ADDENDUM B — PART 2

Annual Campus Safety and Security Report/Handbook 2020-2021

Published September 30, 2021

- Campus Crime Prevention Policy
- Campus Drug Policy
- Campus Crime Statistics Report
- Violence Against Women Policy
- Title IX Harassment Policy
- Cybersecurity Policy

Contents

SOUTH COAST COLLEGE CAMPUS SECURITY / CRIME PREVENTION POLICY

South Coast College– Orange County Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Report

INTRODUCTION

South Coast College *(the "College")* is providing the following information to all of its employees and students as part of the College's commitment to safety and security pursuant to the requirements of the federal Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act. If you should have questions about any of the information provided in this Report, please contact:

Kevin Magner
Dean of Operations
South Coast College
2011 Chapman Ave.
Orange, CA 92868 (714) 867-5009
kjmagner@southcoastcollege.com

CAMPUS SECURITY AND CRIME PREVENTION POLICY

The College's Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Report is distributed through the South Coast College internet.

REPORTING CRIMES AND EMERGENCIES

A safe environment is everyone's responsibility. Students, faculty and staff are encouraged to report all criminal acts, suspicious activities or emergencies promptly and have the right to report these matters confidentially. Victims or witnesses to a crime are encouraged to file a report of the incident. Reports can be filed on a voluntary, confidential basis for inclusion in the annual disclosure of crime statistics by contacting the Dean of Operations, Kevin Magner. Reports are kept in a secure location in the office of the Dean of Operations, Room 103. Names of victims or witnesses are not disclosed in the crime report. It is the policy of the College that all criminal acts or other emergencies be properly documented and reported to local authorities as required by law.

Students and employees should promptly report all criminal actions and emergencies occurring on or around the College facilities to:

Director of Operations, Kevin Magner, either in person or by calling (714) 867-5009. If the Dean of Operations is not available, you may contact the Receptionist at (714) 867-5009; Jila Andelibi, Dean of Finance, at (714) 830-0251; Yolanda Krieger, Court Reporting Program Director, or William Dixon, Paralegal Program Director, and the Orange Police Department by dialing 911 or (714) 744-7444.

In the event of fire or medical emergencies, staff and employees should contact the Orange Police by dialing 911 and then notify the Dean of Operations.

Timely Warning

Policy

It is the policy of South Coast College to comply with provisions of The Clery Act regarding the issuance of Timely Warnings. In the event that a situation arises, either on or off campus, that, in the judgment of the Campus President constitutes a serious or continuing threat to students and employees, a campus wide Timely Warning will be issued.

Procedure

Under the provisions of The Clery Act, schools have a responsibility to alert the school community of certain crimes in a manner that is timely and will aid in the prevention of similar crimes. These crimes include all The Clery Act crimes that are:

- Reported to school security authorities; and
- Are considered by the school to represent a serious or continuing threat to the students and employees. As a reminder The Clery Act crimes include:
- Criminal Homicide – Murder & Non-negligent Manslaughter – Negligent Manslaughter
- Sex Offenses – Forcible – Non-forcible
- Robbery
- Aggravated Assault
- Burglary
- Motor Vehicle Theft
- Arson

Issuance of a Timely Warning will be decided on a case by case basis in light of all facts surrounding the crime, the continuing danger to the school community and the possible risk of compromising law enforcement efforts. Before a Timely Warning is issued the Campus President must consult with their applicable Director of Operations and the Dean of Finance and Administration who oversees all aspects of Human Resources. If the collective decision is made to issue a Timely Warning the Campus President has the responsibility to issue the warning within two business days.

In the event of a Timely Warning, it will be posted to the school's website under the NEWS category should a Timely Warning occur.

- A description of the offense
- Description of the suspects
- Additional information (any other information that pertains to the incident that ensures all members of the community [students, administration, and faculty] understand the nature of the incident.

Warnings will be issued through the following means:

1. E-mail to faculty, staff and students. Text messages may also be utilized.
2. Post a copy of the warning in each classroom, lab, break room (student and staff) and all entrances and exits. The warning will be reproduced on fluorescent orange paper. This color paper will be used only for Timely Warnings.
3. Post to the NEWS portion of the campus specific section of the campus web site.
4. The Campus President or another member of the school's management team will visit each classroom or lab to inform all students of the situation. In the event that a warning is issued, the Campus President will inform all applicable local law enforcement agencies.

