College Coordinating Council Meeting

Wednesday, November 14, 2018
A124 – President's Conference Room
9:00 a.m. – 10:00 a.m.

Type of Meeting: Regular
Note Taker: Patty McClure
Please Review/Bring: Agenda, Minutes

Committee Members:
Dr. Susan Lowry/Van Rider, Academic Senate
Jorge Hernandez, Associated Student Organization
Ed Knudson, President
Pamela Ford, Classified Union
Michelle Hernandez, Confidential/Management/Supervisory/Administrators
LaDonna Trimble, Deans
Dr. Scott Lee, Faculty Union
Vacant, Vice President of Academic Affairs
Mark Bryant, Vice President of Human Resources
Dr. Erin Vines, Vice President of Student Services

AGENDA

Items	Person(s) Responsible	Time	Action
STANDING ITEMS:			
I. Approval of Previous Minutes of October 10, 2018.	All		
II. Constituent Reports	All		
INFORMATION/DISCUSSION/ACTION ITEMS:			
III. AP 3720 – Computer, Network and Telecommunications Use	Rick	3 minutes	
IV. AP 3721 – Virtual Private Network (VPN)/Remote Access Procedure	Rick	3 minutes	
V. AP 3722- Acceptable Use Agreement	Rick	3 minutes	
VI. AP 6200 – Budget Preparation	Diana	5 minutes	
FUTURE AGENDA ITEMS:			
NEXT MEETING DATE: November 28, 2018			

College Coordinating Council Minutes

Wednesday, October 10, 2018
A124 – President's Conference Room
9:00 a.m. – 10:00 a.m.

Type of Meeting: Regular
Note Taker: Patty McClure
Please Review/Bring: Agenda, Minutes

Committee Members:
Van Rider, Academic Senate
Jorge Hernandez, Associated Student Organization - **ABSENT**
Ed Knudson, President - **ABSENT**
Pamela Ford, Classified Union
Michelle Hernandez, Confidential/Management/Supervisory/Administrators
LaDonna Trimble, Deans - **ABSENT**
Dr. Scott Lee, Faculty Union
~~Vacant, Vice President of Academic Affairs~~
Mark Bryant, Vice President of Human Resources
Dr. Erin Vines, Vice President of Student Services

MINUTES

Items	Person(s) Responsible	Time	Action
STANDING ITEMS:			
I. Approval of Previous Minutes of September 12, 2018.	All		The minutes were approved as presented.
II. Constituent Reports	All		**Dr. Lee** stated that ballots were going out for the second VP position. **Van** stated that the call for VP will be going out and that he will be covering on Budget. **Pamela** stated that the Annual Craft Fair will be held on November 10th from 9:00 a.m. – 3:00 p.m. and that the proceeds will go towards scholarships.
INFORMATION/DISCUSSION/ACTION ITEMS:			
III. AP 6330 – Purchasing	Diana	2 minutes	It was agreed to go to the November 13, 2018 board meeting.
IV. BP & AP 6340 – Bids and Contracts	Diana	2 minutes	It was agreed to go to the November 13, 2018 board meeting.
V. BP & AP 6380 – Vendors	Diana	2 minutes	It was agreed to go to the November 13, 2018 board meeting.
VI. AP 7360 – Discipline and Dismissal – Academic Employees	Mark	2 minutes	It was agreed to go back out to the constituent groups for another 30 days and return back for final approval.
VII. Guided Pathways – Committee	Van	2 minutes	Van will revise and send out via email. It was agreed to approve with the discussed revisions. The committee will

			meet on October 23rd and the call for membership will go out.
FUTURE AGENDA ITEMS:			
NEXT MEETING DATE: **October 24, 2018**			

AP 3720 Computer, Network and Telecommunications Use

References:

17 U.S.C. Section 101 et seq.;
Penal Code Section 502;
Cal. Const., Art. 1 Section 1;
Government Code Section 3543.1(b);
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45

The District Computer, Network and Telecommunications systems, and the data that resides upon them, are the sole property of Antelope Valley Community College District; except where explicitly addressed by collective bargaining agreements. The Computer, Network and Telecommunications systems are for District instructional and ~~work related~~work-related purposes only.

