs) by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).

AP

3737 Information Security Payment Card Industry Requirements



Non 10+13 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ No Matching BP or AP Exists

- Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:
 - Only trusted keys and certificates are accepted.
 - The protocol in use only supports secure versions or configurations.
 - The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to:
 - The Internet.
 - Wireless technologies, including 802.11 and Bluetooth.
 - Cellular technologies, for example, Global System for Mobile Communications (GSM), and Code Division Multiple Access (CDMA).
 - General Packet Radio Service (GPRS).
 - Satellite communications.

References:

PCI DSS Requirements and Security Assessment Procedures:

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

PCI DSS Quick Reference Guide

Version3.0: https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3.pdf**End Recommendation for AP 3737 Information Security Payment Card Industry Requirements**

BP 5030 Fees



Non 10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Torres ♦ Both BP & AP Exist

Reasons for Review

> FYI only.

Level 2 Review Schedule

- 07/25/2024 ♦ Recommendation Received
- 09/19/2024 ♦ PPAC Approves Review Level
- 09/20/2024 ♦ Level 2 to Constituents and AS for Feedback
- 10/02/2024 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input
- 10/17/2024 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3
- 11/14/2024 ♦ BOT 1st Read
- 12/13/2024 ♦ BOT Final Approval

Begin Recommendation for BP 5030 Fees

The Board of Trustees authorizes the following fees. All fees must comply with Education Code and Title 5 regulations. The Chancellor is responsible for establishing procedures for the collection, deposit, waiver, refund, and accounting for fees as required by law. The procedures shall also assure those who are exempt from or for whom the fee is waived are properly enrolled and accounted for. Fee amounts shall be published in the college catalogs or class schedules (Schedule of Classes).

Enrollment Fee (Education Code Section 76300)

Each student shall be charged a fee for enrolling in credit courses as required by law.

Baccalaureate Degree Program Fees (Title 5 Section 58520)

Each student shall be charged a fee in addition to an enrollment fee for upper division coursework in a baccalaureate degree program.

Course Auditing Fees (Education Code Section 76370)

Persons auditing a course shall be charged a fee (see AP 5030). The fee amount shall be adjusted proportionally based upon the term length. Students enrolled in classes to receive credit for 10 or more semester credit units shall not be charged this fee to audit three or fewer units per semester.

Parking Fee (Education Code Section 76360)

Students shall be required to pay a fee (see AP 5030). To encourage ride sharing, a student may certify in writing at the time of payment of the fee that they regularly have two or more passengers commuting with them.

Instructional Materials (Education Code Section 76365; Title 5 Sections 59400 et seq.)

Students may be required to provide required instructional and other materials for a credit or non-credit course, provided such materials are of continuing value to the student outside the classroom and provided that such materials are not solely or exclusively available from the District. (See BP/AP 5031 titled Instructional Materials Fees)

10/6/2024
/3/2024

BP 5030 Fees



Non 10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Torres ♦ Both BP & AP Exist

Physical Education Facilities (Education Code Section 76395)

Where the District incurs additional expenses because a physical education course is required to use non-district facilities, students enrolled in the course may be charged a fee for participating in the course. Such fee shall not exceed the student's calculated share of the additional expenses incurred by the District.

Student Representation Fee (Education Code Section 76060.5)

Students will be charged a fee (see AP 5030) to be used to provide support for student governmental affairs representation. A student may refuse to pay the fee and shall submit such refusal on a form provided by the District to collect fees.

Student Transportation Costs (Education Code Section 76361)

Students shall be charged a fee (see AP 5030) for the purpose of recovering transportation costs incurred by the District for services provided by common carriers to students. These fees will only be paid by students who use the transportation services, unless a vote of the students in accordance with the Education Code establishes otherwise.

Transcript Fees (Education Code Section 76223)

The District shall charge a reasonable amount for furnishing copies of any student record to a student or former student. The Chancellor is authorized to establish the fee (see AP 5030), which shall not exceed the actual cost of furnishing copies of any student record. No charge shall be made for furnishing up to two transcripts of students' records, or for two verifications of various records. There shall be no charge for searching for or retrieving any student record.

International Students Application Processing Fee (Education Code Section 76142)

The District shall charge students who are both citizens and residents of a foreign country a fee to process their application for admission. This processing fee and regulations for determining economic hardship may be established by the Chancellor. The fee shall not exceed the lesser of 1) the actual cost of processing an application and other documentation required by the U.S. government; or 2) one hundred dollars (\$100), which shall be deducted from the tuition fee at the time of enrollment.

Fee Refunds

The Board of Trustees authorizes refunds to be made according to administrative procedures established by the Chancellor. All refunds must comply with Education Code and Title 5 regulations, and the refund schedule shall be published in the college catalogs and class schedules.

References:

Education Code Section 76300 et seq;
Title 5 Sections 58520;
ACCJC Accreditation Eligibility Requirement 20

End Recommendation for BP 5030 Fees

10/6/2024
13/2024

AP 5030 Fees



Non 10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Torres ♦ Both BP & AP Exist

Reasons for Review

> Per Chapter Lead to incorporate BookSaver Program

Begin Recommendation for AP 5030 Fees

Required fees include:

- Enrollment (Education Code Section 76300 and 76300.5; Title 5 Sections 58500 and 58509)
- Baccalaureate degree program fees (Title 5 Section 58520)

As prescribed by state law.

- Nonresident tuition with these permissive exemptions (Education Code Sections 76140 and 76140.5):

As prescribed by state law and established by the Board of Trustees no later than March 1 for the succeeding fiscal year.

- All nonresident students enrolling for 6 or fewer units; or
- A student who is a citizen and resident of a foreign country who demonstrates financial need and this required exemption (Education Code Section 68130.5);
- All students, other than non immigrant aliens under 8 U.S. Code Section 1101(a)(15), who meet the following requirements:
 - high school attendance in California for three or more years;
 - graduation from a California high school or attainment of the equivalent thereof;
 - registration or enrollment in a course offered for any term commencing on or after January 1, 2002;
 - completion of a questionnaire form prescribed by the California Community Colleges Chancellor's Office verifying eligibility for this nonresident tuition exemption; and
 - in the case of a student without lawful immigration status, the filing of an affidavit that the student has filed an application to legalize their immigration status, or will file an application as soon as they are eligible to do so.
- A nonresident student who enrolls in a credit English as a Second Language (ESL) course at the district and who is any of the following:
 - A recent immigrant, as defined in 8 U.S. Code Section 1101(a)(15);

AP 5030 Fees



Non 10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Torres ♦ Both BP & AP Exist

- A recent refugee, as defined in 8 U.S. Code Section 1101(a)(42); or
- A person who has been granted asylum by the United States, as defined in 8 U.S. Code Section 1158.

This exemption applies only to individuals who, upon entering the United States, settled in California and who have resided in California for less than one year. This exemption applies only to the tuition fee for credit ESL courses.

- Student representation (Education Code Section 76060.5; Title 5 Section 54805)

Fees authorized by law include:

- Non-District physical education facilities (Education Code Section 76395)
- Noncredit courses (Education Code Section 76385)
- Community service courses (Education Code Section 78300)
- Auditing of courses (Education Code Section 76370)
- Instructional materials (Education Code Sections 73365, 81457, and 81458; Title 5 Sections 59400 and 59408)
- Athletic insurance (Education Code Section 70902 subdivision (b)(9))
- Cross-Enrollment with the California State University (CSU) or University of California (UC) (Education Code Section 66753)
- Health (Education Code Section 76355)
- Parking (Education Code Section 76360)
- Transportation (Education Code Sections 76361 and 82305.6)
- Student Center (Education Code Section 76375; Title 5 Section 58510)
- Copies of student records (Education Code Section 76223)
- Dormitory (Education Code Section 81670)
- Child care (Education Code Sections 79121 et seq. and 66060)
- Nonresident capital outlay (Education Code Section 76141)
- Nonresident application processing (Education Code Section 76142)
- Credit for Prior Learning (Education Code Section 76300; Title 5 Section 55050)
- Use of facilities financed by revenue bonds (Education Code Section 81901 subdivision (b)(3))
- Refund processing (Title 5 Section 58508)
- ~~Telephone registration (Education Code Section 70902 subdivision (a))~~

10/6/2024
13/2024

AP 5030 Fees



Non 10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Torres ♦ Both BP & AP Exist

- Physical fitness test (Education Code Section 70902 subdivision (b)(9))
- Instructional Tape Lease/Deposit (Education Code Section 70902 subdivision (b)(9))
- Credit Card Use (Education Code Section 70902 subdivision (b)(9))
- International Student Medical Insurance (Education Code Section 70902 subdivision (b)(9))

Prohibited fees include:

- Late application (CCCCO Student Fee Handbook)
- Add/drop (CCCCO Student Fee Handbook)
- Mandatory student activities (CCCCO Student Fee Handbook)
- Student Identification Cards (CCCCO Student Fee Handbook)
- Student Body Organization (CCCCO Student Fee Handbook)
- Nonresident application (CCCCO Student Fee Handbook)
- For dependents of certain veterans (Education Code Section 66025.3)
- For dependents of certain victims of the September 11, 2001, terrorist attacks (CCCCO Student Fee Handbook)
- For certain recipients of the Medal of Honor and certain children of the recipients of the Medal of Honor (Education Code Section 66025.3)
- For surviving spouses and children of a firefighter employed by the federal government whose duty assignment involved the performance of firefighting services in California (Education Code Section 68120)
- For students who have been exonerated of a crime though writ of habeas corpus or pardon that meet certain conditions (Education Code Section 69000)
- Required or funded services (CCCCO Student Fee Handbook)
- Refundable deposits (CCCCO Student Fee Handbook)
- Distance education (other than the statutorily authorized enrollment fee) (CCCCO Student Fee Handbook)
- Mandatory mailings (CCCCO Student Fee Handbook)
- Rental of practice rooms (CCCCO Student Fee Handbook)
- Apprenticeship courses (Education Code Section 76350)
- Technology fee (CCCCO Student Fee Handbook)
- Late payment fee (Title 5 Sections 58502 and 59410)
- Nursing/healing arts student liability insurance (Title 5 Section 55234)

