SBVC Academic Senate Legislative Committee Report
October 2, 2024

PPAC 9/19/24 Meeting Events

- 2024-2025 PPAC Annual Review List Approved
- 7250 Educational Administrators and 7340 Leaves –10+1 Designation Removed
- 5500 Standards of Student Conduct- Level 3 Academic Senate Input reviewed. Will move to BoT approval on 10/10/24

Level 1: INFORMATION ONLY-Goes to Board on 10/10/24

Generally consists of Chapter Lead Recommendations for P&Ps which are:

- Reviewed with no changes,
- Reviewed with only minor clerical edits or legal reference changes, or
- Chapters 1 and 2 BOT P&Ps which are not designated 10+1.

2015 Student Trustees
2355 Decorum
2430 Delegation of Authority to the Chancellor
2510 Participation in Local Decision-Making
2715 Code of Ethics/Standards of Practice
2731 Trustee Emeritus

Level 2: MINOR REVIEW (NON 10+1)-Feedback Needed for 10/17 PPAC Meeting

Generally consists of Chapter Lead Recommendations on:

- Existing P&Ps which are simple and non-controversial.
- New P&Ps that are simple and non-controversial.

3720 Computer and Network Use
3725 Information and Communications Technology Accessibility & Acceptable Use
3726 Information Security Data Classification
3727 Information Security Access Control
3728 Information Security Physical Security
3729 Information Security Logging & Monitoring
3730 Information Security Remote Access
3731 Information Security Internally Developed Systems Change Control
3732 Information Security-Security Incident Response
3733 Information Security-Security Secure Operations
3734 Information Security-Security Network Security
3735 Information Security Disaster Recovery
3736 Information Security Cloud Storage
3737 Information Security Payment Card Industry Requirements
5030 Fees
6925 Refreshments or Meals Served at Meetings

Level 3: EXTENSIVE REVIEW - Feedback Needed for 10/17 PPAC Meeting

Generally consists of Chapter Lead Recommendations on:

- Existing P&Ps with substantial changes and/or subject to 10+1.
- New P&Ps that are controversial, complex and/or subject to 10+1.
- May return to PPAC in

4300 Field Trips and Excursions

POLICIES & PROCEDURES 2024-25 ANNUAL REVIEW LIST AS OF 9/19/2024

Title	10+1?	Reason	Current Step Date	Current Step
BP 2015 Student Trustees	Non 10+1	*> Legal Update 44: Updated to add voting privileges for student members of the governing board and clarify the student member's rights pursuant to changes in the Education Code.* *> Chapter Lead request to improve accuracy and efficiency, and to reflect current practice.*	9/19/2024	PPAC Approves Review Level
BP 2110 Vacancies on the Board	Non 10+1	*> Minor clerical edit.*	10/31/2024	Recommendation Requested
AP 2110 Vacancies on the Board	Non 10+1	*> Added Legal Language identified by Sr. EA Ford regarding the resigning member's not having the right to vote for successor.* *> Legal Update 44: Updated to add vacancy notice requirements pursuant to changes in the Education Code and best practice.*	10/31/2024	Recommendation Requested
BP 2315 Closed Sessions	Non 10+1	*> Proposed adoption of legally required BP*	10/31/2024	Recommendation Requested
AP 2325 Teleconferenced Meetings	Non 10+1	*> Legal Update 44: Updated to align with the Ralph M. Brown Act requirements pursuant to changes in the Government Code.*	10/31/2024	Recommendation Requested
BP 2355 Decorum	Non 10+1	*> Legal Update 44: Updated to add references to the Government Code and update language pursuant to changes in the Government Code.*	9/19/2024	PPAC Approves Review Level
BP 2430 Delegation of Authority to the Chancellor	Non 10+1	*> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standard and related language pursuant to the 2024 changes in the ACCJC Accreditation Standards.*	9/19/2024	PPAC Approves Review Level
AP 2430 Delegation of Authority to the Chancellor	Non 10+1	*> Should SBCCD Adopt CCLC Good Practice AP?* *> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards.*	9/19/2024	PPAC Approves Review Level
BP 2510 Participation In Local Decision-Making	10+1	*> Recommendation from VC Hannon* *> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standards pursuant to the 2024 changes in the ACCJC Accreditation Standards.*	9/19/2024	PENDED
AP 2510 Participation In Local Decision-Making	10+1	*> FYI Only* *> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standards pursuant to the 2024 changes in the ACCJC Accreditation Standards.*	9/19/2024	PENDED
BP 2710 Conflict of Interest	Non 10+1	*> Gender language update, and citation update per CCLC version.*	10/31/2024	Recommendation Requested
AP 2710 Conflict of Interest	Non 10+1	*> Legal Update 44: Updated to provide legally advised language regarding the prohibition on outside employment that is inconsistent, incompatible, or in conflict with the individual's District duties, functions, and responsibilities.* *> Gender language update.*	10/31/2024	Recommendation Requested
BP 2715 Code of Ethics/Standards of Practice	Non 10+1	*> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standard and add supporting language pursuant to the 2024 changes in the ACCJC Accreditation Standards. The Service also updated this policy to change a reference to the "Superintendent/President" to "[CEO]."*	9/19/2024	PPAC Approves Review Level
BP 2731 Trustee Emeritus	Non 10+1	*>Requested by Board Executive Committee.*	9/19/2024	PPAC Approves Review Level

POLICIES & PROCEDURES 2024-25 ANNUAL REVIEW LIST AS OF 9/19/2024

Title	10+1?	Reason	Current Step Date	Current Step
BP 2740 Board Education	Non 10+1	*> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards.* *> Delete superfluous langage from ACCJC Accreditation Standard.* *> Minor clerical update.*	09/30/2024	Recommendation Requested
BP 3250 Institutional Planning	Non 10+1	*> 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.*	10/31/2024	Recommendation Requested
AP 3250 Institutional Planning	Non 10+1	*> 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.*	10/31/2024	Recommendation Requested
BP 3430 Prohibition of Harassment	Non 10+1	*> FYI only*	10/31/2024	Recommendation Requested
AP 3430 Prohibition of Harassment	Non 10+1	*> Legal Update 44 Summer: This procedure was revised to update references to BP 3433 Prohibition of Sex Discrimination under Title IX, AP 3433 Prohibition of Sex Discrimination under Title IX, and AP 3434 Responding to Sex Discrimination under Title IX and clarify to whom the procedure applies.*	10/31/2024	Recommendation Requested
BP 3433 Prohibition of Sexual Harassment under Title IX	Non 10+1	*> Legal Update 44 Summer: This policy was revised to update the title and align with the requirements of the 2024 Title IX regulations.*	10/31/2024	Recommendation Requested
AP 3433 Prohibition of Sexual Harassment under Title IX	Non 10+1	*> Legal Update 44 Summer: This procedure was revised to update the title, add a definition for sex discrimination under Title IX, and revise the definition of sex-based harassment under Title IX to align with the requirements of the 2024 Title IX regulations.*	10/31/2024	Recommendation Requested
AP 3434 Responding to Harassment Based on Sex under Title IX	Non 10+1	*> Legal Update 44 Summer: This procedure was revised to update the title and align the grievance processes with the requirements of the 2024 Title IX regulations.* *> Legal Update 43: The Service updated this procedure to clarify that written confidentiality agreements with Parties and Advisors are good practice but not required under federal Title IX law and regulations.* *> Legal Update 42: The Service updated this procedure to include required information on sexual assault and domestic violence counselors pursuant to changes in the Education Code.* *> Legal Update 41: The Service updated this procedure to remove a historically offensive term, to align to FBI crime definitions, and to clarify that the contents of a written investigative report should not include findings or determinations of law or fact, consistent with the 2020 regulations.*	10/31/2024	Recommendation Requested

POLICIES & PROCEDURES 2024-25 ANNUAL REVIEW LIST AS OF 9/19/2024

Title	10+1?	Reason	Current Step Date	Current Step
AP 3435 Discrimination and Harassment Resolution Procedures	Non 10+1	*> Legal Update 44 Summer: This procedure was revised to update references to BP 3433 Prohibition of Sex Discrimination under Title IX, AP 3433 Prohibition of Sex Discrimination under Title IX, and AP 3434 Responding to Sex Discrimination under Title IX.* *> Legal Update 44: Updated to align the deadline for complaints of discrimination, harassment, or retaliation in employment to the statute of limitations allowed under the Fair Employment and Housing Act.* *> Legal Update 43: The Service updated this procedure to provide optional language regarding a governing board's review of an appeal of the district's administrative determination under Title 5 regulations.* *> Legal Update 42: The Service updated this procedure to reflect the new name of the California Civil Rights Department and to align with updated Title 5 regulations.*	10/31/2024	Recommendation Requested
BP 3501 Campus Security and Access	Non 10+1	*> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standard and add supporting language pursuant to the 2024 changes in the ACCJC Accreditation Standards.*	10/31/2024	Recommendation Requested
AP 3501 Campus Security and Access	Non 10+1	*> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards.*	10/31/2024	Recommendation Requested
BP 3510 Workplace Violence	Non 10+1	*> Minor clerical edit*	10/31/2024	Recommendation Requested
AP 3510 Workplace Violence	Non 10+1	*> Legal Update 44: Updated to add citations to the Labor Code and identify requirements of a workplace violence prevention plan and file retention requirements pursuant to changes in the Labor Code.*	10/31/2024	Recommendation Requested
BP 3530 Weapons on Campus	Non 10+1	*> Minor clerical update*	10/31/2024	Recommendation Requested
AP 3530 Weapons on Campus	Non 10+1	*> Legal Update 44: Updated to clarify the prohibition on weapons.*	10/31/2024	Recommendation Requested
BP 3540 Sexual and Other Assaults on Campus	Non 10+1	*> Legal Update 42: The Service updated this policy to apply to victims of domestic violence and to any location, expanding the application beyond a district's grounds pursuant to changes in the Education Code. The Service updated the title to align to current law.*	10/31/2024	Recommendation Requested
AP 3540 Sexual and Other Assaults on Campus	Non 10+1	*> Legal Update 44 Summer: This procedure was revised to update references to AP 3434 Responding to Sex Discrimination under Title IX.* *> Legal Update 42: The Service updated this procedure to set out options for victims including information about sexual assault and domestic violence counselors pursuant to changes in the Education Code. The Service updated the title of this procedure to align to current law.*	10/31/2024	Recommendation Requested