This procedure applies to all District students, faculty, ~~and~~ staff, and to others granted use of District information resources. ~~A user is defined as any individual or group who uses college technology or computing facilities~~resources.
This procedure refers to all District information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and telecommunication facilities owned, leased, operated, or contracted by the District. This includes, but is not limited to, personal computers, personal ~~digital assistants (PDAs)~~mobile devices, ~~handheld~~ computing or telecommunications devices, workstations, mainframes, minicomputers, and associated peripherals, software, networks, telephone and telecommunications equipment, including cellular telephones, and information resources, regardless of whether used for administration, research, teaching or other purposes.

AVC Information Technology Resource Guidelines

The District shall produce and maintain guidelines that clarify procedures or processes relating to the use of District information technologies. These guidelines shall be reviewed regularly for relevance and made available to the public.

Conditions of Use

Individual units within the District may define additional conditions of use for information resources under their control. These statements must be consistent with this overall procedure but may provide additional detail, guidelines and/or restrictions.

Account Provisioning and Deprovisioning

All employees and students are assigned an email account upon joining the college. Email is the official channel for all communications from the college. All employees and students are encouraged to check it regularly to stay current on all issues related

to instruction and services. Upon departure from the college, all students, retirees, and emeriti may retain their email account. Employee access that does not meet the above criteria may be deprovisioned upon separation. Access to services within myAVC will be deprovisioned two-years after departure. Accounts for persons no longer actively affiliated with the District will be disabled after one year of inactivity. If you need access to records that are within myAVC, please contact the appropriate office directly.

Legal Process

This procedure exists within the framework of the District Board Policy and state and federal laws. A user of District information resources who is found to have violated any of these policies will be subject to disciplinary action up to and including but not limited to loss of information resources privileges; disciplinary suspension or termination from employment or expulsion; and/or civil or criminal legal action.

Copyrights and Licenses

~~Computer user~~Users must respect copyrights and licenses to software and other on-line information.

Copying

Software protected by copyright may not be copied except as expressly permitted by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, from, or by any District facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.

Number of Simultaneous Users

The number and distribution of copies must be handled in such a way that the number of simultaneous users does not exceed the number of original copies purchased by the District, unless otherwise stipulated in the purchase contract.

Copyrights

In addition to software, all other copyrighted information (text, images, icons, programs, audio, video, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is prohibited in the same way that plagiarism of any other protected work is prohibited. ~~Refer to the AVC Computer Use and Electronic Mail Guidelines for additional information.~~

Integrity of Information Resources

~~Computer user~~Users must respect the integrity of computer-based information resources.

Modification or Removal of Equipment

Computer and telecommunications users must not attempt to modify or remove computer, network or telecommunications equipment, software, or peripherals that are allocated to other District users without proper authorization.

Unauthorized Use

Users must not interfere with others' access and use of the District computers. This includes but is not limited to: the sending of chain letters or excessive messages, either locally or off-campus; printing excess copies of documents, files, data, or programs, running ~~grossly~~ inefficient programs ~~when efficient alternatives are known by the user to be available~~that adversely impact performance of the network; unauthorized modification of system facilities, operating systems, or disk partitions; ~~attempting to crash or tie up a District computer or network;~~ and damaging or vandalizing District computing facilities, equipment, software or computer files.

Unauthorized Programs

Users must not intentionally develop or use programs which disrupt other ~~computer user~~users or which access private or restricted portions of the system, or which damage the software or

hardware components of the system. ~~Computer user~~Users must ensure that they do not use programs or utilities that interfere with other ~~computer user~~users or that modify normally protected or restricted portions of the system or user accounts. The use of any unauthorized or destructive program will result in disciplinary action as provided in this ~~procedure, and~~procedure and may further lead to civil or criminal legal proceedings.

Unauthorized Access

~~Computer user~~Users must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access.

Abuse of Computing Privileges

Users of District information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the District. For example, abuse of the networks to which the District belongs or the computers at other sites connected to those networks will be treated as an abuse of District computing privileges.

Reporting Problems

Any defects discovered in system accounting or system security must be reported promptly to the appropriate administrator so that steps can be taken to investigate and solve the problem.

Password Protection

A ~~computer user~~user who has been authorized ~~to use a~~for password-protected accounts may be subject to both civil and criminal liability if the user discloses their password or otherwise makes the account available to others.