AP 5030 Fees



Non 10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Torres ♦ Both BP & AP Exist

- Cleaning (CCCCO Student Fee Handbook)
- Breakage (CCCCO Student Fee Handbook)
- Test proctoring (CCCCO Student Fee Handbook)

Collection and Refund of Fees

- A. Associated Students Discount Sticker
 - \$9.50 - CHC
 - \$7.50 - SBVC
- B. Breakage/Lost Property Fee
 - Replacement cost of item(s) broken or lost
- C. Campus Center Fee
 - \$1.00/unit (not to exceed \$10 per fiscal year)
- D. Capital Outlay Fee
 - As allowed by law and approved by the Board of Trustees prior to March 1 for the succeeding fiscal year.
- E. Catalog
 - \$6.00 - purchased on campus
- F. Enrollment Fee
 - \$46.00/unit
- G. Upper Division Coursework Fee
 - \$84/unit
- H. Insufficient Funds Check
 - \$15.00
- I. International Student Application
 - \$25.00 (nonrefundable)
- J. Key Deposit/Replacement
 - \$15.00 plus cost of rekeying if needed (metal/electronic key)
- K. Learning Center Reproduction Fees, SBVC
 - \$0.20 - Laser printout: text, black and white printer
 - \$0.50 - Laser printout: graphics, black and white printer (over ½ page)
 - \$1.00 - Laser printout: graphics and/or text, color

AP 5030 Fees



Non 10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Torres ♦ Both BP & AP Exist

\$2.00 - Scan text or graphics to disk, per scan

L. Library Fines – SBVC/CHC

\$0.10 - Books: per day for 50 days; after 50 days, bill \$5 fine plus the replacement value \$0.25 - Reserve Books/Multimedia: per hour to a maximum of the replacement value of the reserve materials; after 14 days, bill \$5 fine plus the replacement value

\$0.50 - Videos: per day for 50 days; after 50 days, bill \$5 fine plus the replacement value

\$0.10 - Per page for laser printout of Internet, CD ROM, Periodicals

\$2.00 - replacement for lost library card

M. Parking Permit Fees

\$45.00 - one semester (\$25 Promise Grant students)

\$24.00 - summer session

\$3.00 - daily

N. Student Health and Accident Insurance

\$26.00 - per semester (includes \$1.50 accident insurance)

\$22.00 - summer session (includes \$1.50 accident insurance)

\$1.50 - accident insurance only

O. Student Representation

\$2.00

P. Supplemental Health Services Fee

At cost - TB skin test (one-step test)

At cost - All Vaccines

\$25.00 - Physical Exams

\$50.00 - DMV Physical Exams

At cost - Prescription medications

At cost - In-house Lab Tests

At cost - Lab Test sent to external lab

At cost - Optional Medical Procedures

At cost - Optional Medical Supplies

\$ 2.00 per item - Duplication of medical records

At cost - Birth Control Pills

AP 5030 Fees



Non 10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Torres ♦ Both BP & AP Exist

Q. Transcripts/Verification

No cost - First two transcripts

\$10.00 - Additional transcripts

\$20.00 - Immediate requests for transcripts

\$5.00 plus cost - Online transcripts

R. Transportation Fee

Students registering for Spring or Fall semester to pay:

\$9.00 for 6 or more credits/semester

\$8.00 for less than 6 credits/semester

\$6.00 for 6 or more credits/summer

\$5.00 for less than 6 credits/summer

S. Crafton Hills College Recreation Fee

Students registering for CHC for Spring, Fall, or Summer semesters have the option to pay for the use of the aquatic and fitness centers:

\$8.00 per semester

T. Book Rental Program Fee

Students registering for credit courses have the option to participate in the book rental program:

\$20.00 per unit

Fee Refunds

A. Designated Fees

This regulation covers the following fees:

1. Enrollment fee
2. Nonresident tuition
3. Parking fee
4. Health fee
5. Accident Insurance fee
6. Student Services Card fee
7. Student Center fee
8. Student Representation Fee
9. Capital Outlay Fee

AP 5030 Fees



Non 10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Torres ♦ Both BP & AP Exist

10. Student Transportation Fee

B. Conditions

If a refund is requested for parking or student services card fees, the parking decal or the student services card must be attached to the refund request.

C. Military Service Exception

If a student who is a member of an active or reserve military service receives orders compelling a withdrawal from courses, the District shall, upon petition and a copy of received orders of the affected student, refund the entire enrollment fee unless academic credit is awarded.

D. Refund Schedule

This refund schedule applies to all fees listed in Paragraph A, above.

1. Fees collected in error

Fees collected in error will be refunded in their entirety.

2. Class canceled by the college

If a class is canceled by the college, enrollment and/or non-resident tuition fees will be refunded in their entirety. If that cancellation results in a student's withdrawal from the college, refunds of the appropriate fees listed in Paragraph "A" will apply.

3. Withdrawal from the College

a. Enrollment Fee/Nonresident Tuition

If a student withdraws during the first two weeks of a full-term class or during the first 10% of a short-term class, enrollment fees or nonresident tuition fees will be refunded.

b. Parking Fee, Health Fee, Accident Insurance Fee, Student Services Card Fee, Student Center Fee, Student Representation Fee, Capital Outlay Fee, Student Transportation Fee.

In order to be eligible for a refund, a student must withdraw prior to the first day of the term for a full-term class or prior to the first day of instruction for a short-term class.

4. Unit Reduction

If a change of program within the first two weeks of a full-term class or during the first 10% of a short-term class results in a reduction in the number of units taken, the enrollment fee or non-resident fee will be refunded at the per unit cost of the reduction.

5. A student who withdraws from a class or the college after the second week of instruction for a full-term class or the

10/6/2024
10/3/2024

AP 5030 Fees



Non 10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Torres ♦ Both BP & AP Exist

first 10% of a short-term class is not eligible for any refund.

Waiver of Fees

The District will waive campus fees for students participating in the California Virtual Campus (CVC). Students attending online courses through the California Community Colleges online course exchange will be responsible for the tuition of courses.

The District may also waive enrollment fees which were not collected in a previous session where the enrollment fees were not collected as a result of the District's error in awarding a Board of Governors Fee Waiver to an ineligible student and not through the fault of the student, and to collect the enrollment fee would cause the student undue hardship.

References:

Education Code Sections 66025.3, 68120, 70902(b)(9), 76300, and 76300.5

Title 5 Sections 51012, 58520, and 58629

California Community College Chancellor's Office (CCCCO) Student Fee Handbook

ACCJC Accreditation Eligibility Requirement 20

End Recommendation for AP 5030 Fees

BP

6925 Refreshments or Meals Served at Meetings and District Events



Non 10+1 ♦ Non CCLC ♦ Chapter Lead Torres ♦ Both BP & AP Exist

Reasons for Review

>Chapter Lead to retire policy and procedure which is no longer relevant due to more efficient process

Level 2 Review Schedule

07/17/2024 ♦ Recommendation Received

09/19/2024 ♦ PPAC Approves Review Level

09/20/2024 ♦ Level 2 to Constituents and AS for Feedback

10/02/2024 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

10/17/2024 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

11/14/2024 ♦ BOT 1st Read

12/13/2024 ♦ BOT Final Approval

Begin Recommendation for BP 6925 Refreshments or Meals Served at Meetings and District Events

*****RETIRE POLICY & PROCEDURE*****

(Replaces current SBCCD BP 3750)

~~The Board of Trustees authorizes the Chancellor to develop administrative procedures allowing for a limited expenditure of funds for refreshments and/or meals served while conducting District business and District approved Associated Student Club business.~~

-

References:

None

End Recommendation for BP 6925 Refreshments or Meals Served at Meetings and District Events

AP

6925 Refreshments or Meals Served at Meetings and District Events



Non 10+1 ♦ Non CCLC ♦ Chapter Lead Torres ♦ Both BP & AP Exist

Reasons for Review

>Chapter Lead to retire policy and procedure which are no longer relevant due to more efficient process

Begin Recommendation for AP 6925 Refreshments or Meals Served at Meetings and District Events

****RETIRE POLICY & PROCEDURE****

(Replaces current SBCCD AP 3750)

1.—Refreshments and/or Meals

The Board of Trustees authorizes the expenditure of funds for refreshments and/or meals served at District or approved Associated Students meetings and trainings in order to conduct District business or Associated Student Clubs business under the conditions set forth in sections A.1 and A.2.

1.—Attended by Employees and/or Students

For meetings or trainings attended only by employees and/or currently enrolled students are authorized for up to a total \$1000 for that meeting or training. Expenditures in excess of \$1,000 require Board approval prior to the meeting or training. Bottled water for individual use is exempt from the conditions below.

2.—Attended by Employees and/or Students as well as Non-employees or Non-Students

For meetings or training attended by employees, currently enrolled students, and by one or more non-employees and/or non-students of the District, are authorized for up to \$500. Expenditures in excess of a total \$500 for that meeting or training require Board approval prior to the meeting or training.