POLICIES & PROCEDURES 2024-25 ANNUAL REVIEW LIST AS OF 9/19/2024

Title	10+1?	Reason	Current Step Date	Current Step
BP 3550 Drug Free Environment and Drug Prevention Program	Non 10+1	*> Legal Update 44: Updated this policy to add additional requirements related to fentanyl test strips and specify the need to identify supporting administrative procedures pursuant to changes to the Education Code.* *> Legal Update 43: The Service updated this policy to clarify that only districts with a campus health center are required to include certain language about distributing opioid overdose reversal medication.* *> Legal Update 42- The Service updated this policy to add requirements related to providing information on opioid overdose reversal medication in campus orientations and the ability of campus health centers to distribute opioid overdose reversal medication pursuant to changes in the Education Code.*	10/31/2024	Recommendation Requested
AP 3550 Drug Free Environment and Drug Prevention Program	Non 10+1	*> Legal Update 44: Updated this procedure to include provisions related to fentanyl test strips pursuant to changes in the Education Code.* *> Legal Update 43: The Service updated this policy to clarify that only districts with a campus health center are required to include certain language about distributing opioid overdose reversal medication.* *> Legal Update 42: The Service updated this procedure to add requirements related to providing information on opioid overdose reversal medication in campus orientations and the ability of campus health centers to distribute opioid overdose reversal medication pursuant to changes in the Education Code.*	10/31/2024	Recommendation Requested
BP 3600 Auxiliary Organizations	Non 10+1	*> Assess adoption of AP legally required for auxiliary organizations*	10/31/2024	Recommendation Requested
AP 3600 Auxiliary Organizations	Non 10+1	*> Assess adoption of BP legally required for auxiliary organizations*	10/31/2024	Recommendation Requested
BP 3720 Computer and Network Use	Non 10+1	*> Chapter Lead review of IT security*	9/19/2024	PPAC Approves Review Level
AP 3720 Computer and Network Use	Non 10+1	*> Chapter Lead review of IT security*	9/19/2024	PPAC Approves Review Level
BP 3725 Information and Communications Technology Accessibility & Acceptable Use	Non 10+1	*> 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.*	9/19/2024	PPAC Approves Review Level
AP 3725 Information and Communications Technology Accessibility & Acceptable Use	Non 10+1	*> 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)*	9/19/2024	PPAC Approves Review Level
AP 3726 Information Seurity Data Classification	Non 10+1	*> New AP resulting from Chapter Lead review of IT security*	9/19/2024	PPAC Approves Review Level

POLICIES & PROCEDURES 2024-25 ANNUAL REVIEW LIST AS OF 9/19/2024

Title	10+1?	Reason	Current Step Date	Current Step
AP 3727 Information Security Access Control	Non 10+1	*> New AP resulting from Chapter Lead review of IT security*	9/19/2024	PPAC Approves Review Level
AP 3728 Information Security Physical Security	Non 10+1	*> New AP resulting from Chapter Lead review of IT security*	9/19/2024	PPAC Approves Review Level
AP 3729 Information Security Logging & Monitoring	Non 10+1	*> New AP resulting from Chapter Lead review of IT security*	9/19/2024	PPAC Approves Review Level
AP 3730 Information Security Remote Access	Non 10+1	*> New AP resulting from Chapter Lead review of IT security*	9/19/2024	PPAC Approves Review Level
AP 3731 Information Security Internally Developed Systems Change Control	Non 10+1	*> New AP resulting from Chapter Lead review of IT security*	9/19/2024	PPAC Approves Review Level
AP 3732 Information Security-Security Incident Response	Non 10+1	*> New AP resulting from Chapter Lead review of IT security*	9/19/2024	PPAC Approves Review Level
AP 3733 Information Security-Security Secure Operations	Non 10+1	*> New AP resulting from Chapter Lead review of IT security*	9/19/2024	PPAC Approves Review Level
AP 3734 Information Security-Security Network Security	Non 10+1	*> New AP resulting from Chapter Lead review of IT security*	9/19/2024	PPAC Approves Review Level
AP 3735 Information Security Disaster Recovery	Non 10+1	*> New AP resulting from Chapter Lead review of IT security*	9/19/2024	PPAC Approves Review Level
AP 3736 Information Security Cloud Storage	Non 10+1	*> New AP resulting from Chapter Lead review of IT security*	9/19/2024	PPAC Approves Review Level
AP 3737 Information Security Payment Card Industry Requirements	Non 10+1	*> New AP resulting from Chapter Lead review of IT security*	9/19/2024	PPAC Approves Review Level
BP 4010 Academic Calendar	10+1	*> FYI Only: No Changes*	10/31/2024	Recommendation Requested
AP 4010 Academic Calendar	10+1	*> Legal Update 44: Updated to identify optional language pursuant to changes in the Education Code.*	10/31/2024	Recommendation Requested
BP 4020 Program, Curriculum, and Course Development	10+1	*> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards.*	10/31/2024	Recommendation Requested
AP 4020 Program, Curriculum, and Course Development	10+1	*> 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.*	10/31/2024	Recommendation Requested

POLICIES & PROCEDURES 2024-25 ANNUAL REVIEW LIST AS OF 9/19/2024

Title	10+1?	Reason	Current Step Date	Current Step
BP 4100 Graduation Requirements for Degrees and Certificates	10+1	*> 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*	10/31/2024	Recommendation Requested
AP 4100 Graduation Requirements for Degrees and Certificates	10+1	*> 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)*	10/31/2024	Recommendation Requested
BP 4103 Work Experience	10+1	*> FYI only to support Legal Update 43 review of AP.*	10/31/2024	Recommendation Requested
AP 4103 Work Experience	10+1	*> Legal Update 43: The Service updated this procedure to revise the title and content to align with changes in the Title 5 regulations.*	10/31/2024	Recommendation Requested
AP 4222 Remedial Coursework	10+1	*> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards. The Service also updated this procedure to identify requirements related to placement pursuant to the 2024 changes in the Education Code.*	10/31/2024	Recommendation Requested
AP 4227 Repeatable Courses	10+1	*> Legal Update 43: The Service updated this procedure to align with revised Title 5 regulations.*	10/31/2024	Recommendation Requested
BP 4230 Grading and Academic Record Symbols	10+1	*> 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 though 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)*	10/31/2024	Recommendation Requested

POLICIES & PROCEDURES 2024-25 ANNUAL REVIEW LIST AS OF 9/19/2024

Title	10+1?	Reason	Current Step Date	Current Step
AP 4230 Grading and Academic Record Symbols	10+1	*> 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)*	10/31/2024	Recommendation Requested
BP 4250 Probation, Dismissal, and Readmission	10+1	*> Minor Clerical Update*	10/31/2024	Recommendation Requested
AP 4250 Probation, Dismissal, and Readmission	10+1	*> Legal Update 42: The Service updated this procedure to align with updated Title 5 regulations.*	10/31/2024	Recommendation Requested
AP 4255 Dismissal and Readmission	10+1	*> SBCCD has not yet adopted this legally required process. This needs to be reviewed and adopted.* *> Legal Update 42: The Service updated this procedure to align with updated Title 5 regulations.*	10/31/2024	Recommendation Requested
BP 4260 Prerequisites and Co-requisites	10+1	*> Requested by CHC Academic Senate at 3/11/2024 PPAC to review to change the five-day timeframe in which to resolve challenges to a ten-day time frame, and to define what working days mean for faculty.*	10/31/2024	Recommendation Requested
AP 4260 Prerequisites and Co-requisites	10+1	*> Requested by CHC Academic Senate at 3/11/2024 PPAC to review to change the five-day timeframe in which to resolve challenges to a ten-day time frame, and to define what working days mean for faculty.*	10/31/2024	Recommendation Requested
BP 4300 Field Trips and Excursions	10+1	*> 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.*	9/19/2024	PPAC Approves Review Level
AP 4300 Field Trips and Excursions	10+1	*> 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.*	9/19/2024	PPAC Approves Review Level
AP 5012 International Students	10+1	*> SBCCD has not yet adopted this legally required process. This needs to be reviewed and adopted.*	10/31/2024	Recommendation Requested
BP 5020 Nonresident Tuition	Non 10+1	*> Legal Update 42: The Service updated this policy to provide an exemption to a nonresident student who enrolls in a credit English as a Second Language course if they meet certain requirements pursuant to changes in the Education Code.*	10/31/2024	Recommendation Requested
AP 5020 Nonresident Tuition	Non 10+1	*> Legal Update 42: The Service updated this procedure to provide an exemption to a nonresident student who enrolls in a credit English as a Second Language course if they met certain requirements pursuant to changes in the Education Code.*	10/31/2024	Recommendation Requested
BP 5030 Fees	Non 10+1	*> FYI only.*	9/19/2024	PPAC Approves Review Level