SECURITY AND ACCESS TO THE COLLEGE

It is the policy of the College that access to all campus facilities be limited to authorized personnel, students and invited visitors. Visitors are at all times subject to College policies and conduct codes. Students and employees are responsible for the conduct of their guests at all times. Students, staff and faculty are required to have their valid identification card in their possession at all times while on campus and must be prepared to present it upon request. Visitors must sign in at the front desk and should be escorted by a staff or faculty person at all times.

ACCESS TO ACADEMIC BUILDINGS

The front receptionist desk is located in the north entrance on the first floor at 2011 West Chapman Avenue. It is staffed Monday through Friday from 7:00 a.m. until 8:00 p.m. After hours, the building is protected with locked security doors and devices including cameras, and proper procedures are followed to ensure limited access to secured areas. The front doors will be locked at 10:00 p.m. weekdays Monday through Thursday and at 8:00 p.m. on Friday by the custodial staff. Exterior lighting is provided around the building and parking areas, and shrubs and hedges are kept low for safety reasons. Suspicious persons will be questioned and asked to leave the campus. All students, faculty, staff and graduates in the building must have their identification card in their possession at all times and must be prepared to present it upon request. All visitors must be escorted by a staff or faculty person at all times..

SCHOOL-SPONSORED HOUSING

At the present time, the College does not have any school-sponsored housing.

CAMPUS LAW ENFORCEMENT

The College does not maintain a security staff, rather, the Dean of Operations, Program Directors, receptionist, and custodial staff are instructed in security, security problems, specific school rules and regulations and the proper procedures of how to enforce them. These procedures and rules and regulations are reviewed periodically to ensure that security needs are being met. In the event of an emergency of any sort, staff and students are to immediately contact any of these people. In any emergency situation, any individual providing assistance should call 911. Evening staff are available to assist students, faculty and staff of the College. Someone is on duty during all hours the building is occupied. Reception and custodial personnel are responsible for ensuring that persons entering the building are employees, students, their families or invited guests. They are authorized to request identification from those individuals who are unfamiliar to them. The Dean of Operations has the authority to evict unauthorized persons from the campus premises and will notify local law enforcement authorities of all actual or suspected criminal activities, including trespassing. The staff does not have the authority to arrest individuals. Students are required to carry their South Coast College identification card at all times and to present them upon request. The staff may not make arrests, but are instructed to promptly contact Kevin Magner, Dean of Operations if any illegal activity occurs. It is the policy of South Coast College to promptly, accurately and completely document all criminal activity with the Orange Police Department as deemed appropriate. Other staff members will assist, as appropriate, with this reporting. Students should contact appropriate personnel immediately in the case of an incident.

RELATIONSHIPS WITH LOCAL AND STATE POLICE

South Coast College is located in the city of Orange, California. The college maintains a close working relationship with the Orange Police department, with periodic contact initiated by the College personnel to ensure that the College is aware of criminal offenses and arrests occurring on or near the campus so that they can be properly reported, and if necessary, provide for timely warning reports on crimes that represent a continuing threat. Timely warning reports are provided to the campus community via the following means: email, letters, posters in campus common areas, notices placed in faculty and staff mailboxes, announcements read in class, etc.

PROGRAMS TO INFORM STUDENTS AND EMPLOYEES ABOUT CAMPUS SECURITY

All current employees and students receive the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Report on an annual basis. All new College employees and students are instructed on crime awareness, prevention and campus security during orientation, and encouraged to take responsibility for their own security, as well as for the safety of others.

The orientation program, which takes place six times per year, includes a description of campus security policies and procedures, suggestions on how to avoid becoming a crime victim, evacuation plans for the campus and procedures for reporting any criminal activity or emergency.

PROGRAMS TO INFORM STUDENTS AND EMPLOYEES ABOUT THE PREVENTION OF CRIMES

The college also provides in-service programs designed to heighten awareness of crime and its prevention. These in-service programs are conducted by local law enforcement officials and/or local experts in the field once each year. Topics for these informational programs may include personal safety & self-defense, living in a city, crime prevention, and neighborhood watch programs. Crime prevention presentations may include the topics of sexual assault, domestic violence, workplace violence and hate crimes. All students, staff and faculty are invited to attend these presentations. In addition to the annual campus security report, students and staff are notified of specific security concerns as they arise throughout the year.

In the event the College, working with local police, determines that a particular criminal offense continues to be a threat to the campus community, it will notify the campus community by bulletin board notices, notices read by instructors in classrooms and notices on the student intranet web site.