2.—Refreshments or Meals for events

Events are defined as activities in which non-employees and/or non-students will be or can be attending and/or participating (e.g. job fair, holiday event, recruitment event); or is on a large enough scale to be considered neither a meeting nor training. Any refreshments and/or meals for an event require Board approval prior to the event.

3.—Refreshments or Meals Charged to Grant Funds

Any expenditure for refreshments or meals charged to grant funds must meet the requirements set forth in paragraphs A and B above. In addition, such expenditures must be specifically authorized by the terms and conditions set forth in the grant agreement.

4.—Purchase Order and/or Requisition

Expenditures for refreshments and/or meals must specify on the District purchase order, trust account requisition, or submitted with Cal Card statement reconciliation:

- 1.—The name(s) of the individuals or group name, or general description of the parties, for which the refreshments or meals are to be served.
- 2.—The agenda or purpose of the meeting, training, or event.
- 3.—The location and date of the meeting, training or event.
- 4.—If required by Section A.1, A.2, or B, the Board approval date for the expenditure.

Expenditures for Associated Student accounts must be made in accordance with Board Policy (BP) 5420 titled Associated Students Finance and approved by appropriate person listed within BP 5420.

References:

None

End Recommendation for AP 6925 Refreshments or Meals Served at Meetings and District Events

BP 3250 Institutional Planning



Non 10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Torres ♦ Both BP & AP Exist

Reasons for Review

- > Legal Update 43: The Service updated this policy to align with changes in the Title 5 regulations.
- > Legal Update 44 - Updated to revise the reference to the ACCJC Accreditation Standards and add supporting language pursuant to the 2024 changes in the ACCJC Accreditation Standards.

Level 2 Review Schedule

- 10/06/2024 ♦ Recommendation Received
- 10/17/2024 ♦ PPAC Approves Review Level
- 10/18/2024 ♦ Level 2 to Constituents and AS for Feedback
- 11/06/2024 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input
- 11/21/2024 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3
- 12/13/2024 ♦ BOT 1st Read
- 01/09/2025 ♦ BOT Final Approval

Begin Recommendation for BP 3250 Institutional Planning

The Chancellor shall ensure that the District has and implements a broad-based comprehensive, systematic and integrated system of planning that involves appropriate segments of the college community and is supported by institutional effectiveness research.

The Chancellor shall ensure the Board has an opportunity to assist in developing the general institutional mission and goals for the comprehensive plans. The institution's mission directs resource allocation, innovation, and continuous quality improvement through ongoing systematic planning and evaluation of programs and services.

The institution's mission and goals are the foundation for financial planning. Financial information is disseminated to support effective planning and decision-making and provide opportunities for stakeholders to participate in the development of plans and budgets

The planning system shall include all plans required by law and or policy, including, but not limited to:

- A. Long Range Educational or Academic Master Plan, which shall be updated periodically as deemed necessary by the Board of Trustees
- B. Facilities Plan
- C. Safety Plan
- D. Equal Employment Opportunity Plan
- E. Student equity Plan
- F. Student Success and Support Program Plan
- G. Transfer Center Plan
- H. ~~Cooperative Work Experience Plan~~
- I. Extended Opportunity Programs and Services (EOPS) Plan
- J. District Technology Strategic Plan

The Chancellor shall submit those plans to the Board for which Title 5 requires Board approval.

The Chancellor shall inform the Board about the status of planning and the various plans.

~~The Chancellor shall ensure the Board has an opportunity to assist in developing the general institutional mission and goals for the comprehensive plans.~~

BP 3250 Institutional Planning



Non 10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Torres ♦ Both BP & AP Exist

References:

ACCJC Accreditation Standards [I.B.9, III.B.4, III.C.2, III.D.2, IV.B.3, and IV.D.5 \(formerly I.B\);1.4 and 3.5](#)
Title 5 Sections 51008, 51010, 51027, 53003, 54220, 55080, 55190, ~~55250~~, 55510, and 56270 et seq.

End Recommendation for BP 3250 Institutional Planning

AP 3250 Institutional Planning



Non 10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

> Legal Update 44: The Service updated this procedure to revise the reference to the ACCJC Accreditation Standards pursuant to the 2024 changes in the ACCJC Accreditation Standards.

Begin Recommendation for AP 3250 Institutional Planning

- A. The colleges and District Office, through established committees with representation from faculty, administration, classified staff, and students, will review and recommend planning decisions related to human, physical, technological, and financial resources.

Applying the criteria of accreditation standards, the planning process will be guided by adopted mission, vision, and values and will develop specific goals, objectives, and strategies, which have measurable outcomes and specific accountability.

Action plans will be reviewed and revised annually and approved by the respective planning bodies.
- B. Academic Senate will be the representative body in all academic and professional matters, as defined by Title 5 Section 53200.
- C. Institutional effectiveness research, program reviews, and individual unit plans are utilized in the planning process, which is intended to complement and inform the resource allocation process.
- D. The Board may assist in developing the general institutional mission and goals for the comprehensive plans through a variety of means.
- E. Planning documents will be submitted to the California Community College Chancellor's Office in a timely manner when required.

References:

ACCJC Accreditation Standards ~~I.B.9, III.B.4, III.C.2, III.D.2, IV.B.3, and IV.D.5 (formerly I.B)~~; 1.4 and 3.5
Title 5 Sections 51008, 51010, 51027, 53003, 54220, 55080, 55190, 55510, and 56270 et seq.

End Recommendation for AP 3250 Institutional Planning

BP 4010 Academic Calendar



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

> FYI Only: No Changes

Level 3 Review Schedule

10/06/2024 ♦ Recommendation Received

10/17/2024 ♦ PPAC Approves Review Level

10/18/2024 ♦ Level 2 to Constituents and AS for Feedback

11/06/2024 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

11/21/2024 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

12/04/2024 ♦ AS Reviews Level 3 for Final Input

12/20/2024 ♦ PPAC Reviews Final AS Input

01/09/2025 ♦ BOT 1st Read

02/13/2025 ♦ BOT Final Approval

Begin Recommendation for BP 4010 Academic Calendar

The Chancellor shall, in consultation with the appropriate groups, develop an annual academic calendar.

Reference:

Education Code Section 70902(b)(12)

End Recommendation for BP 4010 Academic Calendar

AP 4010 Academic Calendar



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

> Legal Update 44 - Updated to identify optional language pursuant to changes in the Education Code.

Begin Recommendation for AP 4010 Academic Calendar

The traditional academic calendar is composed of at least 175 scheduled days of instruction and evaluation. Mandated holidays are determined by the State Chancellor's Office. The Board of Trustees may declare other days to be holidays and close the colleges and offices when good reason exists.

A districtwide subcommittee meets to coordinate the academic calendar for the District. The deliberations from this subcommittee are shared with the Academic Senates for both colleges before they are reported to the Institutional Effectiveness Advisory Committee (IEAC). The IEAC will review recommendations and submit to the Chancellor's Council and Chancellor for approval followed by Board action.

Holidays include:

New Year's Day (January 1)
 Dr. Martin Luther King, Jr. Day (third Monday in January)
 Lincoln Day (February 12 or see note below)
 Washington Day (third Monday in February)
 Memorial Day (last Monday in May)
 Juneteenth (June 19)
 Independence Day (July 4)
 Labor Day (first Monday in September)
 Veterans Day (November 11)
 Thanksgiving Day (fourth Thursday in November)
 Christmas Day (December 25)

The following are local options if collectively bargained (Education Code Sections 79020 subdivision (k); 79020 subdivision (l), 79020 subdivision (m), and 79020 subdivision (n):

- Cesar Chavez Day ~~and~~
- Native American Day
- Genocide Remembrance Day (April 24)
- Lunar New Year

Lincoln Day is selected from the dates provided by the State Chancellor's Office.

Other Holidays—The Board of Trustees may declare other days to be holidays and close the colleges and offices when good reason exists. (These holidays traditionally have been New Year's Eve day, the day after Thanksgiving, and Christmas Eve day.)

References:

Education Code Sections 79020; ~~and 88203~~;
 Title 5 Sections 55700 et seq. and Section 58142

AP 4010 Academic Calendar



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

End Recommendation for AP 4010 Academic Calendar

BP

4020 Program, Curriculum, and Course Development



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

> Legal Update 44 - Updated to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards.

Level 3 Review Schedule

10/06/2024 ♦ Recommendation Received

10/17/2024 ♦ PPAC Approves Review Level

10/18/2024 ♦ Level 2 to Constituents and AS for Feedback

11/06/2024 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

11/21/2024 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

12/04/2024 ♦ AS Reviews Level 3 for Final Input

12/20/2024 ♦ PPAC Reviews Final AS Input

01/09/2025 ♦ BOT 1st Read

02/13/2025 ♦ BOT Final Approval

Begin Recommendation for BP 4020 Program, Curriculum, and Course Development

The programs and curricula of the District shall be of high quality, relevant to community and student needs, and evaluated regularly to ensure quality and currency. To that end, the Chancellor shall establish procedures for the development and review of all curricular offerings, including their establishment, modification, or discontinuance.

Furthermore, these procedures, following the guidelines of Title 5, shall include:

- appropriate involvement of the faculty and Academic Senate in all processes;
- regular review and justification of programs and course descriptions;
- opportunities for training for persons involved in aspects of curriculum development; and
- consideration of job market and other related information for career and technical education programs.