POLICIES & PROCEDURES 2024-25 ANNUAL REVIEW LIST AS OF 9/19/2024

Title	10+1?	Reason	Current Step Date	Current Step
AP 5030 Fees	Non 10+1	*> Per Chapter Lead to incorporate BookSaver Program*	9/19/2024	PPAC Approves Review Level
BP 5035 Withholding of Student Records	10+1	*> 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.*	10/31/2024	Recommendation Requested
AP 5035 Withholding of Student Records	10+1	*> FYI Only*	10/31/2024	Recommendation Requested
BP 5040 Student Records, Directory Information, and Privacy	10+1	*> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards. The Service also updated this policy to clarify when a district may use a student's gender or legal name as indicated in a government-issued identification document pursuant to changes in the Education Code.*	10/31/2024	Recommendation Requested
AP 5040 Student Records, Directory Information, and Privacy	10+1	*> Legal Update 44: Updated to add a legal citation, clarify when a district may use a student's gender or legal name as indicated in a government-issued identification document, and clarify the records a district shall update to reflect an affirmed name and gender pursuant to changes in the Education Code. The Service also updated this procedure to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards.*	10/31/2024	Recommendation Requested
BP 5055 Enrollment Priorities	10+1	*> FYI only to support Legal Update 43 review of AP.*	10/31/2024	Recommendation Requested
AP 5055 Enrollment Priorities	10+1	*> 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.*	10/31/2024	Recommendation Requested
BP 5070 Attendance Accounting	10+1	*> BP requires an annual review; last updated 12/8/2023*	10/31/2024	Recommendation Requested
AP 5070 Attendance Accounting	10+1	*> AP being forwarded to support annual review of BP*	10/31/2024	Recommendation Requested
BP 5075 Course Adds, Drops, and Withdrawals	10+1	*> Per discussion at 5/13/2024 PPAC requesting Chapter Lead clarification of "Intervention Program" and the impact of the "FW" grade.* *> Minor Clerical Edit*	10/31/2024	Recommendation Requested
AP 5075 Course Adds, Drops, and Withdrawals	10+1	*> 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.*	10/31/2024	Recommendation Requested
BP 5130 Financial Aid	Non 10+1	*> 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 42: The Service updated this policy to implement the California Ban on Scholarship Displacement Act of 2021 pursuant to changes in the Education Code.*	10/31/2024	Recommendation Requested
AP 5130 Financial Aid	Non 10+1	*> Legal Update 44: Updated to add a legal citation pursuant to changes in the Education Code. The Service also updated this procedure to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards.* *> Legal Update 42: The Service updated this procedure to implement the California Ban on Scholarship Displacement Act of 2021 pursuant to changes in the Education Code.*	10/31/2024	Recommendation Requested

POLICIES & PROCEDURES 2024-25 ANNUAL REVIEW LIST AS OF 9/19/2024

Title	10+1?	Reason	Current Step Date	Current Step
BP 5220 Shower Facilities for Homeless Students	10+1	*> Chapter Lead: Good Practice BP being Presented for adoption*	10/31/2024	Recommendation Requested
AP 5220 Shower Facilities for Homeless Students	10+1	*> Chapter Lead: Good Practice AP Presented for adoption*	10/31/2024	Recommendation Requested
BP 5410 Associated Students Elections	10+1	*> Legal Update 42: The Service updated this policy to allow a disabled student or student enrolled in a district's adult education program to serve on student government pursuant to changes in the Education Code.*	10/31/2024	Recommendation Requested
AP 5410 Associated Students Elections	10+1	*> Please note SBCCD has not adopted this AP; should it be adopted?*	10/31/2024	Recommendation Requested
BP 5500 Standards of Student Conduct	10+1	*> 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 42: The Service updated this policy to add legal citations.*	9/19/2024	PPAC Review Level 3 AS Final Input
AP 5500 Standards of Student Conduct	10+1	*> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards.* *> Chapter Lead Changes resulting from legal review of BP*	9/19/2024	PPAC Review Level 3 AS Final Input
BP 5510 Off-Campus Student Organizations	10+1	*>Need to adopt; this is a legally required policy.*	10/31/2024	Recommendation Requested
AP 5510 Off-Campus Student Organizations	10+1	*> Need to adopt; this is a legally required procedure*	10/31/2024	Recommendation Requested
AP 5520 Student Discipline Procedures	10+1	*> Legal Update 44: Updated to clarify and simplify language regarding determination of discipline and student discipline hearings.* *> Legal Update 40: The Service updated this procedure to reflect recent legislation that complainants or witnesses in an investigation of sexual assault, domestic violence, dating violence, or stalking will not be subject to disciplinary sanctions for violations of the student conduct policy unless the violation was egregious. (2022-23 carryover)* *> Legal Update 38: The Service updated this procedure to change the abbreviation AS to state "Associated Students" and to add optional language to highlight diversity, equity, and inclusion issues.(2022-23 carryover)*	10/31/2024	Recommendation Requested
AP 6355 Job Order Contracts	Non 10+1	*> Legal Update 44: Updated to revise the citations to the California Public Records Act pursuant to changes in the Government Code.* *> Legal Update 40: The Service updated this procedure to reflect recent amendments to the Public Contract Code that extended authorization for districts to enter into job order contracts and requirements that contractors use a workforce that involves apprenticeship occupations in the building and construction trades.*	10/31/2024	Recommendation Requested
BP 6520 Security for District Property	Non 10+1	*> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards.*	10/31/2024	Recommendation Requested
AP 6520 Security for District Property	Non 10+1	*> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards.*	10/31/2024	Recommendation Requested

POLICIES & PROCEDURES 2024-25 ANNUAL REVIEW LIST AS OF 9/19/2024

Title	10+1?	Reason	Current Step Date	Current Step
BP 6610 Local, Minority, Women, and Veteran Owned Enterprise Program	Non 10+1	*> Chapter Lead: Requested changes to align with SBCCD goals and legal constraints.*	10/31/2024	Recommendation Requested
BP 6620 Naming of Buildings and Other Properties	Non 10+1	*> For information only to support review of AP 6620*	10/31/2024	Recommendation Requested
AP 6620 Naming of Buildings and Other Properties	Non 10+1	*> Request from CHC VPI Wurtz and CHC Development Director Riggs to revise amounts*	10/31/2024	Recommendation Requested
BP 6700 Civic Center and Other Facilities Use	Non 10+1	*> Legal Update 44: The Service updated this policy to align with changes in the Education Code.*	10/31/2024	Recommendation Requested
AP 6700 Civic Center and Other Facilities Use	Non 10+1	*> Legal Update 43: The Service updated this procedure to align with the Education Code.*	10/31/2024	Recommendation Requested
BP 6910 Housing	Non 10+1	*> Legal Update 42: The Service updated this policy to identify how a district may prioritize and restrict occupancy in affordable housing, to include language regarding prioritizing affordable housing for students, and to include language regarding data collection pursuant to changes in the Education Code and Health and Safety Code.* *> Legal Update 41: The Service updated this policy to delete a legal reference to Education Code Sections 94110 et seq., to add a reference to Education Code Section 76010, and to remove provisions required by that section.* *> Legal Update 38: The Service updated this procedure to add optional language to highlight diversity, equity, and inclusion issues.*	10/31/2024	Recommendation Requested
AP 6910 Housing	Non 10+1	*> Legal Update 44: Updated to add a usage note regarding a district's ability to offer groups priority for housing.* *> Legal Update 42: The Service updated this procedure to identify how a district may prioritize and restrict occupancy in affordable housing and to include language regarding data collection pursuant to changes in the Education Code and Health and Safety Code.* *> Legal Update 41: The Service updated this procedure to delete a legal reference to Education Code Sections 94110 et seq., to add a reference to Education Code Section 76010, to remove provisions required by that section, and to update the template to align to current law.*	10/31/2024	Recommendation Requested
BP 6925 Refreshments or Meals Served at Meetings and District Events	Non 10+1	*>Chapter Lead to retire policy and procedure which is no longer relevant due to more efficient process*	9/19/2024	PPAC Approves Review Level
AP 6925 Refreshments or Meals Served at Meetings and District Events	Non 10+1	*>Chapter Lead to retire policy and procedure which is no longer relevant due to more efficient process*	9/19/2024	PPAC Approves Review Level
BP 7110 Delegation of Authority, Human Resources	Non 10+1	*> Minor clerical edit*	10/31/2024	Recommendation Requested
AP 7110 Delegation of Authority, Human Resources	Non 10+1	*> Legal Update 44: Updated to add a usage note regarding a district's ability to offer groups priority for housing.*	10/31/2024	Recommendation Requested