Students are requested to review the College's *Catalog* where sections discussing Crime Awareness and Campus Security and the Student Conduct Policy can be found. Employees are requested to review the College's *Employee Handbook* where information regarding Standards of Conduct and Safety can be found.

OFF-CAMPUS STUDENT ORGANIZATIONS

At the present time, the College does not have any off-campus student organizations.

DRUG AND ALCOHOL POLICIES

South Coast College is committed to achieving a safe, healthy, productive work environment for all employees and students, free from effects of illegal drugs and employee/student alcohol consumption. It is the policy of South Coast College to prohibit illegal drug usage, possession, sale and distribution on or in the South Coast College property, or while performing South Coast College business, and to prohibit alcohol/drug usage which may affect a person's job performance. Having an illegal drug in the body while on or in South Coast College property and /or being under the influence of alcohol/drugs while on duty or performing South Coast College business are prohibited. South Coast College conducts a biannual review of its drug and alcohol policies and procedures for effectiveness and makes any changes deemed necessary.

South Coast College provides assistance to our employees and students in getting help. However, it is the responsibility of each employee or student to seek assistance before alcohol and drug problems lead to a violation of school policy. Once a violation of this policy occurs, subsequently seeking assistance or voluntarily entering a rehabilitation program will not necessarily lessen any disciplinary action and may be disregarded in any disciplinary decision.

Violation of this policy or any other policy of South Coast College relating to alcohol or drugs may result in disciplinary action, up to and including suspension pending termination. Because of the importance to all employees and students of enforcement of the College's drug and alcohol policies, disciplinary action involving these policies may be implemented with or without warning to the disciplined employee or student.

Students receiving Title IV funds who are convicted of a criminal drug offense during the period of enrollment for which the funds were awarded will lose eligibility for all Title IV funds. In such cases the student will be given written information on how they can regain eligibility.

Procedure

South Coast College provides an employee/student assistance program for persons with drug or alcohol problems which provides:

1. Assistance in the form of referral for any employee or student who feels he or she has developed an addiction to, dependency upon, or is suffering from the use of alcohol or drugs.
2. Leave of absence in accordance with school policy, on the same basis and with the same restrictions and limits as other disabilities.
3. Reinstatement to the same or similar job, when practical, upon successful completion of a rehabilitation program.

It is the responsibility of all managers to make employees and students aware of the assistance program and to assure that no person who requests diagnosis and treatment will have his or her job tenure or promotional opportunities jeopardized by this request. Any employee or student suffering from drug or alcohol usage or dependency who rejects treatment when requested by the school or who leaves the treatment program prior to being properly discharged is subject to disciplinary action up to and including suspension pending termination. The recurrence of a drug or alcohol dependency may also result in disciplinary action.

The employee assistance program's job is to assist employees and students in finding methods or resolving problems that affect their job performance. Most people are not aware of the resources which are available to them. Sometimes they are so overburdened by their problems they have difficulty reaching out for help. The counselor can assist employees and students in obtaining the needed help in a humane and confidential manner.

The earliest possible identification and treatment of the problem best serves the interest of both the employee/student and the College. The decision to undertake treatment is the responsibility of the employee or the student. The overall objective is to retain valuable employees and students by providing assistance when the problem becomes evident rather than waiting until the employee or student is no longer employable.

Various health risks are associated with the misuse of illegal drugs, legal drugs and/or alcohol. These health risks should be discussed with a qualified health professional, such as a primary care physician. There are also online sites which describe risks for specific types of substance abuse. We recommend the Federal Drug Administration web site at www.fda.gov/drugs . Other reputable sites include The Mayo Clinic at www.mayoclinic.com and Web MD at www.webmd.com.

When the problem is chemical abuse, the employee or student is given information on the different programs available. The employee assistance program offers to do a free individualized evaluation to determine what kind of help the person needs. From this evaluation, the appropriate treatment program (inpatient versus out-patient) is determined.

Drug dependency is a medically recognized illness with physical, physiological, emotional, and social implications. Treatment must focus on educating individuals to their disease, as well as assist and support them in developing the necessary skills to manage their lives in a more productive manner.

California's Medical Marijuana Program

Students, faculty, and staff who qualify under California's Proposition 215 to use marijuana for medical reasons are not permitted the use, storage, or possession of marijuana or paraphernalia on College property or at a College-sponsored event.
Students who violate this policy are subject to discipline.