The Board acknowledges that District faculty, the college curriculum committees, and the college Academic Senates have the shared responsibility to ensure that curriculum review committee members and discipline experts work together to provide Diversity, Equity, Inclusion, and Anti-Racism (DEIA) frameworks and principles in curriculum review and approval processes for credit and noncredit, including programs and curricula in ethnic studies that encompass instruction and infusion of perspectives of African American, Asian American, Native American, and Latinx people. The curriculum process is supported by Administrators and classified professionals throughout the District who will collaborate to work with faculty to implement equity-minded practices.

All new programs and program discontinuances shall be approved by the Board of Trustees.

BP

4020 Program, Curriculum, and Course Development



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

All new programs shall be submitted to the California Community College Chancellor's Office for approval as required.

Individual degree-applicable credit courses offered as part of a permitted educational program shall be approved by the Board. Non-degree-applicable credit and degree-applicable courses that are not part of an existing approved program must satisfy the conditions authorized by Title 5 regulations and shall be approved by the Board.

Credit Hour

Consistent with federal regulations applicable to federal financial aid eligibility, the District shall assess and designate each of its programs as either a "credit hour" program or a "clock hour" program.

The Chancellor shall establish procedures:

- which prescribe the definition of "credit hour" consistent with applicable federal regulations, as they apply to community college districts.
- to assure that curriculum at the District complies with the definition of "credit hour" or "clock hour," where applicable.
- for using a clock-to-credit hour conversion formula to determine whether a credit hour program is eligible for federal financial aid. The conversion formula is used to determine whether such a credit hour program has an appropriate minimum number of clock hours of instruction for each credit hour it claims.

References:

Education Code Sections 70901(b), 70902(b), and 78016; Title 5 Sections 51000, 51022, 55002.5, 55100, 55130 and 55150; U.S. Department of Education regulations on the Integrity of Federal Student Financial Aid Programs under Title IV of the Higher Education Act of 1965, as amended; 34 Code of Federal Regulations Sections 600.2, 602.24, 603.24, and 668.8; ACCJC Accreditation Standards [II.A](#) and [II.A.9 2](#)

End Recommendation for BP 4020 Program, Curriculum, and Course Development

AP

4020 Program, Curriculum, and Course Development



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

- > Legal Update 44 - Updated to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards.
- > Legal Update 43: The Service updated this procedure to clarify that Title 5 regulations require districts to develop and offer programs and curricula in ethnic studies, but districts have the option to develop and offer programs and curricula that infuse a global perspective into the curricular offerings and programs and curricula that include instruction on the perspectives of persons with low socioeconomic status in the topic.
- > Legal Update 42: The Service updated this procedure to align with updated Title 5 regulations.

Begin Recommendation for AP 4020 Program, Curriculum, and Course Development

Note: This procedure is legally required in an effort to show good faith compliance with the applicable federal regulations

District faculty, the college curriculum committees, and the college Academic Senates have the shared responsibility to ensure that curriculum review committee members and discipline experts work together to provide Diversity, Equity, Inclusion, and Anti-Racism (DEIA) frameworks and principles in curriculum review and approval processes for credit and noncredit, including programs and curricula in ethnic studies that encompass instruction and infusion of perspectives of African American, Asian American, Native American, and Latinx people. The curriculum process is supported by Administrators and classified professionals throughout the District who will collaborate to work with faculty to implement equity-minded practices.

Curriculum development procedures for each college are developed by the campus curriculum committees under the purview of the academic senates. The respective curriculum handbooks prepared and revised by each campus committee are posted on the college's curriculum committee webpage.

- One hour of classroom or direct faculty instruction and a minimum of two hours of out of class student work each week for approximately [15 weeks for one semester or trimester hour of credit], [or 10 to 12 weeks for one quarter hour of credit], or the equivalent amount of work over a different amount of time; or
- At least an equivalent amount of work as required in the paragraph above, of this definition for other academic activities as established by the institution including laboratory work, internships, practica, studio work, and other academic work leading to the award of credit hours.

[The District shall develop and offer programs and curricula in ethnic studies. The District shall develop programs and curricula that infuse a global perspective into the curricular offerings, and programs and curricula that include instruction on the perspectives of persons with low socioeconomic status in the topic.](#)

Curriculum development procedures for each college in the District are documented in the respective curriculum handbooks prepared by each campus.

Faculty, the college curriculum committees, and the college Academic Senates have the shared responsibility to ensure that Ethnic Studies course materials and curriculum:

- Are written by and for Native American, Black and African American, Latinx, and Asian American communities rather than only about those communities.
- Address structural and institutional racism, discrimination, oppression, and privilege.
- Focus on the eleven principles of Ethnic Studies:
 1. Love
 2. Respect
 3. Reflection

AP

4020 Program, Curriculum, and Course Development



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

- 4. Hope
- 5. Solidarity
- 6. Critical Consciousness
- 7. Community
- 8. Interconnection
- 9. Wellness
- 10. Healing
- 11. Transformation

References:

Title 5 Sections 51021, 55000 et seq., and 55100 et seq.;

34 Code of Federal Regulations Part 600.2; ACCJC Accreditation Standard [II.A; 2](#)

U.S. Department of Education regulations on the Integrity of Federal Student Financial Aid Programs under Title IV of the Higher Education Act of 1965, as amended.

End Recommendation for AP 4020 Program, Curriculum, and Course Development

BP

4100 Graduation Requirements for Degrees and Certificates



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

- > At 5/13/2024 PPAC, the impact of Legal Update 44 on the recommendation was substantial and it was decided to bring this item to 2024-25 as a new recommendation.
- > Legal Update 44: Updated to remove the requirement regarding publishing graduation requirements in the District's catalog pursuant to changes in the Title 5 regulations.
- > Chapter Lead suggestions

Level 3 Review Schedule

- 10/06/2024 ♦ Recommendation Received
- 10/17/2024 ♦ PPAC Approves Review Level
- 10/18/2024 ♦ Level 2 to Constituents and AS for Feedback
- 11/06/2024 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input
- 11/21/2024 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3
- 12/04/2024 ♦ AS Reviews Level 3 for Final Input
- 12/20/2024 ♦ PPAC Reviews Final AS Input
- 01/09/2025 ♦ BOT 1st Read
- 02/13/2025 ♦ BOT Final Approval

Begin Recommendation for BP 4100 Graduation Requirements for Degrees and Certificates

~~(Replaces current SBCCD BP 4100)~~

The District grants the degrees of Associate in Arts, Associate in Arts-Transfer, Associate in Science and Associate in Science-Transfer to those students who have completed the subject requirements for graduation. ~~The District also grants Certificates of Achievement and Certificates of Completion. and who have maintained a 2.0 grade point average in degree applicable courses/subjects attempted unless otherwise stipulated by the major. Students must also complete the general education residency and competency requirements set forth in Title 5 regulations and Education Code.~~

~~Students may be awarded a Certificate of Achievement upon successful completion with a grade of C or higher of a minimum of 16 or more semester units or 27 or more quarter units of degree applicable coursework designed as a pattern of learning experiences designed to develop certain capabilities that may be oriented to career or general education.~~

The Chancellor shall establish procedures to determine degree and certificate requirements that include appropriate involvement of the local curriculum committee. ~~The procedures shall assure that graduation requirements are published in the college catalog(s) and included in other resources that are convenient for students.~~

References:

Education Code Section ~~66746 (a) and (b)~~, 70902 subdivision (b)(3);
Title 5, Sections ~~55002(b), 55070, 55800, et seq.~~ 55060 et seq.

End Recommendation for BP 4100 Graduation Requirements for Degrees and Certificates

AP

4100 Graduation Requirements for Degrees and Certificates



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

- > At 5/13/2024 PPAC, the impact of Legal Update 44 on the recommendation was substantial and it was decided to bring this item to 2024-25 as a new recommendation.
- > Legal Update 44: Updated to revise associate degree requirements to align with changes in the Title 5 regulations.
- > Legal Update 42: The Service updated this procedure to align with updated Title 5 regulations.
- > Legal Update 40: The Service updated this procedure to reflect new Title 5 Regulations regarding direct assessment competency-based education. (2022-23 carryover)

Begin Recommendation for AP 4100 Graduation Requirements for Degrees and Certificates

(Replaces current SBCCD AP 4100)

Graduation Requirements for Degrees and Certificates

~~for graduating with a~~ Degree or Certificate ~~graduation requirements~~ are developed through collegial consultation on each campus, approved by the Board of Trustees, and published in the respective college catalogs.

For ~~the Associate in Arts or Associate in Science~~ Degrees (AA/AS), the requirements include: ~~a student must~~

- ~~D~~emonstrate competence in reading, in written expression, and in mathematics.
- ~~The student must~~ satisfactorily complete at least 60 semester units of college work and have maintained a 2.0 grade point average in subjects attempted unless otherwise stipulated by the major. Students must also complete the general education residency and competency requirements set forth in Title 5 regulations and Education Code.
- Complete least 18 semester units in general education and at least 18 semester units in a major listed in the State Chancellor's Taxonomy of Programs.
- Complete at least 12 semester units of study in residence; exceptions to the residence requirement can be made by the Governing Board when an injustice or under hardship would result.
- Complete a minimum of general education course work in the natural sciences, the social and behavioral sciences, humanities and language and rationally..

College work includes all courses acceptable toward the associate degree that have been properly approved pursuant to Title 5 Section 55002(a), or, if completed at other than a California community college, would reasonably be expected to meet the standards of that section.