POLICIES & PROCEDURES 2024-25 ANNUAL REVIEW LIST AS OF 9/19/2024

Title	10+1?	Reason	Current Step Date	Current Step
BP 7150 Evaluation	10+1	*> Academic Senate Request at 11/14/2022 meeting to review process and timeliness (2022-23 carryover)* *> Legal Update 44: Updated to clarify the records a district shall update to reflect an affirmed name and gender pursuant to changes in the Education Code.*	10/31/2024	Recommendation Requested
AP 7150 Evaluation	10+1	*> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards. The Service also updated this procedure to align content to the ACCJC Accreditation Standard and add a usage note to clarify optional language.* *> Academic Senate Request at 11/14/2022 meeting to review process and timeliness (2022-23 carryover)*	10/31/2024	Recommendation Requested
BP 7160 Professional Development	10+1	*> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standard and add supporting language pursuant to the 2024 changes in the ACCJC Accreditation Standards.*	10/31/2024	Recommendation Requested
AP 7160 Professional Development	10+1	*> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards. The Service also updated this procedure to align content to the ACCJC Accreditation Standard.*	10/31/2024	Recommendation Requested
AP 7211 Faculty Service Areas, Minimum Qualifications, and Equivalencies	10+1	*> Legal Update 44: Updated to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards.*	10/31/2024	Recommendation Requested
AP 7235 Probationary Period - Classified Employees	Non 10+1	*> Legal Update 42: The Service updated this procedure to implement requirements in non-merit system districts regarding employees who do not successfully complete their probationary period pursuant to changes in the Education Code.* *> Legal Update 40: The Service updated this procedure to reflect recent legislation that shortened the probationary period for classified employees and to clarify this change is not applicable to collective bargaining agreements entered into before January 1, 2022.*	10/31/2024	Recommendation Requested
AP 7237 Layoffs	Non 10+1	*> Legal Update 40: The Service updated this procedure to add legal citations regarding new requirements for layoffs and hearing rights of classified employees. (carryover from 2022-23)*	10/31/2024	Recommendation Requested
BP 7240 Confidential Employees	Non 10+1	*> Legal Update 42: The Service updated this policy to align with updated Title 5 regulations.*	10/31/2024	Recommendation Requested
AP 7240 Confidential Employees	Non 10+1	*> FYI Only*	10/31/2024	Recommendation Requested
BP 7250 Educational Administrators	10+1	*> Request from Chapter Lead to reverse 10+1 Designation.* *> Legal Update 42: The Service updated this policy to align with updated Title 5 regulations.* *> Legal Update 38: The Service updated this policy to add clarifying language regarding the term "vacancy" as used in this policy. (2022-23 carryover)* *> Other Chapter Lead review. (2022-23 carryover)*	10/31/2024	Recommendation Requested
AP 7250 Educational Administrators	10+1	*> Request from Chapter Lead to remove 10+1 Designation* *> Minor Clerical Edit*	10/31/2024	Recommendation Requested
BP 7260 Classified Supervisors, Managers and Administrators	Non 10+1	*> Legal Update 42: The Service updated this policy to align with updated Title 5 regulations.*	10/31/2024	Recommendation Requested
AP 7260 Classified Supervisors, Managers and Administrators	Non 10+1	*> FYI Only*	10/31/2024	Recommendation Requested

POLICIES & PROCEDURES 2024-25 ANNUAL REVIEW LIST AS OF 9/19/2024

Title	10+1?	Reason	Current Step Date	Current Step
BP 7340 Leaves	10+1	*> Request from Chapter Lead to remove 10+1 Designation.* *> Legal Update 44: Updated to add a citation to the Government Code and add language providing leave for reproductive loss pursuant to changes in the Government Code.* *> Legal Update 42: The Service updated this policy to add legal citations.* *> Legal Update 40: The Service updated this policy to include references to Government Code Sections 12945.2 and 12945.21. (2022-23 carryover)*	10/31/2024	Recommendation Requested
AP 7340 Leaves	10+1	*> Request from Chapter Lead to remove 10+1 Designation* *> Legal Update 44: Updated to add a legal citation regarding leave for reproductive loss pursuant to changes in the Government Code.*	10/31/2024	Recommendation Requested
AP 7346 Employees Called to Military Duty	Non 10+1	*> Legal Update 44: Updated to align with language from the Uniformed Services Employment and Re-employment Rights Act of 1994 ("USERRA"), the Education Code, and the Military and Veterans Code.*	10/31/2024	Recommendation Requested
BP 7360 Discipline & Dismissal - Academic Employees	Non 10+1	*> Minor Clerical Edit*	10/31/2024	Recommendation Requested
AP 7360 Discipline and Dismissal - Academic Employees	Non 10+1	*> Legal Update 42 Addendum: The Service updated this procedure to align with updated Title 5 regulations, add legal references, move some detail from the board policy to this procedure, and ensure consistent formatting between this procedure and the BP 7600 template.* *> Legal Update 42: The Service updated this procedure to add new legal requirements that law enforcement agencies obtain approval from the governing board before purchasing, raising funds for, or acquiring military equipment.* *> Legal Update 40: The Service updated this procedure to reflect recent clarifications to the requirements for placement on involuntary paid administrative leave. (2022-23 carryover)* *> Legal Update 38: The Service updated this procedure to add optional language to highlight diversity, equity, and inclusion issues.*	10/31/2024	Recommendation Requested
BP 7365 Discipline & Dismissal - Classified Employees	Non 10+1	*> Minor Clerical Edit*	10/31/2024	Recommendation Requested
AP 7365 Discipline and Dismissal - Classified Employees	Non 10+1	*> Legal Update 42: The Service updated this procedure to implement requirements related to employee status during discipline proceedings pursuant to changes in the Education Code.*	10/31/2024	Recommendation Requested

POLICIES & PROCEDURES 2024-25 ANNUAL REVIEW LIST AS OF 9/19/2024

Title	10+1?	Reason	Current Step Date	Current Step
BP 7600 District Police Department	Non 10+1	*> Legal Update 43: The Service updated this policy to clarify that Chief(s) of Police need not report to the CEO.* *> Legal Update 42 Addendum: The Service updated this policy to align with updated Title 5 regulations, make language corrections, move some detail to the accompanying procedure, and ensure consistent formatting between this policy template and the AP 7600 template.* *> Legal Update 42: The Service updated this policy to add new legal requirements that law enforcement agencies establish a board policy before purchasing, raising funds for, or acquiring military equipment.* *> Legal Update 40: The Service updated this procedure to add new legal requirements that law enforcement agencies obtain approval from the governing board before purchasing, raising funds for, or acquiring military equipment. (2022-23 carryover)* *> Legal Updates 38: The Service updated this procedure to add optional language to highlight diversity, equity, and inclusion issues. (2022-23 carryover)*	10/31/2024	Recommendation Requested

Title	10+1?	Reason	Current Step Date	Current Step
AP 7600 District Police Department	Non 10+1	*> Legal Update 42 Addendum: The Service updated this policy to align with updated Title 5 regulations, make language corrections, move some detail to the accompanying procedure, and ensure consistent formatting between this policy template and the AP 7600 template.* *> Legal Update 42: The Service updated this policy to add new legal requirements that law enforcement agencies establish a board policy before purchasing, raising funds for, or acquiring military equipment.* *> Legal Update 40: The Service updated this procedure to add new legal requirements that law enforcement agencies obtain approval from the governing board before purchasing, raising funds for, or acquiring military equipment. (2022-23 carryover)* *> Legal Updates 38: The Service updated this procedure to add optional language to highlight diversity, equity, and inclusion issues. (2022-23 carryover)*	10/31/2024	Recommendation Requested

BP 5500 Standards of Student Conduct

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 42: The Service updated this policy to add legal citations.

Level 3 Review Schedule

03/18/24 ♦ Recommendation Received

04/08/24 ♦ PPAC Approves Review Level
04/09/24 ♦ Level 2 to Constiutents and AS for Feedback
04/17/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input
05/13/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3
05/15/24 ♦ AS Reviews Level 3 for Final Input
08/15/24 ♦ PPAC Reviews Final AS Input
09/12/24 ♦ BOT 1st Read
10/10/24 ♦ BOT Final Approval

Begin Recommendation for BP 5500 Standards of Student Conduct

~~*(Replaces current SBCCD BP 5500)*~~

The Chancellor shall establish procedures for the imposition of discipline on students in accordance with the requirements for due process of the federal and state laws and regulations.

The Chancellor shall establish procedures that clearly define the conduct that is subject to discipline, and shall identify potential disciplinary actions, including but not limited to the removal, suspension, or expulsion of a student.

The Board shall consider any recommendation from the Chancellor for expulsion. The Board shall consider an expulsion recommendation in closed session unless the student requests that the matter be considered in a public meeting. Final action by the Board on the expulsion shall be taken at a public meeting.

The procedures shall be made widely available to students through the college catalog and other means.

References:

Education Code Sections 66300, ~~and~~ 66301, and 76120;
ACCJC Accreditation Standards ~~I.C.8 and 10 (formerly II.A.7.b)~~ 2

End Recommendation for BP 5500 Standards of Student Conduct

AP 5500 Standards of Student Conduct

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.
> Chapter Lead Changes resulting from legal review of BP

Level 3 Review Schedule

03/18/24 ♦ Recommendation Received

04/08/24 ♦ PPAC Approves Review Level
04/09/24 ♦ Level 2 to Constiutents and AS for Feedback
04/17/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input
05/13/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3
05/15/24 ♦ AS Reviews Level 3 for Final Input
08/15/24 ♦ PPAC Reviews Final AS Input
09/12/24 ♦ BOT 1st Read
10/10/24 ♦ BOT Final Approval

Begin Recommendation for AP 5500 Standards of Student Conduct

~~*(Replaces current SBCCD AP 5500)*~~

Standards of Student Conduct

The District may impose discipline for the commission, or attempted commission, of the following types of violations by Students, or for aiding or abetting, inciting, conspiring, assisting, hiring or encouraging another person to engage in a violation of this Standards of Student Conduct, or for any violation of state or Federal law. Being under the influence of drugs and/or alcohol, or the existence of other psychological impairment does not excuse a violation of this Standards of Student Conduct.