Definitions for the purpose of this policy:

"Drug" as defined by the Federal Food, Drug, and Cosmetic Act and also includes the drugs specified under "illegal drug" below.

"Having an illegal drug in the body" means the presence in a detectable amount of any illegal drug (or chemical substance of residue from which the presence of any illegal drug may be reasonably inferred) in the body of an employee.

"Illegal drug" means any drug (1) that is not legally obtained in California, or (2) that is being used in a manner different from that lawfully prescribed, or (3) that can be legally obtainable but has not been legally obtained. "Illegal drug" includes the following drugs unless used in accordance with a valid prescription:

Heroin	Hallucinogens	Codeine
Morphine	Amphetamines	Cocaine
Dilaudid	Barbiturates	Marijuana
Tranquilizers	Sedatives	MDMA (Ecstasy)
	PCP	

"Legal drug" means prescribed drugs and over-the-counter drugs which have been legally obtained and are being used for the purpose for which they have been prescribed or manufactured. Alcohol is also considered a legal drug, except in cases of underage drinking.

"Management" means supervisors, managers, directors and officers of South Coast College.

"Under the influence" means that an employee or student is affected in an observable manner by the presence of alcohol, or alcohol and other substances, in any detectable amount in the body" The symptoms of influence need not involve misbehavior or obvious impairment of physical or mental ability such as slurred speech or difficulty in maintaining balance.

In keeping with section 120(a) through (d) of The Higher Education Act of 1965, as amended, including the Drug-Free Schools and Communities Amendments of 1989 (Public Law 101-226), a "Drug Free Schools and Campuses" publication, the Drug Prevention Policy, is provided to all College students, staff and faculty annually.

For more drug and alcohol policy information, see the Drug and Alcohol Policy Section. Pursuant to federal and state drug laws, students are prohibited from the unlawful manufacture, distribution, possession, sale or use of illicit/illegal drugs. The College also enforces state laws regarding underage drinking. This prohibition applies while on the property of the school or when participating in any institutional activity. Students or employees who violate this policy will be subject to disciplinary action up to, and including, expulsion from school or termination of employment.

South Coast College supports and endorses the Federal Drug-Free Workplace Act of 1988 and the Drug-Free Schools and Communities Act amendments of 1989. The unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance or abuse of alcohol by an employee or student on South Coast College's property or as part of any South Coast College activity is prohibited. Any student or employee of South Coast College found to be abusing alcohol or using, possessing, manufacturing, or distributing controlled substances in violation of the law on South Coast College property or at South Coast College events shall be subject to disciplinary action. For employees, the school will take appropriate personnel action for such infractions, up to and including termination. Students who violate this policy will be subject to sanctions that include suspension and dismissal from South Coast College. For purposes of this policy, "conviction" means a finding of guilt (including a plea of nolo contendere) or imposition of sentence or both, by any judicial body charged with the responsibility of the federal or state criminal drug statutes.

Health Risks

Abuse of alcohol and use of drugs is harmful to one's physical, mental, and social wellbeing. With excessive drug use, life becomes centered on drugs to the exclusion of health, work, school, family, and general well-being. Accidents and injuries are more likely to occur if alcohol and drugs are used. Alcohol and drug users can lose resistance to disease and destroy one's health. Increasing tolerance developed by the user complicates the effects of drug use. This tolerance may be psychological, physiological, or both and may lead to greater danger of overdose. Alcoholism is the number one drug problem in the United States. Alcoholism takes a toll on personal finances, health, social relationships, and families. Abuse of alcohol or use of drugs may cause an individual driving a motor vehicle to injure himself or herself or others and may subject the person to criminal prosecution. Drunk drivers are responsible for more than half of all traffic fatalities.

The following summarizes the effects and dangers of the major categories of drugs:
Amphetamines: Physical dependency, heart problems, infections, malnutrition, and death may result from continued high doses of amphetamines.
Narcotics: Chronic use of narcotics can cause lung damage, convulsions, respiratory paralysis, and death.

Depressants: These drugs, such as tranquilizers and alcohol, can produce slowed reactions, slowed heart rate, damage to liver and heart, respiratory arrest, convulsions, and accidental overdoses.
Hallucinogens: These drugs may cause psychosis, convulsions, coma, and psychological dependency.