~~The work must include at least 18 semester units in general education, (Note: SBVC requires at least 24 units) and at least 18 semester units in a major listed in the Community Colleges "Taxonomy of Programs".~~

~~The work must include at least 12 semester units of study in residence; exceptions to the residence requirement can be made by the Scholastic Standards Committee when an injustice or undue hardship would result.~~

~~The general education requirements must include a minimum of work in the natural sciences, the social and behavioral sciences, humanities, and language and rationality, (note: ethnic studies must be offered in at least one of these four areas), communication and analytical thinking, and lifelong learning and self-development as applicable. In addition, the general education transfer requirements may apply.~~

Students may petition to have noncredit courses counted toward the satisfaction of requirements for an associate degree.

The District must offer ethnic studies as part of the general education curriculum.

District policies and procedures regarding general education and degree requirements must be published in the college catalog and must be filed with the State Chancellor's Office.

AP

4100 Graduation Requirements for Degrees and Certificates



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Certificates

Successful completion of a course of student or curriculum that consists of 16 or more semester units of degree-applicable credit coursework for a certificate of achievement shall be designed to demonstrate that the students has completed coursework and developed capabilities relating to a career or general pathway.

~~For a certificate of achievement, a student must successfully complete a course of study or curriculum that consists of 16 or more semester units of degree-applicable credit coursework. The certificate of achievement shall be designed to demonstrate that the student has completed coursework and developed capabilities relating to career or general education.~~

Requirements for the District include:

- Shorter credit programs that lead to a certificate may be established by the District.
- Content and assessment standards for certificates shall ensure that certificate programs at either college are consistent with the mission of the college, meet a demonstrated need, are feasible, and adhere to guidelines on academic achievement.
- The District may obtain approval of a direct assessment competency-based program from the California Community College Chancellor's office.

~~Certificates for which State Chancellor's Office approval is not sought may be given any name or designation deemed appropriate except for certificate of achievement, certificate of completion, or certificate of competency.~~

References:

[Education Code Section 70902\(b\)\(3\):](#)

Title 5, Sections [55070, 55800, et seq.](#) 55060 et seq. [and 55270 et seq.](#)

End Recommendation for AP 4100 Graduation Requirements for Degrees and Certificates



4230 Grading and Academic Record Symbols



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

> Per discussion at 5/13/2024 PPAC requesting Chapter Lead clarification of "Intervention Program" and the impact of the "FW" grade.
 > Legal Update 39: The Service updated this policy to reflect additions to Title 5 Regulations requiring districts to grant students credit for satisfactory completion of International Baccalaureate or College Level Examination Program examinations and requiring districts to ensure that students' academic records clearly annotate credit earned through such examinations. (Title 5 Section 55052.5) To the extent that districts grant students prior credit for successful completion of other prior learning experiences or examinations, such as Advanced Placement examinations, the Service recommends that districts use the same academic record symbol. (2022-23 carryover)

Level 3 Review Schedule

10/06/2024 ♦ Recommendation Received
 10/17/2024 ♦ PPAC Approves Review Level
 10/18/2024 ♦ Level 2 to Constituents and AS for Feedback
 11/06/2024 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input
 11/21/2024 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3
 12/04/2024 ♦ AS Reviews Level 3 for Final Input
 12/20/2024 ♦ PPAC Reviews Final AS Input
 01/09/2025 ♦ BOT 1st Read
 02/13/2025 ♦ BOT Final Approval

Begin Recommendation for BP 4230 Grading and Academic Record Symbols

~~(Replaces current SBCCD BP 4230, BP 4232, and BP 4233)~~

Courses shall be graded using the grading system established by Title 5.

The grading system shall be published in the college catalogs and made available to students.

~~Withdrawal/Military Withdrawal~~

~~The grading symbols used in the District shall include Withdrawal. The Chancellor is responsible for establishing administrative procedures to implement this policy specifying when it may be assigned.~~

Reference:

Title 5 Section 55023 [and 55050 et seq.](#)

End Recommendation for BP 4230 Grading and Academic Record Symbols

AP 4230 Grading and Academic Record Symbols



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

- > Per discussion at 5/13/2024 PPAC requesting Chapter Lead clarification of "Intervention Program" and the impact of the "FW" grade.
- > Legal Update 42: The Service updated this procedure to align with updated Title 5 regulations.
- > Legal Update 39: The Service updated this procedure to reflect additions to Title 5 Regulations requiring districts to grant students credit for satisfactory completion of International Baccalaureate or College Level Examination Program examinations and requiring districts to ensure that students' academic records clearly annotate credit earned through such examinations. (Title 5 Section 55052.5) To the extent that districts grant students prior credit for successful completion of other prior learning experiences or examinations, such as Advanced Placement examinations, the Service recommends that districts use the same academic record symbol for such purposes. (2022-23 carryover)

Begin Recommendation for AP 4230 Grading and Academic Record Symbols

(Replaces current SBCCD AP 4230, AP 4232, and AP 4233)

Grade assignments can only be made by an instructor. Grades assigned are final except in cases of mistake, fraud, bad faith, or incompetence. No grade will be changed for any reason or under any circumstance after three (3) years from the end of the term in which the grade was assigned. The following evaluative and non-evaluative symbols shall be used to denote a student's academic progress.

1.

Evaluative Symbols

Symbol	Definition	Grade Points
A	Excellent	4
B	Good	3
C	Satisfactory	2
D	Less than Satisfactory	1
F	Failing	0
FW	Failing Withdrawal	0
P	Passing (at least Satisfactory) - units awarded not counted in GPA	0
NP	No Pass (less than Satisfactory, or failing – units not counted in GPA)	0
SP	Satisfactory Progress towards completion of the course (Used for noncredit courses only and is not supplanted by any other symbol)	0
SP	Satisfactory Progress towards completion of the course (used for noncredit courses only and is not supplanted by any other symbol)	

2. ~~Non-Evaluative Symbols~~

Symbol	Definition
I	Incomplete
W	Withdrawal
MW	Military Withdrawal
IP	In Progress
RD	Report Delayed



4230 Grading and Academic Record Symbols



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Incomplete

The grading symbols used in the District shall include Incomplete. The Chancellor is responsible for establishing administrative regulations to implement this policy specifying when it may be assigned and how it may be removed.

Failing Withdrawal

The use of the "FW" grade symbol to indicate that a student has both ceased participating in a course some time after the last day to officially withdraw from the course without having achieved a final passing grade, and that the student has not received district authorization to withdraw from the course under extenuating circumstances. The "FW" symbol may not be used if a student has qualified for and been granted military withdrawal. If "FW" is used, its grade point value shall be zero (0).

Non-Evaluative Symbols

I – Incomplete: Incomplete academic work for unforeseeable, emergency and justifiable reasons. The condition for the removal of the "I" shall be stated by the instructor in a written record. The record shall contain the conditions for the removal of the "I" and the grade assigned in lieu of its removal. The record must be given to the student with a copy on file with the registrar until the "I" is made up or the time limit has passed. A final grade shall be assigned when the work stipulated has been completed and evaluated, or when the time limit for completing the work has passed. The "I" may be made up no later than one year following the end of the term in which it was assigned. The "I" symbol shall not be used in calculating units attempted nor for grade points.

IP – In Progress: The "IP" symbol shall be used only in courses that extend beyond the normal end of an academic term. It indicates that work is "in progress," but that assignment of an evaluative symbol (grade) must await its completion. The appropriate evaluative symbol (grade) and unit credit shall be assigned and replace the IP symbol once the course is completed.

RD – Report Delayed: The "RD" symbol may be assigned by the registrar only. It is to be used when there is a delay in reporting the grade of a student due to circumstances beyond the control of the student. It is a temporary notation to be replaced by a permanent symbol as soon as possible. "RD" shall not be used in calculating grade point averages.

W – Withdrawal: The "W" symbol may be used to denote withdrawal in accordance with the requirements of Title 5 Section 55024.

MW – Military Withdrawal: The "MW" symbol may be used to denote military withdrawal in accordance with Title 5 Section 55024.

EW – Excused Withdrawal: The "EW" symbol may be used to denote withdrawal in accordance with Title 5 Section 55024.

Refer to Administrative Procedure 5075 Course add, drops, and withdrawals for more information.

CPL- Credit for Prior Learning

The "CPL" symbol may be used to denote credit earned through successful completion of International Baccalaureate (IB), College Level Examination Program (CLEP), Advanced Placement (AP) examinations, or other prior learning experiences, in accordance with Title 5 Section 55052.5. The district shall ensure that students' academic records clearly annotate credit earned through these experiences. The same academic record symbol, "CPL", shall be used for all prior learning credits to maintain consistency.

A. Assignment of Grade

The Incomplete grade may be assigned at the discretion of the instructor when a substantial portion of the class work has been completed by the student but some part of student's work remains to be completed at the end of the term.

B. Removal of Grade

In order to have the Incomplete removed from ~~his/her~~ their record, a student must complete the work as prescribed by the instructor of record

AP

4230 Grading and Academic Record Symbols



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

within one year of the end of the term in which it was assigned.

C. Conditions for Removal of Grade

Each instructor shall provide an Incomplete Grade Report form for each student whose work is incomplete. The instructor will indicate what the student must do to complete the course and what grade the student will receive if the work is not completed in the time prescribed by this procedure.

D. Records Requirement

The Records Office will notify students of an incomplete grade and will keep a copy of the form on file. The instructor will also keep a copy of the form on file.

Reference: Title 5 Section 55023, [55024](#), [55051](#), [55052](#), and [55052.5](#).

End Recommendation for AP 4230 Grading and Academic Record Symbols

BP 5012 International Students



10+1 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

> Chapter Lead recommendation to adopt.