1. Academic Misconduct. All forms of academic misconduct including, but not limited to, cheating, fabrication, plagiarism, or facilitating academic dishonesty.
2. Alcohol. Manufacture, distribution, dispensing, possession, use, consumption or sale of, or the attempted manufacture, distribution, dispensing, distribution, consumption or sale of alcohol that is unlawful or otherwise prohibited by, or not in compliance with, District policy, administrative procedures, or campus regulations.
3. Assault/Battery. Assault, battery, or any threat of force or violence upon a Student or upon any Member of the District Community. This includes, but is not limited to:
    1. Inflicting bodily harm upon any Member of the District Community;
    2. taking any action for the purpose of inflicting bodily harm upon any Member of the District Community;
    3. taking any reckless, but not accidental action, from which bodily harm could result to any Member of the District Community;
    4. Causing a Member of the District Community to believe that the offender or their agent may cause bodily harm to that person or any member of their family or any other Member of the District Community;
    5. Inflicting or attempting to inflict bodily harm on oneself.
4. Bias. Bias-related incidents are behavior that constitutes an expression of hostility against a person or property or another due to the

AP 5500 Standards of Student Conduct

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

targeted person's race, religion, sexual orientation, ethnicity, national origin, gender, age, marital status, political affiliation, or disability. These acts or behaviors may not rise to the level of a crime, or a violation of state or federal law, but may constitute to creating an unsafe, negative, or unwelcome environment for the targeted person.

~~4.~~5. Bullying. Defined as the aggressive and hostile acts of an individual or group of individuals which are intended to humiliate, mentally or physically injure or intimidate, and/or control another individual or group of individuals.

6. Continued Misconduct or Repeat Violation. Repeated misconduct or violations of this Policy, when other means of correction have failed to bring about proper conduct.

~~5.~~7. Cyber Bullying. Defined as bullying an individual using any electronic form, including, but not limited to, the Internet, interactive and digital technologies, or mobile phones.

~~6.~~8. Dating Violence. Violence committed by a member of the District Community who is, or has been, in a social relationship of a romantic or intimate nature with the victim.

~~7.~~9. Destruction of Property. The damaging, destroying, defacing, or tampering with District Property or the property of any person or business on District Property or at a District function, including but not limited to, taking down, defacing, or otherwise damaging District authorized posters, handbills and/or notices posted on District property.

~~8.~~10. Discrimination. Unlawful discrimination against a person on the basis of race, ethnicity, color, religion, national origin, sex, age, disability, military or veteran status, gender identification, gender expression, marital status; sexual orientation, or genetic information, except where such distinction is authorized by law.

~~9.~~11. Dishonesty. All forms of dishonesty including but not limited to fabricating information, furnishing false information, or reporting a false emergency to the District.

~~10.~~12. Disorderly or ~~lewd~~ Lewd ~~conduct~~Conduct. Engaging in disorderly or lewd, indecent or obscene behavior on District Property or at a District function.

~~11.~~13. Disruption of Educational Process. Destruction or disruption on or off District Property of the District educational process(es), including but not limited to interrupting, impeding, obstructing or causing the interruption or impediment of any class (regardless of modality), lab, administrative office, teaching, research, administration, disciplinary procedures, District activity or District authorized Student activity or administrative process or other District function; or disturbing the peace on District Property or at any District function.

~~12.~~14. Disruptive Behavior. Disruptive behavior, disobedience, profanity, vulgarity, or the open defiance of the authority of or abuse of District personnel, or which adversely ~~effects~~ affects the delivery of educational services to Students and the District Community.

~~13.~~15. Disturbing the Peace. Disturbing the peace and good order of the District by, among other things, fighting, quarreling, disruptive behavior, or participation in a disturbance of the peace or unlawful assembly.

~~14.~~16. Drugs. Unlawful or attempted manufacture, distribution, dispensing, possession, use, distribution or sale of, controlled substances, dangerous drugs, restricted dangerous drugs or narcotics, as those terms are used in state or federal statutes on District Property or at any District function. Possession of medicinal marijuana on District premises is prohibited.

~~15.~~17. Endangering the Welfare of Others. Violation of any state or federal law relating to the placing at risk of physical or emotional harm of a member of the District Community.

~~16.~~18. Failure to Appear. Failure to appear before a District official when directed to do so.

~~17.~~19. Failure to Comply or Identify. Failure to identify oneself to, or comply with the directions of, a District employee when requested.

~~18.~~20. Failure to Repay Debts or Return District Property. Failure to (a) repay debts to the District; (b) return District property; (c) return property of any member of the District Community.

~~19.~~21. False Report of Emergency. Knowingly and purposefully, causing, making, and/or circulating a false report or warning of a fire,

AP 5500 Standards of Student Conduct

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

explosion, crime, or other catastrophe.

~~20.~~22. Forgery. Any forgery, alteration, or misuse of any District document, record, key, electronic device, or identification, or knowingly furnishing false information to a District official.

~~21.~~23. Fraud. Any attempt to steal, take, carry, lead, or take away the personal property of another, or who fraudulently appropriated property which has been entrusted to him/~~ or~~ her/they, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or property, or who causes or procures or obtains credit and thereby, or fraudulently gets or obtains possession of money, or property, or obtains the labor or service of another, is guilty of theft.

~~22.~~24. Gambling. Unauthorized gambling on District Property or at any District function.

~~23.~~25. Harassment/Bullying. A specific act, or series or acts, of a verbal or physical nature, including threats, intended to annoy, intimidate, pester, aggravate, irritate, dominate, ridicule, or cause fear to a member of the District Community, occurring within the jurisdiction of the District as set forth in Section 1.4.

~~24.~~26. Hateful Behavior. Hateful behavior aimed at a specific person or group of people.

~~25.~~27. Hazing. Participation in hazing or any method of initiation or pre-initiation into a campus organization or other activity engaged in by the organization or members of the organization at any time that causes, or is likely to cause, physical injury or personal degradation or disgrace which can inflict psychological or emotional harm to any Student or other person.

~~26.~~28. Infliction of Mental Harm. (a) Inflicting mental harm upon any member of the District Community; (b) taking any action for the purpose of inflicting mental harm upon any Member of the District Community; (c) taking any reckless, but not accidental action, from which mental harm to Member of the District Community could result; (d) causing a Member of the District Community to believe that the Student or their agent may cause mental harm to that person or any member of their family or any other member of the District Community; (e) any act which purposefully demeans, degrades, or disgraces any person.

~~27.~~29. Library Materials. Cutting, defacing, or otherwise damaging or theft of college library or bookstore materials or property.

AB. Misrepresentation. A false statement or representation based upon the intentional disregard of false or possibly false information, or knowingly entering into a transaction based upon false information, or misrepresenting oneself to be an agent, employee, or representative of the District or its colleges.

AC. Misuse of Identification. Transferring, lending, borrowing, altering or unauthorized creation of identification.

AD. Possession of Stolen Property. Possession of District Property, or the property of any other person, when the Student knows or reasonably should know, that the property was stolen.

AE. Possession of Weapons. Unauthorized possession, use, storage, or manufacture of explosives, dangerous chemicals, firebombs, firearms, or other destructive devices or weapons as defined in Section K of Appendix A.

AF. Public Intoxication. Public intoxication or being under the influence of alcoholic beverages, any illegal narcotics, or any substance that causes impairment on District/College Property or at any District/College function.

AG. Sexual Harassment. Sexual harassment against a member of the District Community. Sexual harassment is defined as (a) unwelcome verbal harassment, e.g., epithets, derogatory comments, or slurs; (b) physical harassment, e.g., assault, impeding or blocking movement, or any physical interference with normal work or movement when directed at an individual; (c) visual forms of harassment, e.g., derogatory posters, cartoons, or drawings; (d) unwelcome sexual advances, requests for sexual favors; or (e) an intimidating, hostile, or offensive environment. "Unwelcome conduct" is defined as conduct which the member of the District Community does not solicit or initiate, and which the person regards as undesirable or offensive.

AH. Sexual Misconduct. C~~c~~omprises a broad range of unwelcome behaviors focused on sex and/or gender that may or may not be sexual in nature. Any intercourse or other intentional sexual touching or activity without the other person's consent is sexual assault, is a form of Sexual Misconduct under this Procedure. Sexual Misconduct is any form of gender-based harassment, including, but not limited to, sexual harassment, sexual assault, and sexual exploitation, as well as harassment based on gender identity, gender expression, and non-conformity with gender stereotypes. Sexual misconduct may also include acts of a sexual nature, including acts of stalking, domestic

AP 5500 Standards of Student Conduct

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

violence, and dating violence, intimidation, or for retaliation following an incident where alleged Sexual Misconduct or has occurred. Sexual Misconduct can occur between strangers or acquaintances, or people who know each other well, including between people involved in an intimate or sexual relationship, can be committed by anyone regardless of gender identity and can occur between people of the same or different sex or gender.

AI. Serious Injury or Death. Any intentional, unintentional or reckless action or conduct which results in serious injury or death to a Member of the District Community or their family.

AJ. Smoking. Smoking in an area where smoking has been prohibited by law or regulation of the District.

AK. Stalking. Stalking behavior in which a Student repeatedly engages in the course of conduct directed at another person and makes a credible threat with the intent to place that person in reasonable fear for ~~his or her~~their safety, or the safety of ~~his/her/ or~~ their~~her~~ family; where the threat is reasonably determined by the College Conduct Officer to create substantial emotional distress, torment, create fear, or to terrorize the person.