Usage

~~Computer user~~Users must respect the rights of other ~~computer users~~. Attempts to circumvent these mechanisms in order to gain unauthorized access ~~to the system or to another person's information~~ are a violation of District procedure and maybe subject to civil or criminal lability ~~violate applicable law~~.

Unlawful Messages

Users may not use electronic communication facilities to send defamatory, fraudulent, harassing, obscene, threatening, malicious, or other messages that violate applicable federal, state or other law or District policy, or which constitute the unauthorized release of confidential information.

Commercial Use

Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions. District information resources may not be used for commercial purposes. Users are also reminded that the ".cc" and ".edu" domains on the Internet have rules restricting or prohibiting commercial use. ~~However, where legally permissible, District electronic media such as message boards or mail systems may be designated for selling or fundraising.~~

~~Information Belonging to Others Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, voice messages or passwords belonging to other users, without the permission of those other users.~~ [RS1]

Rights of Individuals

Users must not release any individual's (student, faculty, and staff) personal information to anyone without proper authorization.

User identification

Users shall not send communications or messages anonymously or without accurately identifying the originating account or station.

~~Political,~~ Personal and Commercial Use

The District is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state and local laws regarding sources of income, political activities, use of property and similar matters. Use of District resources for personal gain is expressly prohibited.

Political Use

District information resources must not be used for ~~partisan~~ political activities where prohibited by federal, state or other applicable laws.

Personal Use

District information resources should not be used for personal activities not related to appropriate District functions, except in a purely incidental manner.

Nondiscrimination

All users have the right to be free from any conduct connected with the use of Antelope Valley Community College District network, telecommunications and computer resources which discriminates against any person in violation of Board Policy 3410. No user shall use the District network, telecommunications or computer resources to transmit any message, create any communication of any kind, or store information which violates any District procedure regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

Disclosure

No Expectation of Privacy

The District reserves the right to monitor all use of the District network and computer resources to assure compliance with these policies. Users should be aware that they have no expectation of privacy in the use of the District network and computer resources. The District will exercise this right only for legitimate District purposes, including but not limited to ensuring compliance with this procedure and the integrity and security of the system.

Possibility of Disclosure

Users must be aware of the possibility of unintended disclosure of communications.

Retrieval

It is often possible for information entered on or transmitted via computer and communications systems to be retrieved, even if a user has deleted such information.

Public Records

The California Public Records Act (Government Code Sections 6250 *et seq.*) includes computer transmissions in the definition of "public record" and nonexempt communications made on the District network and computer must be disclosed if requested by a member of the public, in accordance with BP 3300 & AP3300.

Litigation

Computer transmissions and electronically stored information may be discoverable in litigation.

Dissemination and User Acknowledgment

All users shall be provided access to these procedures and be directed to familiarize themselves with them. Periodically users will be reminded of these procedures.

Users shall acknowledge that they have reviewed BP 3720 and the associated procedures and guidelines in the manner and frequency as specified in the IT Resource Guidelines. This acknowledgement is a condition of use of any District information technology resource.

Revised: 11/7/05, 1/8/07, 9/10/07

DRAFT

AP 3721 Virtual Private Network (VPN) / Remote Access Procedure

Reference:

An expansion of mobile employees, and the need for after hours and remote access by employees and partners necessitates procedures for such. Secure/encrypted access to college resources is essential for off campus, after hours, or vendor sponsored access. Permission to use the college's Virtual Private Network (VPN) is subject to the approval of the Executive Director, Technology, and is allowed only under the following circumstances:

Vendor Support of Network Services

~~The district relies on v~~Vendor support ~~to assist with the administration of~~ for select ~~network~~ computing or network resources~~systems~~ to facilitate ~~. Several departments have requested the ability to allow vendors and consultants to remotely connect to the district network in order to fix an~~ urgent ~~issue~~access, or to help ~~keep~~ reduce consultant ~~fees to a minimum by reducing the need for~~ travel expenses, or ~~and~~ in accommodation fors ~~when~~ services ~~could be~~ rendered from a distance. ~~Previously, AVC did not have the technology to allow vendors to connect to the district network without exposing the network to unnecessary risks.~~ Requests are to be submitted for review to help@avc.edu. Vendor VPN access will have a CMS or Administrative sponsor, will have a ninety (90) day expiration, and can be renewed by email request by the sponsor by email or support ticket.