Level 3 Review Schedule

- 10/06/2024 ♦ Recommendation Received
- 10/17/2024 ♦ PPAC Approves Review Level
- 10/18/2024 ♦ Level 2 to Constituents and AS for Feedback
- 11/06/2024 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input
- 11/21/2024 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3
- 12/04/2024 ♦ AS Reviews Level 3 for Final Input
- 12/20/2024 ♦ PPAC Reviews Final AS Input
- 01/09/2025 ♦ BOT 1st Read
- 02/13/2025 ♦ BOT Final Approval

Begin Recommendation for AP 5012 International Students

The District admits international students in approved study programs in accordance with regulations established by the United States Bureau of Citizenship and Immigration Service. The District will maintain specific admission criteria, requirements, and procedures that govern the selection of international student applicants for admission.

End Recommendation for AP 5012 International Students

AP 5012 International Students



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

> SBCCD has not yet adopted this legally required process. This needs to be reviewed and adopted.

Level 3 Review Schedule

10/06/2024 ♦ Recommendation Received

10/17/2024 ♦ PPAC Approves Review Level

10/18/2024 ♦ Level 2 to Constituents and AS for Feedback

11/06/2024 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

11/21/2024 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

12/04/2024 ♦ AS Reviews Level 3 for Final Input

12/20/2024 ♦ PPAC Reviews Final AS Input

01/09/2025 ♦ BOT 1st Read

02/13/2025 ♦ BOT Final Approval

Begin Recommendation for AP 5012 International Students

Enrollment Process for Prospective International (F-1) Students

Prospective students shall submit an international application package that includes the following documents:

- High School diploma, or proof of high school graduation.
- Submit a district application via CCCApply and an International Student Application which includes a processing fee.
- California Department of Health Tuberculosis Risk Assessment. Submit TB Risk Assessment and TB test result (dated within the past 6 months) or get tested at the campus Student Health Services.
- If the student's home country's official language is not English, applicants must provide of English language proficiency demonstrated by the Test of English as a Foreign Language (TOEFL) score of 45-46 on the internet-based exam or by the International Testing System (IELTS) band score of 5.0.
- English proficiency may also be demonstrated through the following proficiency waivers: 1) High/Secondary school completion in countries where English is the primary language of Instruction. 2) Completion of 3+ years at an international high/secondary school where English is the primary language of instruction. 3) Completed college-level English at a College or University where English is the primary of Instruction.
- Official transcript(s) or official academic records from high school and college/university attended, accompanied by a notarized translation if the originals are not in English. Applicants with higher education need to have a minimum of C grade average from college/university in order to be considered for admission.
- Financial documents and bank certification letter showing proof of sufficient funds to cover a minimum of one year of studies. This includes the financial ability to obtain housing.
- Affidavit of Support Form (for sponsors outside of the US to complete).

AP 5012 International Students



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

- I-134/Affidavit of Support and Instructions for Form I-134 (for sponsors in the US to complete)

Additional requirements:

- Applicants applying for Admissions who currently hold an F-1 visa are considered “Transfer” International Students. In addition to the requirements stated for prospective applicants, international transfer students must provide a copy of current passport, Visa with an I-94 stamp and current Form I-20.
- Students who will be attending pursuant to an F-1 visa, submission of paperwork to substantiate issuance by the District of Form I-20.
- Exemptions from nonresident tuition as authorized by Education Code Section 76140 subdivision (a)(2) for financial need.
- Students must complete the college’s general application through CCC Apply.

If an applicant is admitted to the college, a letter of acceptance and an I-20 Form (used to apply for a student visa in an American embassy) will be mailed to the applicant.

International student program rules:

- Must enroll in a minimum of twelve (12) units per semester (Spring and Fall semesters) to maintain full-time status for their F-1 visa but may choose to enroll in more than twelve (12) units at current non-resident rate per unit. Enrolling in summer courses is optional.
- Must maintain a minimum of a 2.0 GPA at all times.
- Maintain a current passport valid for at least six months into the future at all times.
- Request authorization from the Designated School Official before dropping below full-time enrollment.
- Report all address changes within 10 days.
- Report a change in program of study to the Designated School Official and request a new I-20.
- Request transferring to another accredited school as soon as possible.
- Request travel signature before you depart the US.
- Request an I-20 Extension at least two weeks before the program end date.
- Maintain valid medical insurance during your attendance at the college.

International Student Employment

F-1 Students may not work off campus during the first academic year but may accept on-campus employment subject to certain conditions and restrictions. After the first academic year, F-1 students may engage in three types of, off campus employment:

- Curricular Practical Training (CPT)
- Optional Practical Training (OPT) (pre-completion)
- Science, Technology, Engineering, Mathematics (STEM) Optional Practical Training Extension (OPT)

F-1 students may also be eligible to work off campus on a case-by-case result of special situations such as severe economic hardship or special student relief.

Fee Assessment:

- Nonresident Tuition: All international students will be charged nonresident tuition for each unit of credit coursework they enroll in.
- Capital Outlay fee may also be charged to cover infrastructure costs. This fee shall not exceed 50% of the nonresident tuition fee in accordance with Education Code Section 76141
- Student Services fee: international students are required to pay all regular college fees applicable to non-resident students, including health services, student representation and technology fees, as outlined in AP 5030 (Fees)
- Health Insurance: international students must purchase a medical insurance plan that is approved by the District and maintain this insurance throughout their period of study.

AP 5012 International Students



10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Exemptions: International students will be exempt from paying international student application fee in case of demonstrated economic hardship, as defined by the California Education Code section 76142. Additionally, students exempt from paying nonresident tuition as per Education Code section 76140 will also be exempt from paying the international student application fee.

References:

- Education Code Sections 76141 and 76142;
- Title 5 Section 54045;
- Title 8 U.S. Code Sections 1101 et seq.

End Recommendation for AP 5012 International Students



5035 Withholding of Student Records



10+1 ♦ CCLC | Legally Advised ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

> Legal Update 42: The Service updated this policy to include an additional citation to the Education Code and clarify when a district may withhold registration privileges or transcripts.

Level 3 Review Schedule

- 10/06/2024 ♦ Recommendation Received
- 10/17/2024 ♦ PPAC Approves Review Level
- 10/18/2024 ♦ Level 2 to Constituents and AS for Feedback
- 11/06/2024 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input
- 11/21/2024 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3
- 12/04/2024 ♦ AS Reviews Level 3 for Final Input
- 12/20/2024 ♦ PPAC Reviews Final AS Input
- 01/09/2025 ♦ BOT 1st Read
- 02/13/2025 ♦ BOT Final Approval

Begin Recommendation for BP 5035 Withholding of Student Records

Students or former students who have been provided with written notice that they have failed to pay a proper financial obligation may have registration privileges withheld until the outstanding obligation is paid or otherwise settled.

District must provide a student or former student with written notice that he/she/they have failed to pay a financial obligation due to the District before the District commences any activity to collect the debt.

The District may not withhold grades or transcripts for a student or former student as a consequence of the student's outstanding financial obligation to the District. The District may not withhold registration privileges for a student or former student as a consequence of defaulting on a loan or loans under the Federal Family Education Loan Program only. The District may withhold diplomas as a consequence for a student or former student of defaulting on a loan.

Reference:

Education Code Section 66022:
Title 5 Section 59410

End Recommendation for BP 5035 Withholding of Student Records

AP**5035 Withholding of Student Records**

10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

> FYI Only

Begin Recommendation for AP 5035 Withholding of Student Records

The Director of Admissions & Records or designee may withhold registration privileges from any student or former student who fails to pay a proper financial obligation to the District. The student shall be given written notification and the opportunity to explain if the financial obligation is in error.

The definition of proper financial obligation shall include, but is not limited to: student fees; obligations incurred through the use of facilities, equipment or materials; library fines; unreturned library books; materials remaining improperly in the possession of the student; and/or any other unpaid obligation a student or former student owes to the District. A proper financial obligation does not include any unpaid obligation to a student organization.

For additional information see Board Policy/Administrative Procedure 5030 Fees or visit the campus websites.

Reference:

Title 5 Section 59410

End Recommendation for AP 5035 Withholding of Student Records

BP**5055 Enrollment Priorities**

10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

> FYI only to support Legal Update 43 review of AP.

Level 3 Review Schedule

10/06/2024 ♦ Recommendation Received

10/17/2024 ♦ PPAC Approves Review Level

10/18/2024 ♦ Level 2 to Constituents and AS for Feedback

11/06/2024 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

11/21/2024 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

12/04/2024 ♦ AS Reviews Level 3 for Final Input

12/20/2024 ♦ PPAC Reviews Final AS Input

01/09/2025 ♦ BOT 1st Read

02/13/2025 ♦ BOT Final Approval

Begin Recommendation for BP 5055 Enrollment Priorities

All courses of the District shall be open to enrollment, subject to a priority system that may be established. Enrollment also may be limited to students meeting properly validated prerequisites and co-requisites, or due to other, practical considerations.

The Chancellor is responsible for establishing procedures defining enrollment priorities, limitations, and processes for student challenge, which shall comply with Title 5 regulations.

References:

Title 5, Sections 51006, 58106; and 58108

End Recommendation for BP 5055 Enrollment Priorities

AP 5055 Enrollment Priorities



10+1 ♦ CCLC | Good Practice/Optional ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

- > Legal Update 43: The Service updated this procedure to align with revised Title 5 regulations
- > Legal Update 42: The Service updated this procedure to include an additional category of students eligible for priority for enrollment pursuant to changes in the Education Code.

Begin Recommendation for AP 5055 Enrollment Priorities

Enrollment in courses and programs may be limited to students meeting properly established prerequisites and co-requisites. (See BP and AP 4260 titled Prerequisites and Co-requisites.)