Counseling, Treatment, or Rehabilitation Programs

As indicated previously, the administration of South Coast College maintains a list of hospital and community agencies available to assist employees and students seeking alcohol and drug counseling and treatment. Employees and students who have a substance-dependency problem are strongly encouraged to obtain counseling and treatment. Anyone seeking additional information about health problems and treatment related to alcohol and drug problems can contact the Campus President or Human Resources. Requests for assistance will be held in complete confidentiality and will be provided on a need-to-know basis only.

Sanctions

A student who violates any provision of this policy shall be subject to appropriate disciplinary action, up to and including suspension and/or administrative withdrawal from South Coast College. Students may reapply for admission, through review, at a later date.
A student suspected of the possession, sale, manufacture, use, or distribution of a controlled substance, may be suspended from the student's program of study and may become ineligible for continued participation in the Higher Education Act (HEA), Title IV Student Assistance Programs. If convicted, the student's relationship with South Coast
College will be terminated, and the student may lose the ability to participate in the HEA, Title IV Student Assistance Programs.

In addition, any student or employee who violates the standards of conduct as set forth in this policy may be subject to referral for prosecution.

A student who violates any provision of this policy shall be subject to appropriate disciplinary action, up to and including suspension and/or administrative withdrawal from South Coast College. Students may reapply for admission, through review, at a later date.

Legal Sanctions

Students and employees are reminded that unlawful possession, distribution, or use of illicit drugs or alcohol may subject individuals to criminal prosecution. South Coast College will refer violations of prescribed conduct to appropriate authorities for prosecution.

Federal and state sanctions for illegal possession of controlled substances range from up to four years' imprisonment and up to $20,000 in fines for each offense. Under federal laws, possession of drugs such as heroin or cocaine may result in sanctions of not less than five years and up to life imprisonment for a first offense involving 100 grams or more. Offenses involving lesser amounts, 10-99 grams, may result in sanctions up to and including 20 years' imprisonment and a fine of up to $4 million.

Under California law, possession of marijuana is a misdemeanor, punishable by not more than one year in county jail or in state prison for a period of not less than one year or more than 10 years. Under California law, a person may still be deemed to be in possession of a controlled substance even if the controlled substance has been consumed. Delivery or sale of marijuana to a minor is punishable by up to five years in state prison. Possession or distribution of any controlled substance, such as heroin or cocaine, shall be punished by imprisonment in the state prison for two, three, or four years.

The state of California may impose a wide range of sanctions for alcohol related offenses. For example, a person under the age of 21 who presents or offers false identification for the purpose of obtaining alcohol is guilty of a misdemeanor and may be fined at least $250 or be required to perform community service. The driver's license of any person found to have .08 blood alcohol while driving a motor vehicle may be suspended or revoked.

The term "controlled substance" as used in this policy means any narcotic drug, hallucinogenic drug, amphetamine, barbiturate, marijuana, or any other controlled substance, as defined in Schedules I through V of Section 202 of the Controlled Substances Act, 21 U.S.C. 812, and as further defined by regulation 21 C.F.R. 1208.01 et seq. The term does not include the use of a controlled substance pursuant to a valid prescription or other use authorized by law.

Federal, State, and Local Laws and Sanctions Regarding Alcohol

It is South Coast College's belief that all disciplinary sanctions should assist in education and provide the opportunity for personal growth. The following is a summary of federal, state, and local laws regarding drugs and alcohol.

Laws regarding the use of alcohol

South Coast College has established an alcohol use policy based on the tenet that those serving and drinking alcohol will do so legally and responsibly, with concern for others around them, and with an understanding of the social, personal and legal issues involved.

It is the responsibility of persons or groups that use, possess, distribute, or produce alcohol to be familiar with and abide by all laws regarding the sale and use of alcoholic beverages. The following is a summary of the more important laws that directly relate to the College's Alcohol and Substance Abuse Policy:

1. The purchase, possession, or consumption of any alcoholic beverages (including beer and wine) by any person under the age of 21 is prohibited (Business and Professional Code, 25658 and 25662).
2. It is a misdemeanor for anyone to sell, furnish, or give or cause to sell, furnish, or give any alcoholic beverage to a minor (Business and Professional Code 25658(a)).
3. It is prohibited to advertise alcoholic beverages in such a way as to encourage minor to drink (Business and Professional Code 25664).
4. It is a misdemeanor for a minor to have any alcoholic beverage in his or her possession on any street or highway or in any public place or in any place open to the public (Business and Professional Code 25662(a)).
5. Any minor who purchases any alcoholic beverage, or any minor who consumes any alcoholic beverage, or any minor who consumes any alcoholic beverage in any on-sale premises, is guilty of a misdemeanor and shall be punished by a fine of not less than $100.00, no part of which shall be suspended (Business and Professional Code 25658(b)). 6. Minors attempting to purchase alcoholic beverages will be fined $250.00 or required to perform 24-32 hours of community service for the first offense and $500.00 for a second or subsequent offense. Violators may also be required to perform 36-48 hours of community service for a second offense (Business and Professional Code 25658.5).
7. No minor shall knowingly drive any motor vehicle carrying any alcoholic beverage, unless the minor is accompanied by the parent or legal guardian (California Vehicle Code 23224(a)).
8. Peace officers who lawfully enter premises may confiscate alcoholic beverages which are in plain view and possessed by or provided to minors at social gatherings. Alcoholic beverages in open containers that are confiscated may be destroyed while those in unopened containers shall be impounded for no more than seven (7) working days after which they too may be destroyed. Unopened containers may be released within the sever (7) days to the owner or resident of the property provided they are 21 years of age (Business and Professional Code 25662(b)).
9. Any person providing an alcoholic beverage to a minor will be contributing to the delinquency of a minor and guilty of a misdemeanor (Penal Code 272).
10. Possession of Alcohol in a Public Place
    It is unlawful to be in possession of alcoholic beverages in a public place (Orange Municipal Code 9.16.050). A public place is defined as any location where all members of the public have unrestricted access. This includes, but is not limited to, outside walkways within the College Campus and walkways and balconies within the Residence Halls/Apartments.
11. Intoxicated Person
    The use of intoxicating liquor by the average person in such quantity as to produce intoxication causes many commonly known outward manifestations which are “plain” and “easily seen or discovered.” [People of the State of California v. Johnson, 185 P.2d 105 (Cal.App. Sup.Ct. L.A.Cty. 1947), p. 106]., the sale or furnishing of alcoholic beverages to an obviously intoxicated person is a misdemeanor (Business and Professional Code 25602).
12. Operation of a Vehicle

a. It is unlawful for any person who is under the influence of an alcoholic beverage or any drug or under the combined influence of an alcoholic beverage and any drug, to operate a bicycle (California
Vehicle Code 21200.5) or a motor vehicle (California Vehicle Code
23152(a)).
b. No person shall drink any alcoholic beverage while driving a motor vehicle upon any highway (California Vehicle Code 23220).
c. No person shall have in his or her possession, on his or her person, while driving a motor vehicle upon any highway, any bottle, can, or other receptacle, containing an alcoholic beverage which has been opened, or a seal broken, or the contents of which have been partially removed (California Vehicle Code 23223).

13. Sale of Alcohol

It is a misdemeanor to sell alcoholic beverages without a license from the State Alcoholic Beverage Control Board (Business and Professional Code 23300 and 23301). Included are forms of indirect sales such as selling tickets which may be exchanged for drinks, tickets of admission which include an alcoholic beverage or "passing the hat" during an event to cover the cost of alcohol.

	State Law	Federal Law
Legal Drinking Age	You must be 21 to drink or work at a bar in California, and you can work in a restaurant that sells alcohol at age 18.	You must be 21 to drink or work at a bar in California, and you can work in a restaurant that sells alcohol at age 18.
BAC Limits	California's maximum legal blood-alcohol content is .08 percent.	BAC maximum is .08. Minors are held to stricter standards under zero tolerance laws, which hold the driver to much lower blood alcohol content levels for criminal and/or license suspension purposes.
Penalties	$200-$500 average fine, average jail time of 6 months suspension after the first offense, and an average probation of 5 years.	Varies from state to state.
Regulations	In terms of possession of alcohol by minors, it exempts use by minors while under their parents' supervision.	For minors in possession, first offense is $250 and/or 24 to 32 hours of community service, and the second offense is up to a $500 fine and/or 36 to 48 hours of community service.

Criminal Sanctions under California Law for the unlawful possession or distribution of illicit drugs and alcohol include the following:

1. Imprisonment in State prison for possession of specified controlled substances, including opium derivatives and cocaine (Health and Safety Code Section 11350).

2. Imprisonment in State prison for two to four years for possession or sale of specified controlled substances, including opium derivatives and cocaine (Health and Safety Code Section 11351).

3. Imprisonment in State prison for three to five years for possession for sale of cocaine base (Health and Safety Code Section 11351.1).