Employee Remote Access

To ensure secure access of resources from outside the college network, employees will be granted VPN access for portable devices. Use of the VPN is expressly for access of college resources during in execution of the employee's duties. After hours use of VPN services for employees is still subject to Policy, Practices, and CBA conditions for overtime, and is subject to advanced approval of supervisors. Such accounts will have a one hundred eighty (180) day expiration date, and can be renewed by request of their supervisor by email or help desk ticket.

Access Requirements

Remote access to the district ~~network~~ resources~~is for contractors and vendor support personnel only~~, in accordance with application maintenance agreements or a well defined business need, must meet certain criteria. ~~–~~To defend the district network from malware and other potential threats ~~to network and data security~~, vendors, ~~and~~ contractors, and employees will ~~must meet certain security criteria before they will be allowed to connect to the network remotely~~use industry accepted best practices to ensure systems are safe and secure. ~~Contractor and vendor w~~Workstations must be current with operating system and application security patches and have anti-virus software ~~loaded and up to date~~ , before a connection with the AVC network will be established. Devices may be subject to interrogation by a remote security tool to ensure compliance. Failure to meet compliance will result in suspension of access.

Remediation ~~(For Vendors and Contractors)~~

If remote connection to the AVC network is denied because of insufficient security software, ~~the contractor or vendor simply has to~~ devices will need to be brought ~~update or install the missing components~~current (e.g., anti-virus or operating system patches) and attempt a

reconnection to the district remote access device. Contact the help desk and account will be reactivated for purposes of examination. The software on the remote access device (VPN client) will ensure that the workstation the contractor, ~~or~~ vendor or employee is connecting from has met AVC network security requirements. If all workstation prerequisites have been met, the software will establish the connection.

4/13/09
Revised: 01/07/2019 (anticipated adoption)

DRAFT

AP 3722 Acceptable Use Agreement

Reference:

Antelope Valley College (AVC) provides access to its ~~computing, communications and information~~technology resources ~~in to. These resources are the property of AVC and~~ support of the ~~delivery of the~~ college's academic mission and community ~~and accordingly, t~~. These resources (the equipment and content) are the property of AVC, and ~~hey~~ should be used responsibly. These resources include: the physical ~~data~~ and wireless communications network; ~~and~~ all college ~~computers, printers, scanners and other hardware~~equipment attached to that network, ~~, as well as all~~ portable hardware, system software, telephone systems, and means of access ~~to the Internet~~.

All employees, students, or ~~campus~~ visitor, are subject to the provisions of this policy, and services shall abide by this policy, and all applicable local, state, and federal statutes. ~~With regard to the~~Use of any ~~computing, communications and information~~ technology resources of Antelope Valley College ~~,~~ explicitly affirms acceptance of~~all users understand and agree to the following provisions~~ the following conditions of use:

- The district's ~~computing, communication and information~~technology resources are provided for the support of its educational and service goals. ~~and~~ T~~t~~he use of such resources for any other purposes is prohibited.
- Users may not use district resources for conducting a private business or for personal ~~financial~~ gain, or partisan political activities~~.~~.
- ~~However, i~~Incidental personal use is ~~permissible~~ permitted ~~so~~ as long as: (a) it does not violate state or federal law or AVC policy, (b) ~~it does not~~ consume~~s only more than~~ a trivial amount of ~~system~~ resources or time, (c) and, it does not interfere with productivity of ~~students or district employees~~the college, it's employees, students, or visitors.~~, and (d) it does not preempt any district activity. All users of district information technology resources and services shall abide by this policy along with any local, state, and federal law that may apply.~~
- ~~All users are subject to both the provisions of this policy, as well as any policies specific to the individual systems they use.~~
- To ~~protect~~ ensure, and safeguard, the integrity of computing resources, ~~passwords, access codes, or account names~~ account names and passwords must not be shared ~~with others~~. ~~Additionally, p~~Passwords will be subject to complexity requirements and users will be required to change their passwords periodically. ~~-~~ These specifications will be reviewed and published annually by the Information Technology Committee.
- ~~Most educational materials (both commercial and district employee created, including software) are protected under copyright. Any violation of the rights of a person or entity protected by copyright law is prohibited.~~ The unauthorized duplication, installation, or distribution of copyrighted ~~computer~~ software or content ~~utilizing the district's computing, communications and information resources is~~ is ~~specifically~~ expressly prohibited. Unauthorized software, installed on district ~~owned computers~~technology, ~~will not be supported and~~ may be removed if deemed ~~necessary~~in volition of copyright or district policy.
- Users may not bypass, utilize any ~~connect any system/equipment or install software~~device or ~~which~~ software, which circumvents authenticated protections to ~~could~~

allow any user to gains access to the district's systems or services. and information without coordinating with Information Technology Services (ITS).