Enrollment may be limited due to the following:

- health and safety considerations;
- facility limitations;
- faculty workload;
- availability of qualified instructors;
- funding limitations;
- regional planning;
- legal requirements; and
- contractual requirements.

The District will provide priority registration for students who enroll in a community college for the purpose of degree or certificate attainment, transfer to a four-year college or university, or career advancement.

The following students will have the highest and equal priority for enrollment:

- A member of the armed forces or a veteran pursuant to Education Code section 66025.8
- A foster youth, former foster youth, or homeless youth pursuant to Education Code section 66025.9;
- A student who has been determined to be eligible for Student Accessibility Services or Extended Opportunity Programs and Services; and
- A student who is receiving services through CalWORKS;
- A student parent who has a child or children under 18 years of age who will receive more than half of their support from that student;
- A verified homeless youth or former homeless youth under 25 years of age at the commencement of the academic year, as specified in Education Code Section 66025.9;

The following students will have priority for enrollment:

- First time students who have completed orientation, assessment, and developed student education plans.
- Continuing students, who has not lost registration priority, as defined in these policies and procedures.

Registration priority specified above shall be lost at the first registration opportunity after a student:

- Is placed on academic or progress probation or any combination thereof as defined in these Board Policy and Administrative Procedure 4250 for two consecutive terms; or
- Has earned one hundred (100) or more degree-applicable semester or quarter equivalent units at the district.

AP

5055 Enrollment Priorities



10+1 ♦ CCLC | Good Practice/Optional ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

For purposes of this section a unit is earned when a student receives a grade of A, B, C, D or P as defined in Board Policy and Administrative Procedure 4230. This 100-unit limit does not include units for non-degree applicable English as a Second Language or basic skills courses as defined by the Vice President of Instruction, or students enrolled in high unit majors or programs as designated by the Vice President of Instruction.

The District shall notify students who are placed on academic or progress probation, of the potential for loss of enrollment priority.

The District shall notify the student that a second consecutive term on academic or progress probation will result in the loss of priority registration as long as the student remains on probation. The District shall notify students or who have earned 75 percent or more of the unit limit, that enrollment priority will be lost when the student reaches the unit limit.

Appeal of Loss of Enrollment Priority

Students may appeal the loss of enrollment priority when the loss is due to extenuating circumstances. Extenuating circumstances are verified cases of accidents, illnesses or other circumstances beyond the control of the student, or when a student with a disability applied for, but did not receive a reasonable accommodation in a timely manner. The Director of Admission and Records or his/her designee will determine the appeal in his/her sole discretion.

[Note: Districts may allow students who have demonstrated significant academic improvement to appeal the loss of priority enrollment status. Significant academic improvement is defined as achieving no less than the minimum grade point average and progress standard established in Administrative Procedure 4250].

Appeal of Loss of Enrollment Priority

Students may appeal the loss of enrollment priority when the loss is due to extenuating circumstances. Extenuating circumstances are verified cases of accidents, illnesses, or other circumstances beyond the control of the student, or when a student with a disability applied for but did not receive a reasonable accommodation in a timely manner. The appeal will be determined by the appropriate authority designated by the college,

Additionally, students who have demonstrated significant academic improvement may appeal the loss of priority enrollment status. Significant academic improvement is defined as achieving no less than the minimum grade point average and progress standard established in Administrative Procedure 4250. The appeals process for academic improvement will follow the same procedure as for extenuating circumstances, with the decision made by the designated authority at each college.

These mandated enrollment priorities will be effective in the Fall, 2014 term. The District will ensure that these procedures are reflected in course catalogs and that all students have appropriate and timely notice of the requirements of this procedure.

- limiting enrollment to first come, first served, or other non-evaluative selection techniques;
- in the case of intercollegiate completion, honors courses, or public performance courses, allocating available seats to those students judged most qualified;
- limiting enrollment to any selection procedure expressly authorized by statute;
- limiting enrollment in one or more sections to students enrolled in one or more other courses, provided that a reasonable percentage of all sections of the course do not have such restrictions.

A. General Access

AP**5055 Enrollment Priorities**

10+1 ♦ CCLC | Good Practice/Optional ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Every course for state apportionment, wherever offered and maintained by the District, shall be fully open to enrollment and participation by any person who has been admitted to the colleges and who meets such prerequisites as may be established in compliance with Title V 5 of the California Administrative Code.

B. Priorities for Enrollment

Each college shall establish procedures that set priorities for enrollment and publish them in their Class Schedules. Such procedures shall be made available to students during the registration process.

Priority for enrollment must be granted to any member or former member of the Armed Forces of the United States for any academic term within two years of leaving active duty.

C. Matriculation

All students shall be subject to the requirements of the matriculation process at each college. Recommendations for class enrollment based upon testing and evaluation shall be strongly recommended to students but shall be advisory only.

References:

Education Code Sections 66025.8 and 66025.9;
Title 5 Sections 58106 and 58108

End Recommendation for AP 5055 Enrollment Priorities



5530 Student Rights and Grievances



10+1 ♦ Non CCLC ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

> Chapter Lead Recommendation

Level 3 Review Schedule

10/06/2024 ♦ Recommendation Received

10/17/2024 ♦ PPAC Approves Review Level

10/18/2024 ♦ Level 2 to Constituents and AS for Feedback

11/06/2024 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

11/21/2024 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

12/04/2024 ♦ AS Reviews Level 3 for Final Input

12/20/2024 ♦ PPAC Reviews Final AS Input

01/09/2025 ♦ BOT 1st Read

02/13/2025 ♦ BOT Final Approval

Begin Recommendation for BP 5530 Student Rights and Grievances

~~Students may initiate grievance proceedings against a district employee under the procedures provided by the Chancellor.~~

It is the policy of the District that there shall be an appeal process by which a dispute in the assigned final grade received by a student may be resolved in a fair and efficient manner according to State law. (See BP and AP 4231 titled Grade Changes).

References:

Education Code Section 76224(a);

Title 5 Section 55025

Title IX, Education Amendments of 1972

End Recommendation for BP 5530 Student Rights and Grievances



5530 Student Rights and Grievances



10+1 ♦ CCLC | Legally Advised ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Reasons for Review

> Chapter Lead Recommendation

Level 3 Review Schedule

10/06/2024 ♦ Recommendation Received

10/17/2024 ♦ PPAC Approves Review Level

10/18/2024 ♦ Level 2 to Constituents and AS for Feedback

11/06/2024 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input

11/21/2024 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3

12/04/2024 ♦ AS Reviews Level 3 for Final Input

12/20/2024 ♦ PPAC Reviews Final AS Input

01/09/2025 ♦ BOT 1st Read

02/13/2025 ♦ BOT Final Approval

Begin Recommendation for AP 5530 Student Rights and Grievances

The purpose of this procedure is to provide a prompt and equitable means of resolving student grievances. These procedures shall be available to any student who reasonably believes a college decision or action by an instructor, college official, or by another student has adversely affected their status, rights or privileges as a student. The procedures shall include, but not be limited to, grievances regarding:

- **Academic Grievances:** When grades are given for any course of instruction taught in a community college district, the grade given to each student shall be the grade determined by the instructor of the course and the determination of the student's grade by the instructor, in the absence of mistake, fraud, bad faith, or incompetency shall be final (Education Code Section 76224). If a student files a grievance relative to grade, he/she/they must prove that "mistake, fraud, bad faith, or incompetency" as the reason for the grade assignment.
- **Non-Academic Grievances:** Grounds for a non-academic grievance include, but are not limited to:
 - Any act or threat of intimidation;
 - Any act or threat of physical aggression;
 - Arbitrary action, violation of student rights, or imposition of sanctions without proper regard to College policy as specified in the Education Code, Board Policies, and/or Administrative Procedures;
 - **Course Repetition, Withdrawals, and Enrollment Fees:** Students may file complaints related to course repetition, withdrawals or enrollment fees based on evidence of extenuating circumstances. Students should use the Petition for Exceptional Action form and provide supporting documentation. Action will be taken by the appropriate administrator or by the Board of Appeals. Petition for Exceptional Action forms can be found in the offices of Counseling, Admissions and Records, and Student Life. Petitions may be submitted through the Office of the Dean, Student Services for review by the Board of Appeals;
- **For grievances related to sexual harassment, sexual assault, or illegal discrimination Complaints:** (i.e. age, ancestry, citizenship status, color, disability, ethnic group identification, gender, marital status, medical condition, national origin, parental status, race, religion, sexual orientation, or veteran status), students should contact the Human Resources Department and/or the San Bernardino Community College Police. Staff members in those areas will assist students with the correct processes for resolution. Complaint and investigation procedures related to harassment and discrimination (including sexual assault, sexual violence, dating violence, stalking, and domestic violence) can be found in Administrative Procedure 3435.



5530 Student Rights and Grievances



10+1 ♦ CCLC | Legally Advised ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

- Financial ~~a~~Aid Challenge: Financial aid students wishing to file a complaint regarding the financial aid process and/or determination should refer to ~~(see~~ AP 5130 Financial Aid for appeals ~~appeals~~ relating to financial aid);
- ~~Course grades, to the extent permitted by Education Code Section 76224(a) (see AP 4231 Grade Changes for appeals relating to course grades)~~
- The exercise of rights of free expression protected by state and federal constitutions and Education Code Section 76120.