AL. Sexual Stalking. The course of conduct directed at a specific person that would cause a reasonable person to feel fear or suffer substantial emotional distress due to another's sexual interest or gender-based stalking. Stalking involves repeated and continued harassment of a sexual or gender-based nature, against the expressed consent of another individual, which causes the targeted individual to feel emotional distress, including fear or apprehension. Such stalking behaviors may include: pursuing or following; unwanted communication or contact—including face-to-face encounters, telephone calls, voice messages, electronic messages, web-based messages, text messages, unwanted gifts, etc.; trespassing; and surveillance or other types of observation.

AM. Theft or Abuse of District's Computers or Electronic Resources. Theft or abuse of District computers and other District electronic resources such as computer and electronic communications facilities, systems, and services. Abuses include (but are not limited to) unauthorized entry, use, transfer, or tampering with the communications of others, and interference with the work of others, and with the operation of a computer and electronic communications facilities, systems, and services. Theft or attempted theft of any kind, including seizing, receiving, or concealing property with knowledge that is has been stolen, is prohibited. Sale, possession, or misappropriation of any property or services without the owner's permission is also prohibited.

AN. Theft or Conversion of Property. Theft or conversion of District Property or services, or the property of any person or business on District Property or at a District function, or possession of any property when the Student had the knowledge or reasonably should have had knowledge that it was stolen.

AO. Trespass and Unauthorized Possession. Unauthorized or forcible trespass on, entry to, possession of, receipt of, or use of any District services, grounds, equipment, resources, properties, structures, vehicles, boats, water craft or facility, including the unauthorized use of District's name, insignia, or seal without permission or authorization.

AP. Unauthorized Recording. Recording any person on District Property or at any District function without that person's knowledge or consent. This definition shall not apply to recordings conducted in public, in a commonly recognized public forum.

AQ. Unauthorized Use of Course or Copyrighted Materials. Students of the District will abide by all aspects of United States copyright law, Title 17 of the United States Code, to the extent possible, under the authoritative interpretation of the law. Students shall not reproduce copyrighted materials without prior permission of the copyright owner, except as allowed by the "fair use" doctrine. In addition, Students shall not sell, prepare, or distribute for any commercial purpose any course lecture notes or video or audio recordings of any course unless authorized by the District in advance and explicitly permitted by the course instructor in writing. The unauthorized sale or commercial distribution of course notes or recordings by a Student is a violation of these Policies whether or not it was the Student or someone else who prepared the notes or recordings. Copying for any commercial purpose handouts, readers or other course materials provided by an instructor as part of a District course unless authorized by the District in advance and explicitly permitted by the course instructor or the copyright holder in writing (if the instructor is not the copyright holder).

AR. Unauthorized Use of District Keys. Unauthorized use, distribution, duplication or possession of any keys issued for any building, laboratory, facility, room, or other District Property.

AS. Unauthorized Use of Electronic Devices. Unauthorized use of an electronic device on District property or at any District function, including but not limited to, classes, lectures, labs, and field trips.

AT. Unauthorized Use of Property or Services. Unauthorized use of property or services or unauthorized possession of District Property or

AP 5500 Standards of Student Conduct

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

the property of any other person or business.

AU. Unreasonable Demands. Placing repeated, hostile, or unreasonable demands on District staff.

AV. Unwelcome Conduct: ~~conduct~~ Conduct of a sexual, gender-based, or harassing nature, which is considered unwelcome if a person did not request or invite it, and considered the conduct to be unwelcome, undesirable, or offensive. Unwelcome conduct may take various forms, including name-calling, graphic or written statements (including the use of cell phones or the Internet), hazing, bullying, or other conduct that may be physically or psychologically threatening, harmful, or humiliating. Unwelcome conduct does not have to include intent to harm, or directed at a specific target, or involve repeated incidents. Unwelcome conduct can involve persons of the same or opposite sex.

AW. Violation of Driving Regulations. Driving unsafely on District property or while taking part in any District function, or repeated violation of District parking regulations.

AX. Violation of Health & Safety Regulations. Violation of any health, safety or related regulations, rule or ordinance on District property or at any District function.

AY. Violation of Law. Violation of any federal, state or local law on District property, at a District function or involving a member of the District Community.

AZ. Violation of Posted District Rules. Violation of any rule or regulation posted on District property by the District or the College, or printed in any District publication.

BA. Violation of Published Computer/Network Usage Policy(s), Procedures, or Guidelines.

1. Accessing and/or without permission altering, damaging, deleting, destroying, or otherwise using any data, computer, computer system, or computer network belonging to or used by the District or any Member of the District Community.
2. Accessing and/or without permission taking, copying, or making use of any data from a computer, computer system, or computer network, or taking or copying any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network belonging to or used by the District or any Member of the District Community.
3. Using or causing to be used District computer services without permission.
4. Accessing and/or without permission adding, altering, damaging, deleting, or destroying any data, computer software, or computer programs which reside or exist internal or external to a computer, computer systems, or computer network belonging to or used by the District or any Member of the District Community.
5. Disrupting or causing the disruption of computer services or denying or causing the denial of computer services to an authorized user of a computer, computer system, or computer network belonging to or used by the District or any Member of the District Community.
6. Providing or assisting in providing a means of accessing, without permission, a computer, computer, system, or computer network belonging to or used by the District or any Member of the District Community.
7. Accessing or causing to be accessed without authorization any computer, computer system, or computer network belonging to or used by the District or any Member of the District Community.
8. Introducing any computer contaminant or virus into any computer, computer system, or computer network belonging to or used by the District or any Member of the District Community.
9. Sending any message using any computer system or network without authorization or sending any message in the name of another person or entity.
10. Using any account or password without authorization.
11. Allowing or causing to be used an account number or password by any other person without authorization.
12. Accessing or causing to be accessed, downloading or causing to be downloaded, pornographic or obscene materials except when accessing a pornographic website which is part of the instructional process or assignment for a class the Student is currently enrolled in.

AP 5500 Standards of Student Conduct

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

13. Use the District's systems or networks for commercial purposes; for example, by performing work for profit with District resources in a manner not authorized by the district.

~~13.~~14. "Cyberstalking", which is to be understood as any use of the college or district computer system, computer network, or computer programs to stalk another person via excessive messages or inquiries, inappropriate or threatening messages, racially motivated communications, photos or other means of communication.

~~14.~~15. Inappropriate Usage of Social Media. Using social media to harass, intimidate, or threaten other individuals. Usage of social media that will have indirect or direct impact on an individual or interference with the educational process.

References:

Education Code Sections 66300, and 66301~~, 66302, 72122, and 76030-76038;~~
ACCJC Accreditation Standard~~I.C.8 and 10~~ 2

End Recommendation for AP 5500 Standards of Student Conduct

9/13/2024~~9/11/2024~~

BP 2015 Student Trustees

Non 10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Torres ♦ No Matching BP or AP Exists

Reasons for Review

> Legal Update 44 - Updated to add voting privileges for student members of the governing board and clarify the student member's rights pursuant to changes in the Education Code.
> Chapter Lead request to improve accuracy and efficiency, and to reflect current practice.

Level 1 Review Schedule

07/03/2024 ♦ Recommendation Received

09/11/2024 ♦ BPPAC Review of Chapter 1 and 2 Recommendations
09/19/2024 ♦ PPAC Approves Review Level
09/20/2024 ♦ Level 1 to Constituents and AS for Info Only
10/10/2024 ♦ BOT 1st Read
11/14/2024 ♦ BOT Final Approval

Begin Recommendation for BP 2015 Student Trustees

~~*(Replaces current SBCCD BP 2060 and 2070)*~~

The Board of Trustees shall include ~~two~~ one ~~(2)~~ non-voting student member from each college in the district.~~s (one representing each college in the District)~~. The term of office shall be one year commencing June 1.

The student member shall be enrolled in and maintain a minimum of five ~~(5)~~ semester units in the District at the time of nomination and throughout the term of service. The student member is not required to give up employment with the District. The student shall maintain a 2.0 grade point average ~~(GPA)~~ during the term of office.

The student member shall be seated with the Board during the open session portion of meetings and shall be recognized as a full member of the Board at meetings. The student member is entitled to participate in discussion of issues and receive all materials presented to members of the Board, except for issues and items discussed in ~~(except for~~ closed session~~)~~. The student member shall be entitled to any mileage allowance necessary to attend Board meetings to the same extent as publicly elected trustees. The student member shall have the opportunity to cast an advisory vote immediately before the regular members of the Board cast votes. The student member's advisory vote shall not be included in determining the vote required to carry any measure before the Board.

The primary duties of the Student Trustees are to attend and participate in all open board meetings, other duties may include:

- Represent the District at community events
- Advocate for the colleges and students to the legislatures
- Attend ASO/Associated Student Government meetings
- Meet regularly with senior administrators

Pursuant to Education Code Section 72023.5, on or before May 15 of each year, the Board of Trustees shall consider whether to afford the student trustees any of the following privileges:

BP 2015 Student Trustees

Non 10+1 ♦ CCLC | Legally Required ♦ Chapter Lead Torres ♦ No Matching BP or AP Exists

- The privilege to receive compensation for meeting attendance in accordance with Board Policy 2725 Board Member Compensation ~~at a level of $210 per month~~. In the event a student trustee has an unexcused absence to a required meeting, the compensation shall be prorated for the pay period.
- The privilege to make and second motions.
- The privilege to attend closed sessions, other than closed sessions on personnel or collective bargaining matters, at the discretion of the Board.
- The privilege to cast an advisory vote, although the vote shall not be included in determining the vote required to carry any measure before the Board.
- The privilege to serve a term commencing on May 15 instead of on June 1 as stated in Ed Code.