- Users may not use district resources for conducting a private business or for personal financial gain.
- Intentionally sending or accessing pornography or patently obscene material other than for authorized research or instructional purposes is prohibited. The definition of "pornography" and "obscene" shall be as determined by law.
- Computer and information technology uUsers should consider be mindful of the inherently open nature of information transferred electronically, and should not assume an absolute degree of privacy or of authenticatedrestricted access to such information. The district provides the highest degree of security possible when transferring and hosting data, but disclaims responsibility if these security measures are circumvented and the information is compromised.
- The district is not responsible for loss of data, time delay, system performance, software performance, or any other damages arising from the use of district computing resources.
- Authorized district personnel may, while performing routine or investigative operations have access to data, including electronic mail, web browser information, and any other personal data stored on district computers.
- Except where explicitly addressed by labor agreements[RS1], a All content ofstored on district technology is deemed to be the property of the district, including that generated by incidental use.
- Student workstations are subject to routine monitoring. Computer screens attached to student workstations, particularly those accessing the Internet, may be periodically viewed by district personnel to monitor compliance with district policy. However, t
- The district shall not routinely or arbitrarily monitor incidental personal use of district resources by employees. Neither the district nor any employee shall disclose the contents of any observed personal data to any other person or entity except as required by law or Board Policy.
- Activities that place excessive strain on network resources should be avoided. Conducting activities such as Peer-to-peer (P2P) file sharing or use of any other similar technologies is prohibited and subject to disciplinary action.
- The confidentiality of student and employee information is protected under federal and state law and/or regulations. Any information regarding students or employees that might be accessed in the course of using an AVC computer may only be shared with those who are authorized to have such information. Employees and students may not change, alter, copy, or divulge any such information unless it is required to carry out an assignment. Access to, or alteration of, such information is expressly limited to execution of day-to-day assigned duties.
- Employees and students should ensure that their workstation is logged off, or locked, or shutdown, before stepping away from the computer.

Users found in violation of the district's computer and information technology use policies, are subject to disciplinary action, as described in the enforcement section of this document below.

DRAFT

Selected Examples of Unacceptable Use:

- Revealing/Sharing user-id or passwords ~~to~~ with others, or using someone else's account, or allowing ~~someone else to~~ use of your account by others.
- Attempting to defeat data protection schemes or altering network configurations to uncover security vulnerabilities.
- ~~Using someone else's account. Utilizing network or system id numbers/names that are not assigned for one's specific use on the designated system.~~
- Attempting to authorize, delete, or alter files or systems ~~not created by oneself~~ without proper authorization as described in the Computer Use and Electronic Mail Guidelines.
- Not complying with requests from AVC personnel to discontinue activities that ~~threaten~~ degrade or interrupt the integrity or stability of ~~computing~~ resources.
- ~~Attempting to defeat data protection schemes or to uncover security vulnerabilities.~~
- Connecting unauthorized personal equipment ~~wireless access points and other computer equipment~~ to the campus physical network without ~~coordinating~~ authorization from~~with~~ ITS. ~~(Devices such as PDAs, printers, and USB drives that connect to a computer and not directly to the network are acceptable.)~~
- ~~Registering an Antelope Valley College IP address with any other domain name.~~
- Unauthorized network scanning or attempts to intercept network traffic.
- Malicious disruptions ~~such as~~ , e.g., introducing a computer virus or malware to the campus network, or ~~.~~
- ~~H~~harassing or threatening ~~other users~~others ~~of the campus network~~.
- ~~Using district resources for partisan political activities where prohibited by federal, state or other applicable laws.~~

To ensure the integrity and reliability of ~~computer and communications~~ technology~~all~~ resources, ~~all~~ users are encouraged to repo~~r~~rt improper use and violations of this agreement. ~~Individuals may report suspected violations of this agreement~~ to an AVC faculty member, supervisor or administrator as appropriate.