In addition to San Bernardino Community College District Procedures, a student may address a grievance directly to the California Community Colleges Chancellor's Office by accessing the following website:

<https://www.cccco.edu/complaint-process-notice>

This procedure does not apply to:

- Student disciplinary actions, which are covered under separate Board Policies and Administrative Procedures.
- Police citations (i.e. "tickets"); complaints about citations must be directed to the County Courthouse in the same way as any traffic violation.

Definitions of Terms

Party – The student or any persons claimed to have been responsible for the student's alleged grievance, together with their representatives. "Party" shall not include the Grievance Hearing Committee or the College Grievance Officer.

Chancellor/President – The Chancellor/President or a designated representative of the Chancellor/President.

Grievant – A student who has viled a Grievance.

Student – A currently enrolled student, a person who has filed an application for admission to the college, or a former student. A grievance by an applicant shall be limited to a complaint regarding denial of admission. Former students shall be limited to grievances relating to course grades to the extent permitted by Education Code Section 76224(a).

Respondent – Any person claimed by a grievant to be responsible for the alleged grievance.

Business Day – Unless otherwise provided, day shall mean a day during which the college is in session and regular classes are held, excluding Saturdays and Sundays.

Informal Resolution

Each student who has a grievance shall make a reasonable effort to resolve the matter on an informal basis prior to requesting a grievance hearing, and shall attempt to solve the problem with the person with whom the student has the grievance, that person's immediate supervisor, or the local ~~college~~ District administration.

Deans of Student Services shall assist students in seeking resolution by informal means. This person shall be also be known as the Grievance Officer. The Grievance Officer and the student may also seek the assistance of the Associated Student Organization in attempting to resolve a Grievance informally.

Informal meetings and discussion between persons directly involved in a grievance are essential at the outset of a dispute and should be encouraged at all stages. An equitable solution should be sought before persons directly involved in the case have stated official or public positions that might tend to polarize the dispute and render a solution more difficult. At no time shall any of the persons directly or indirectly involved in the



5530 Student Rights and Grievances



10+1 ♦ CCLC | Legally Advised ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

case use the fact of such informal discussion, the fact that a grievance has been filed, or the character of the informal discussion for the purpose of strengthening the case for or against persons directly involved in the dispute or for any purpose other than the settlement of the grievance.

Formal Process

If informal resolution through discussion or mediation does not resolve the conflict, the student shall have the right to request a grievance hearing, in writing, to the Vice president of Student Services. The request for a hearing must be made within 180 calendar days of the incident being grieved.

The determination of whether the Statement of Grievance presents sufficient grounds for a hearing shall be based on the following:

- The statement contains facts which, if true, would constitute a grievance under these procedures;
- The grievant is a student as defined in these procedures, which include applicants and former students;
- The grievant is personally and directly affected by the alleged grievance;
- The grievance was filed in a timely manner;
- The grievance is not clearly frivolous, clearly without foundation, or clearly filed for purposes of harassment.

If the grievance does not meet each of the requirements, the Vice president of Student Services shall notify the student in writing of the rejection of the Request for a Grievance Hearing, together with the specific reasons for the rejection and the procedures for appeal. This notice will be provided within five days of the date the decision is made.

If the Request for Grievance Hearing satisfies each of the requirements, the Vice president of Student Services shall schedule a grievance hearing. The hearing will begin within ten days following the decision to grant a Grievance Hearing. All parties to the grievance shall be given not less than five days notice of the date, time and place of the hearing.

Grievance Hearing

The formal grievance hearing will be scheduled within 10 days (during which the college is in session) of receipt of the request. The grievance hearing committee will be composed of the following:

- One student appointed by the Student Senate president.
- One faculty member appointed by the Academic Senate president if the grievance is against a faculty member.
- One staff member appointed by the Classified Senate president if the grievance is against a staff member.
- Vice president of Student Services, who will chair the committee if the grievance is non-academic, or the Vice president of Instruction if the grievance is academic.

No person shall serve as a member of a Grievance Hearing Committee if that person has been personally involved in any matter giving rise to the grievance, has made any statement on the matters at issue, or could otherwise not act in a neutral manner.

Any party to the grievance may challenge for cause any member of the hearing committee prior to the beginning of the hearing by addressing a challenge to the chair, who shall determine whether cause for disqualification has been shown. If the chair feels that sufficient ground for removal of a member of the committee has been presented, they shall remove the challenged member or members and substitute a member or members from the panel described above. This determination is subject to appeal as defined below.

The chair will conduct the hearing. Possible protective measures that may be utilized include, but are not limited to, no-contact orders, remote participation during the hearing (telephone, videoconferencing, use of a privacy screen, etc.), separate waiting areas during hearing, safety escorts, and prohibitions against retaliation.

The members of the grievance hearing committee will be provided a copy of the grievance and any written response to the grievance.



5530 Student Rights and Grievances



10+1 ♦ CCLC | Legally Advised ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Each party to the grievance may call witnesses and introduce oral and written testimony. ~~Witnesses unable to be present may submit written statements. All witnesses must testify under oath; the Grievance Hearing Committee Chair will administer the oath. The Grievance Hearing Committee will only admit written statements of witnesses under penalty of perjury if the witness is unavailable to testify. A witness who refuses to be tape-recorded shall be considered to be unavailable.~~

Although the hearing is formal, rules of evidence do not apply as they would in a court of law.

Each party to the grievance will be permitted to make an opening statement; thereafter, the grievant will present evidence followed by the respondent.

The student may bring an advocate or attorney to the hearing provided the Vice President of Student Services is notified at least five calendar days in advance of the hearing. In the event the student serves notification that they will have representation, the respondent has the right to legal counsel and a right to receive notification that the student will have counsel present.

The hearing will be recorded, and the recording shall remain in the custody of the Vice president of Student Services. Any party to the grievance may request a copy of the recording.

Hearings shall be closed and confidential unless all parties request that they be open to the public. Any such request must be made no less than three calendar days prior to the date of the hearing. In a closed hearing, witnesses will testify and be excused.

The grievance hearing committee will recommend a resolution of the grievance after listening to all of the participants. The committee will inform the student and the respondent in writing about its recommendation within 10 days of the hearing. The decision shall be based only on the record of the hearing, and not on matter outside of that record. The record consists of the original grievance, any written response, and the oral and written evidence produced at the hearing.

Within five days following the close of the hearing, the Grievance Hearing Committee shall prepare and send to the ~~President~~ Chancellor a written ~~decision~~ recommendation. The recommendation shall include specific factual findings regarding the grievance. The recommendation shall also include ~~relief afforded to the student, if any~~ a specific recommendation regarding the relief for the Grievant, if any. The Grievance Hearing Committee will base its recommendation only on the record of the hearing, and not on matter outside of that record. The record consists of the original Grievance, any written response, and the oral and written evidence produced at the hearing.

~~Within five days following receipt of the Grievance Hearing Committee's decision and recommendation(s), the President shall send to all parties their written decision, together with the Hearing Committee's decision and recommendations. The Chancellor may accept or reject the findings, decisions and recommendations of the Hearing Committee. The factual findings of the Hearing Committee shall be accorded great weight; and if the President does not accept the decision or a finding or recommendation of the Hearing Committee, the President shall review the record of the hearing, and shall prepare a new written decision which contains specific factual findings and conclusions. The decision of the President shall be final, subject only to appeal as provided below~~

Appeals

The student may appeal the recommendation of the grievance hearing committee by writing to the president within 10 calendar days of being notified of the grievance hearing committee's recommendation. The president will send the student a final decision in writing within 10 calendar days of receiving the appeal.

Any appeal relating to a Grievance Hearing Committee decision that the Statement of Grievance does not present a grievance as defined in these procedures shall be made in writing to the president within five days of that decision. The president shall review the Statement of Grievance and Request for Grievance Hearing in accordance with the requirements for a grievance provided in these procedures, but shall not consider any other matters. The Chancellor's decision whether or not to grant a grievance hearing shall be final and not subject to further appeal.

Any party to the grievance may appeal the decision of the president after a hearing before a Grievance Hearing Committee by filing an appeal with the Chancellor. The Chancellor may designate a District administrator to review the appeal and make a recommendation.

AP**5530 Student Rights and Grievances**

10+1 ♦ CCLC | Legally Advised ♦ Chapter Lead Ornelas ♦ Both BP & AP Exist

Any such appeal shall be submitted in writing within five days following receipt of the Chancellor's decision and shall state specifically the grounds for appeal.

The written appeal shall be sent to all concerned parties. All parties may submit written statements on the appeal.

The Chancellor or designee shall review the record of the hearing and the documents submitted in connection with the appeal, but shall not consider any matters outside of the record. Following the review of the record and appeal statements, the Chancellor's designee, if any, shall make a written recommendation to the Chancellor regarding the outcome of the appeal.

The Chancellor's Decision Within five days following receipt of the Grievance Hearing Committee's decision and recommendation(s), the Chancellor shall send to all Parties his/her/their written decision, together with the Hearing Committee's decision and recommendations. The Chancellor may accept or reject the findings, decisions, and recommendations of the Hearing Committee. The factual findings of the Hearing Committee shall be accorded great weight; and if the Chancellor does not accept the decision or a finding or recommendation of the Hearing Committee, the Chancellor shall review the record of the hearing, and shall prepare a new written decision which contains specific factual findings and conclusions. The decision of the Chancellor shall be final.

Time Limits

Any times specified in these procedures may be shortened or lengthened if there is mutual concurrence by all parties.

References:

Education Code Section 76224 subdivision (a);
ACCJC Accreditation Eligibility Requirement 20;
ACCJC Accreditation Standard 4

End Recommendation for AP 5530 Student Rights and Grievances