Reference:
Education Code Section 72023.5

End Recommendation for BP 2015 Student Trustees

BP 2355 Decorum

Non 10+1 ♦ CCLC | Good Practice/Optional ♦ Chapter Lead Torres ♦ No Matching BP or AP Exists

Reasons for Review

> Legal Update 44 - Updated to add references to the Government Code and update language pursuant to changes in the Government Code.

Level 1 Review Schedule

07/03/2024 ♦ Recommendation Received

09/11/2024 ♦ BPPAC Review of Chapter 1 and 2 Recommendations
09/19/2024 ♦ PPAC Approves Review Level
09/20/2024 ♦ Level 1 to Constituents and AS for Info Only
10/10/2024 ♦ BOT 1st Read
11/14/2024 ♦ BOT Final Approval

Begin Recommendation for BP 2355 Decorum

The following will be ruled out of order by the presiding officer:

- Disrupting, disturbing, ~~or otherwise~~ impeding, or rendering infeasible the orderly conduct of the meeting.
- Physical violence or threats of physical violence directed toward any person or property.

In the event that any meeting is willfully interrupted by the actions of one or more persons so as to render the orderly conduct of the meeting unfeasible, the persons may be removed from the meeting room.

Speakers who engage in such conduct may be removed from the podium and denied the opportunity to speak to the Board for the duration of the meeting.

~~Before removal, a warning and a request that the persons curtail the disruptive activity will be made by the Chair of the Board. If the behavior continues, the persons may be removed by a vote of the Board, based on a finding that the person is violating this policy, and that such activity is intentional and has substantially impaired the conduct of the meeting.~~ Before removal for conduct other than an individual's use of force or a true threat of force, the presiding officer shall warn the individual that the behavior is disrupting the meeting and that failure to cease the behavior may result in the individual's removal. The presiding officer or their designee may then remove the individual if they do not promptly cease their disruptive behavior.

If order cannot be restored by the removal in accordance with these rules of individuals who are willfully interrupting the meeting, the Board may order the meeting room cleared and may continue in session. The Board shall only consider matters appearing on the agenda. Representatives of the press or other news media, except those participating in the disturbance, shall be allowed to attend any session held pursuant to this rule.

References:
Education Code Section 72121.5;
Government Code Section 54954.3 - subdivision (b), 54957.9, and 54957.95

End Recommendation for BP 2355 Decorum

BP 2430 Delegation of Authority to the Chancellor

Non 10+1 ♦ CCLC | Required to Meet Accrediting Standards ♦ Chapter Lead Torres ♦ Both BP & AP Exist

Reasons for Review

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

Level 1 Review Schedule

07/03/2024 ♦ Recommendation Received

09/11/2024 ♦ BPPAC Review of Chapter 1 and 2 Recommendations
09/19/2024 ♦ PPAC Approves Review Level
09/20/2024 ♦ Level 1 to Constituents and AS for Info Only
10/10/2024 ♦ BOT 1st Read
11/14/2024 ♦ BOT Final Approval

Begin Recommendation for BP 2430 Delegation of Authority to the Chancellor

The Board delegates to the Chancellor the executive responsibility for administering the policies adopted by the Board and executing all decisions of the Board requiring administrative action. The Board gives the Chancellor full authority to implement board policies and ensure effective operations and fulfillment of the institutional mission.

The Chancellor may delegate any powers and duties entrusted to them by the Board (including the administration of colleges and centers), but will be specifically responsible to the Board for the execution of such delegated powers and duties.

The Chancellor is empowered to reasonably interpret Board policy. In situations where there is no Board policy direction, the Chancellor shall have the power to act, but such decisions shall be subject to review by the Board. It is the duty of the Chancellor to inform the Board of such action and to recommend written board policy if one is required.

The Chancellor is empowered to develop administrative procedures for submittal to the board.

The Chancellor is expected to perform the duties contained in the Chancellor's job description and fulfill other responsibilities as may be determined in annual goal-setting or evaluation sessions. The Board, in consultation with the Chancellor, shall develop the job description and goals and objectives for performance.

The Chancellor shall ensure that all relevant laws and regulations are complied with, and that required reports are submitted in timely fashion.

The Chancellor shall make available any information or give any report requested by the Board as a whole. Individual trustee requests for information shall be met if, in the opinion of the Chancellor, they are not unduly burdensome or disruptive to District operations. Information provided to any trustee shall be made available to all trustees.

The Chancellor is delegated the authority to act on behalf of the Board in an emergency for the protection of life, health, and safety of individuals and the protection of property, and shall update the Board in a timely manner.

BP 2430 Delegation of Authority to the Chancellor

Non 10+1 ♦ CCLC | Required to Meet Accrediting Standards ♦ Chapter Lead Torres ♦ Both BP & AP Exist

The Chancellor is delegated the authority to confer with District Counsel in addressing legal matters of the District with the exception of legal matters directly affecting the Board relationship with the Chancellor.

The Chancellor is delegated the authority to accept written resignations.

The Chancellor shall act as the professional advisor to the Board in policy formation.

References:

Education Code Sections 70902(d) and 72400;
ACCJC Accreditation Standard~~s IV.B.5, IV.C.12, and IV.D.1 (formerly IV.B.1.j and IV.B.2)~~ 4.5

End Recommendation for BP 2430 Delegation of Authority to the Chancellor

AP 2430 Delegation of Authority to the Chancellor

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

Reasons for Review

> Should SBCCD Adopt CCLC Good Practice AP?
> Legal Update 44 - Updated to revise the reference to the ACCJC Accreditation Standard pursuant to the 2024 changes in the ACCJC Accreditation Standards.

Level 1 Review Schedule

07/03/2024 ♦ Recommendation Received

09/11/2024 ♦ BPPAC Review of Chapter 1 and 2 Recommendations
09/19/2024 ♦ PPAC Approves Review Level
09/20/2024 ♦ Level 1 to Constituents and AS for Info Only
10/10/2024 ♦ BOT 1st Read
11/14/2024 ♦ BOT Final Approval

Begin Recommendation for AP 2430 Delegation of Authority to the Chancellor

The Chancellor may delegate any powers and duties entrusted to ~~him/her/~~them by the Board (including the administration of colleges and centers) but will be specifically responsible to the Board for the execution of such delegated powers and duties.

The Chancellor shall be responsible for reasonable interpretation of board policy. In situations where there is no board policy direction, the Chancellor shall have the power to act, but such decisions shall be subject to review by the Board. It is the duty of the Chancellor to inform the Board of such action and to recommend written board policy if one is required.

The Chancellor is expected to perform the duties contained in the Chancellor job description and fulfill other responsibilities as may be determined in annual goal-setting or evaluation sessions.

The Chancellor shall ensure that all relevant laws and regulations are complied with, and that required reports are submitted in timely fashion.

The Chancellor delegates full responsibility and authority to the College Presidents to implement and administer delegated policies without interference and holds College Presidents accountable for the operation of the Colleges.

References:
Education Code Section 70902;
ACCJC Accreditation Standard 4.5

End Recommendation for AP 2430 Delegation of Authority to the Chancellor

BP 2715 Code of Ethics/Standards of Practice

Non 10+1 ♦ CCLC | Required to Meet Accrediting Standards ♦ Chapter Lead Torres ♦ No Matching BP or AP Exists

Reasons for Review

> Legal Update 44 - Updated to revise the reference to the ACCJC Accreditation Standard and add supporting language pursuant to the 2024 changes in the ACCJC Accreditation Standards. The Service also updated this policy to change a reference to the "Superintendent/President" to "[CEO]."

Level 1 Review Schedule

07/03/2024 ♦ Recommendation Received

09/11/2024 ♦ BPPAC Review of Chapter 1 and 2 Recommendations
09/19/2024 ♦ PPAC Approves Review Level
09/20/2024 ♦ Level 1 to Constituents and AS for Info Only
10/10/2024 ♦ BOT 1st Read
11/14/2024 ♦ BOT Final Approval

Begin Recommendation for BP 2715 Code of Ethics/Standards of Practice

~~(Replaces current SBCCD BP 2010)~~

The governing board functions effectively as a collective entity to promote the institution's values and mission and fulfill its fiduciary responsibilities. The governing board demonstrates an ability to self-govern in adherence to its bylaws and expectations for best practices in board governance.

The Board maintains high standards of ethical conduct for its members. Members of the Board are responsible ~~to~~ for establishing, ~~and~~ upholding, implementing and enforc~~e~~ing all laws and codes applying to the District. Given this basic charge, the activities and deliberations of the Board of Trustees will be governed by the following Code of Ethics:

Each member of the Board will:

- Avoid any situation that may constitute a conflict of interest and disqualify ~~him/her~~ themself from participating in decisions in which ~~he or she~~they have ~~has~~ a financial interest. Conflicts of interest may relate not only to the individual trustee but also to ~~his or her~~ their family and business associates, or transactions between the District and trustees, including hiring relatives, friends, and business associates as college employees.
- Recognize that the Board acts as a whole and that the authority rests only with the Board in a legally constituted meeting, not with individual members.
- Maintain confidentiality of all Board discussions held in closed session and recognize that deliberations of the Board in closed session are not to be released or discussed in public without the prior approval of the Board by majority vote, in compliance with BP 2315.
- As an agent of the public - entrusted with public funds - protect, advance, and promote the interest of all citizens maintaining independent judgment unbiased by private interests or special interest groups.