Enforcement[1]

~~Individuals may report suspected violations of these guidelines to an AVC supervisor, faculty member or administrator as appropriate. Reports of violations that are received by ITS will be forwarded to the appropriate supervisor or administrator.~~

- Disciplinary action ~~may~~will be taken in accordance with AVC applicable policies, collective bargaining agreements, state or federal statutes.
- Minor infractions of these guidelines, or those that appear accidental in nature, are typically handled internally by the appropriate supervisor or administrator, in consultation with ~~ITS~~the Executive Director, Technology. In some situations it may be necessary to suspend account or computer access to prevent ongoing misuse.
- More serious infractions or repeated minor violations may result in the temporary or permanent loss of access.

[1] This section is taken directly from the ~~Computer Use and Electronic Mail Guidelines document~~AP 3720: Computer, Network, and Telecommunications Use.

- Offenses that are clearly in violation of local, state or federal laws will be reported to the Los Angeles County Sherrif's Department and -result in the immediate loss of access to computing resources and maybe subject to disciplinary suspension or termination from employment or expulsion; and/or civil or criminal legal action.

~~Disciplinary action may be taken in accordance with one or more of the following: AVC policies, California law or the laws of the United States.~~

~~Minor infractions of these guidelines or those that appear accidental in nature are typically handled internally by the appropriate supervisor or administrator, in consultation with ITS. In some situations it may be necessary, however, to suspend account or computer access to prevent ongoing misuse while the situation is under investigation.~~

~~More serious infractions, such as unauthorized use, attempts to steal passwords or data, unauthorized use or copying of licensed software, violations of college policies or repeated violations of minor infractions may result in the temporary or permanent loss of access to computing facilities.~~

~~Offenses that are clearly in violation of local, state or federal laws will result in the immediate loss of access to computing resources and will be reported to the appropriate law enforcement authorities. In addition, disciplinary action, up to and including dismissal, may be applicable under other AVC policies, guidelines or collective bargaining agreements.~~

10/11/10

Revised: ~~06~~01/~~08~~07/201~~5~~9 (anticipated adoption)

AP 6200 Budget Preparation

References:

Education Code Section 70902(b)(5);
Title 5 Sections 58300 et seq;
ACCJC Accreditation Standard III.D

- **The budget process will include consultation with appropriate groups and will link resource allocations to institutional planning.**

- **The District will have a goal to maintain a 12% reserve in any current budget year to pay obligations, or 60 days of cash on hand in the unrestricted fund, whichever is greater.**

- **A budget calendar that includes presentation of the tentative and final budgets will be distributed with the annual budget call. The tentative budget shall be presented no later than July 1 *[Title 5 Section 58305(a)]*, and the final budget no later than September 15 *[Title 5 Section 58305(c)]*. A public hearing on the budget shall be held on or before September 15 *[Title 5 Section 58301]*.**

- **Two copies of the adopted budget to be submitted to the California Community College Chancellor's Office on or before September 30 *[Title 5 Section 58305(d)]*.**

- **Submission of appropriate financial reports to include upcoming budgets will be submitted to the California Community College Chancellor's Office via the CCFS311 Report.**

~~1. Budget Preparation Philosophy: Refer to Chapter 3, AP 3250 Institutional Planning~~

~~2. Budget Development Processes: Refer to Chapter 3, AP 3250 Institutional Planning~~

~~3. Criteria and Guidelines for Planning and Budgeting: Refer to Chapter 3, AP 3250 Institutional Planning~~

~~4. District Budget Calendar:~~

~~The tentative District budget shall be prepared by the Vice President, Business Services, recommended by the President, approved by the Board, and filed with the Chancellor's Office by July l.~~

~~The Board shall hold a public hearing on the budget on or before the 15th of September, but not earlier than three days following availability of the budget for public inspection. Adoption of the District budget by the Board shall be accomplished on or before September 15 to allow for the filing of the adopted budget (two copies of 311 forms) with the Chancellor's Office on or before September 30.~~

Revised 2015
Revised 2018