4. Fine not exceeding $50,000 for possession for sale of heroin (Health and Safety Code Section 11352.5).

5. Fine of not more than $100 for possession of less than 28.5 grams of marijuana (one ounce); imprisonment in county jail and/or fine of not more than $500, or imprisonment in State prison for possession of concentrated cannabis (Health and Safety Code Section 11357).

6. Imprisonment in State prison for possession or sale of marijuana (Health and Safety Code Section 11359).

	State Law	Federal Law
Cocaine (50-4999 grams)	Possession can be prosecuted as a misdemeanor or felony with up to 3 years in prison. Penalties for possession for sale is 2, 3, or 4 years in the state prison. Possession for sale will often serve from 1 year in county jail or 18month sentence in the state prison. Various enhancements do exist in the California Code which may result in very long prison terms, such as being in possession for sale, or selling multiple kilogram quantities of the drug.	Not less than 5 years and not more than 40 years. If death or serious injury, not less and 20 years or more than life. Fine of not more than $5 million if an individual, $25 million if not an individual.
Cannabis (1 to 49 plants; less than 50 kg)	Possession of one ounce or less can result in a fine of $100 (plus fees). Possession of more than an ounce can result in a fine of $500 (plus fees) and 6 months in jail.	Not more than 5 years; Fine not more than $250,000, $1 million other than individual
Heroin/Opiates	Possession can now be prosecuted as a misdemeanor or felony with up to 3 years in prison. Penalties for possession for sale is 2, 3, or 4 years in the state prison. Those convicted of possession for sale or sale/trafficking will often serve from 1 year in county jail, or 18-month sentence in state prison based upon the quantities and extent of their drug dealing if it is their first offense.	A first conviction for possession can result in up to one year in jail as well as a fine (minimum of $100). Additional convictions will result in mandatory jail time as well as increased minimum fines.

A copy of the South Coast College Drug and Alcohol Policies will be distributed annually in writing to each employee and to each student who is taking one or more classes for any type of academic credit except for continuing education units, regardless of the length of the student's program of study.

EDGAR Part 86, Sec. § 86.100(a). Such notification will occur as follows:

Students: Upon initial enrollment at South Coast College and at registration thereafter

Employees: At hiring and annually thereafter

A copy of the South Coast College Drug and Alcohol Policies is maintained in the Student Services Office and Office of the President and on the South Coast College website:

http://southcoastcollege.edu/images/pdf/da.pdf

List of Community Services Available

A Better Tomorrow
1320 West Pearl
Anaheim, CA 92801
(888) 224-6303
Provides a multitude of programs for treating chemical addictions and mental health issues

Alcoholics Anonymous
2191 North Orange Olive Road
Orange, CA 92865
(714) 637-9860
Provides group counseling, therapy for alcohol dependency

Catholic Charities
1800 East McFadden Ave.
Santa Ana, CA 92705
(714) 347-9600
Provides marriage, family, child, and individual counseling

Chapman Clean House
1412 East Chapman Ave.
Orange, CA 92866
(866)288-9779
Substance Abuse Treatment, Intervention Services, Intervention & Transport Service, Inpatient Care, Family Program, Dual Diagnosis Program and insurance accepted.

Children & Family Services
800 N. Eckhoff St.
Orange, CA 92868
(714) 704-8000
Provides in-home counseling for families

Mental Health Association of Orange
12755 Brookhurst St.
Garden Grove, CA 92840
(714) 638-8277
Residential Treatment Center for women only, self-pay facility.

Salvation Army
1515 W. North Street
Anaheim, CA 92801
(714) 491-1450
Social & Human Services

PROGRAMS AND PROCEDURES REGARDING SEXUAL ASSAULT

Educational programs promoting the awareness of rape, acquaintance rape and other sex offenses are presented informally on campus. Guest speakers present discussions on rape awareness, reducing the risk of being a rape victim and what to do if you are attacked. Brochures on sexual assault issues are available in Operations, Room 103. Should a student be sexually assaulted, it is the student(s) option to notify the appropriate law enforcement authorities, including on-campus authorities and local police. At the student's request, housing personnel, security, the Dean of Operations, the Executive Committee or other College officials will assist in notifying the proper authorities. Victims of sexual assault or rape should follow these recommended steps:

1. Go to a safe place following the attack.
2. Do not shower, bathe or destroy any of the clothing you were wearing at the time of the attack.
3. Go to a hospital emergency room for medical care.
4. Make sure you are evaluated for the risk of pregnancy and venereal disease. (A medical examination is the only way to ensure you are not injured and it could provide valuable evidence should you decide to prosecute.)
5. Call someone to be with you; you should not be alone.