BP 2715 Code of Ethics/Standards of Practice

Non 10+1 ♦ CCLC | Required to Meet Accrediting Standards ♦ Chapter Lead Torres ♦ No Matching BP or AP Exists

- Ensure that the District, in compliance with all applicable Federal and State laws, does not discriminate on the basis of race, color, national origin, ancestry, marital status, age, religion, disability, sex, or sexual orientation in any of its policies, procedures or practices.
- In all decisions hold the educational welfare and equality of opportunity of the students of the District as ~~his or her~~ their primary concern; Board members should demonstrate interest in and respect for student accomplishments by attending student ceremonies and events.
- Attend and participate in all meetings insofar as possible, having prepared for discussion and decision by studying all agenda materials.
- Conduct all District business in open public meetings unless in the judgment of the Board, and only for those purposes permitted by law, it is appropriate to hold a closed session.
- Enhance ~~his or her~~their ability to function effectively as a trustee through devotion of time to study contemporary educational issues, as well as attendance at professional workshops and conferences on the duties and responsibilities of trustees.

Promote and maintain good relations with fellow Board members by:

- Respectfully working with other Board members in the spirit of harmony and cooperation and giving each member courteous consideration of ~~his or her~~their opinion.
- Respecting the opinion of others and abiding by the principle of majority rule.

Promote an effective working relationship with the Chancellor and district staff by:

- Providing the responsibility, necessary authority, and support to effectively perform their duties.
- Referring complaints and/or criticisms through the appropriate channels as previously agreed upon by the Chancellor and the Board.

Be an advocate of the District in the community by encouraging support for and interest in the San Bernardino Community College District.

All Board members are expected to maintain the highest standards of conduct and ethical behavior and to adhere to the Board's Code of Ethics. The Board will be prepared to investigate the factual basis behind any charge or complaint of trustee misconduct. A Board member may be subject to a resolution of censure by the Board should it be determined that trustee misconduct has occurred. Censure is an official expression of disapproval passed by the Board.

A complaint of trustee misconduct will be referred to the Board Executive Committee composed of the board chair, vice chair, and clerk. In a manner deemed appropriate by the committee, a fact-finding process shall be initiated and completed within a reasonable period of time to determine the validity of the complaint. The committee shall be guided in its inquiry by the standards set forth in the Board's Code of Ethics as defined in policy. The trustee subject to the charge of misconduct shall not be precluded from presenting information to the committee. The committee shall, within a reasonable period of time, make a report of its findings to the Board for action.

Reference:
ACCJC Accreditation Standard ~~IV.C.11 (formerly IV.B.1.a, e, & h)~~ 4.6

End Recommendation for BP 2715 Code of Ethics/Standards of Practice

BP 2731 Trustee Emeritus/Emerita/Emeriti

Non 10+1 ♦ Non CCLC ♦ Chapter Lead Torres ♦ No Matching BP or AP Exists

Reasons for Review

> Requested by Board Executive Committee.

Level 1 Review Schedule

09/09/2024 ♦ Recommendation Received

09/11/2024 ♦ BPPAC Review of Chapter 1 and 2 Recommendations
09/19/2024 ♦ PPAC Approves Review Level
09/20/2024 ♦ Level 1 to Constituents and AS for Info Only
10/10/2024 ♦ BOT 1st Read
11/14/2024 ♦ BOT Final Approval

Begin Recommendation for BP 2731 Trustee Emeritus/Emerita/Emeriti

The designation of trustee emeritus/a/i honors on former trustees who have made outstanding contributions to the District. This recognition fosters continued engagement with experienced leaders and enhances the District's ability to benefit from their institutional knowledge and community relationships. By granting trustee emeritus/a/i status, the District acknowledges the Board member's long-term service and leadership.

Process

Trustee emeritus/a/i status may be granted by unanimous vote of the Board, through formal adoption of a resolution, and is conferred upon former trustees who meet the criteria below. Any sitting Board member may submit a nomination for consideration to the Board Chair or Chancellor.

Criteria for Nomination

1. Served SBCCD for a minimum of eight consecutive years.
2. Served in a leadership role on behalf of the Board of Trustees.
3. Contributed significantly to the development of the District.
4. Provided meritorious service in representing SBCCD to the community.
5. Demonstrated a continuous commitment to strengthening educational opportunities for the community.
6. Officially left the Board within the past 12 months.

Privileges, Benefits & Courtesies

Emeritus/a/i status may confer privileges, benefits, and courtesies including, but not necessarily limited to:

1. An official certificate of Emeritus/a/i status signed by the Board Chair and Chancellor.
2. A District-issued card indicating Emeritus/a/i status thereby granting free or discounted rates for select District or College events.
3. Participation by invitation in public ceremonies of the District.
4. Library and Learning Resource Center privileges equivalent to those of current employees subject to District policy and administrative regulations.
5. Eligibility to participate by invitation in District professional development activities.
6. Parking privileges comparable to those of current employees subject to District policy and administrative regulations.
7. Continued use of District e-mail address subject to District policy and administrative regulations.

End Recommendation for BP 2731 Trustee Emeritus/Emerita/Emeriti

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

08/31/24 ♦ Estimated Receipt of Recommendation

09/19/24 ♦ PPAC Approves Review Level
09/20/24 ♦ Level 2 to Constiutents 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 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)

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

BP 5030 Fees

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

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 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 to 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

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

Level 2 Review Schedule

08/31/24 ♦ Estimated Receipt of Recommendation

09/19/24 ♦ PPAC Approves Review Level
09/20/24 ♦ Level 2 to Constiutents 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 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;

AP 5030 Fees

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

- 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);
  - 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)

AP 5030 Fees

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

- 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))
- 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)

AP 5030 Fees

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

- 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)
- 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)

AP 5030 Fees

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

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

$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

AP 5030 Fees

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

At cost - Optional Medical Supplies

$ 2.00 per item - Duplication of medical records

At cost - Birth Control Pills

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

$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

AP 5030 Fees

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

8. Student Representation Fee
9. Capital Outlay Fee
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

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

07/17/24 ♦ Recommendation Received

08/15/24 ♦ PPAC Approves Review Level
08/16/24 ♦ Level 2 to Constiutents and AS for Feedback
09/04/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input
09/19/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3
10/10/24 ♦ BOT 1st Read
11/14/24 ♦ 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

Level 2 Review Schedule

07/17/24 ♦ Recommendation Received

08/15/24 ♦ PPAC Approves Review Level
08/16/24 ♦ Level 2 to Constiutents and AS for Feedback
09/04/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input
09/19/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3
10/10/24 ♦ BOT 1st Read
11/14/24 ♦ BOT Final Approval

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.~~

AP 6925 Refreshments or Meals Served at Meetings and District Events

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

~~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 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 Constiutents 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

AP 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 Constiutents 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 Seurity 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

AP 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

AP 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. Thisclassification 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.

AP 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 Seurity Data Classification

AP 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 Constiutents 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.

AP 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.

AP 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;

AP 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).

AP 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

AP 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 Constiutents 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.

AP 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.

AP 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 Constiutents 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

The following table lists logging checks to be performed on a daily, weekly basis or

EXAMPLE SEEN 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 *Restricted* 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 Constiutents 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.

AP 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.

AP 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 Constiutents 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 Constiutents 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

AP 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: • 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.

AP 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

HIGH	• 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	1. Log incident in IT Service Desk 2. Notify IRC or designee 3. IRC will notify CIRT team members as needed
MEDIUM	• 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	1. Log incident in IT Service Desk 2. IRC will review and notify CIRT team members as needed.
LOW	• Password compromises – single user • Unauthorized access attempts • Account sharing • Account lockouts	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 Constiutents 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 HIPPA 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 Constiutents 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 unsecure 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.

AP 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

AP 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

AP 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 Constiutents 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.

AP 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.

AP 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.

AP 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

AP 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

AP 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)

AP 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)	**Sub-system Outage / Minor Damage** 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. 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.
Level 2 (Medium)	**Short Term Outage** 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. In this scenario, a key computer processing application is unavailable. Communication lines or portions of the network may be down. 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.

AP 3735 Information Security Disaster Recovery

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

Level 3 (High)	**Long Term Outage** Complete loss of a critical application for a period greater than one week but less than two weeks. 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. In this scenario, key portions of the computer processing environment are unavailable. Communication lines or portions of the network may also be down. The goal of the recovery process is to restore minimum critical application functionality either at the primary facility or at the Standby facility.
Level 4 (Critical)	**Total System Disaster** 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. 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. 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.

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 Constiutents 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:

AP 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 Constiutents 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.

AP 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 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

05/13/24 ♦ Recommendation Received

08/15/24 ♦ PPAC Approves Review Level
08/16/24 ♦ Level 2 to Constiutents and AS for Feedback
09/04/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input
09/19/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3
10/02/24 ♦ AS Reviews Level 3 for Final Input
10/17/24 ♦ PPAC Reviews Final AS Input
11/14/24 ♦ BOT 1st Read
12/13/24 ♦ 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.

Level 3 Review Schedule

05/13/24 ♦ Recommendation Received

08/15/24 ♦ PPAC Approves Review Level
08/16/24 ♦ Level 2 to Constiutents and AS for Feedback
09/04/24 ♦ AS Reviews Level 2 for Feedback and Level 3 for Initial Input
09/19/24 ♦ PPAC Hears Feedback on Level 2 and AS Initial Input on Level 3
10/02/24 ♦ AS Reviews Level 3 for Final Input
10/17/24 ♦ PPAC Reviews Final AS Input
11/14/24 ♦ BOT 1st Read
12/13/24 ♦ BOT Final Approval

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.~~

AP 4300 Field Trips and Excursions

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

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 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

AP 4300 Field Trips and Excursions

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

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