It is also recommended that victims call the Rape Crisis Hotline at (714) 957-2737. It is open 24 hours a day and their counselors can help answer medical and emotional questions at any hour and in complete confidence. Reporting the rape to the police is up to the victim, but it is important to remember that reporting a rape is not the same as prosecuting a rape. Victims are strongly encouraged to call the police and report the rape. If the victim requests, the College will assist in identifying off-campus counseling or mental health services. After any campus sexual assaults are reported, the victims of such crimes have the right to request that College personnel take steps or actions reasonably feasible to prevent any unnecessary or unwanted contact or proximity with alleged assailants, including relocation in College housing, if applicable or the transfer of classes.

Other rape crisis centers or mental health agencies available to assist a victim of sexual offenses include:

Rape Crisis Hotline/Sexual Assault Assistance Program
(714) 957-2737 (Northwest Orange County) or
(949) 831-9110 (South Orange County)
1821 East Dyer Road, Suite 200, Santa Ana, CA 92705
National Sexual Assault Hotline
(800) 656-4673 or www.rainn.org (24 hour assistance)

Disciplinary Action and Sanctions

On-campus disciplinary procedures against students will be in accordance with the College published Student Conduct Policy. Both the accuser and the accused are entitled to have others present during a disciplinary proceeding. Both will be informed of the outcome of any campus disciplinary proceeding. For this purpose, the outcome of a disciplinary proceeding means only the College's final determination with respect to the alleged sexual offense and any sanction that is imposed against the accused. Sanctions, which may be imposed following a final determination of a disciplinary proceeding regarding rape, acquaintance rape, or other forcible or non-forcible sex offenses, may include warning, probation, suspension or dismissal. See more regarding specific violence against women acts in the VIOLENCE AGAINST WOMEN ACT Section that follows.

INFORMATION REGARDING REGISTERED SEX OFFENDERS

California's Megan's Law provides the public with certain information on the whereabouts of sex offenders so that members of our local communities may protect themselves and their children. The law requires the California Department of Justice to produce monthly a CD-ROM or other electronic medium containing information on serious and high-risk sex offenders. Access to the CD-ROM is mandated to be available for public viewing at all Sheriff's Departments, at Police Departments in cities with a population of 200,000 or more, and through the California Department of Justice.

Additional information pertaining to registered sex offenders may be accessed at the following local Sheriff and Police Department stations:

Orange Police Department
1107 N. Batavia St.
Orange, CA 92867 714-744-7444 www.cityoforange.org

Orange County Sheriff's Headquarters
550 North Flower, 2nd Floor
Santa Ana, CA 92702
(714) 647-7040
Available Monday through Friday from 8:00 a.m. until 4:00 p.m.

Anaheim Police Department
425 South Harbor Blvd.
Anaheim, CA 92805
(714) 765-1563
Available Tuesday through Thursday from 8:00 a.m. until 4:00 p.m. (Appointment required)

Costa Mesa Police Department
99 Fair Drive
Costa Mesa, CA 92626
(714) 754-5079
Available Tuesday through Friday from 7:00 a.m. until 4:00 p.m. (Appointment required)

Santa Ana Police Department
60 Civic Center Plaza
Santa Ana, CA 92701
(714) 245-8300
Available Monday through Friday from 9:00 a.m. until 4:00 p.m. (Appointment required)

In California law, Assembly Bill 488, sponsored by the Attorney General, now provides the public with internet access to detailed information on registered sex offenders. This expanded access allows the public for the first time to use their personal computers to view information on sex offenders required to register with local law enforcement under California's Megan's Law. Previously, the information was available only by personally visiting police stations and sheriff offices or by calling a 900 toll number. The new law was given final passage by the California Legislature on August 24, 2004 and signed by the Governor on September 24, 2004.

Information about Megan's Law and registered sex offenders can be accessed via the California Attorney General's web page at: http://meganslaw.ca.gov

POLICIES FOR PREPARING THE ANNUAL DISCLOSURE OF CRIMINAL STATISTICS

All incidents are reported and documented on the Incident Report, which is sent to the Dean of Operations, Kevin Magner. Reports are kept in a secure location in the office of the Dean of Operations, Room 103. The annual crime report is prepared by gathering campus crime statistics and data from local and state police and sheriff departments and other relevant information by Kevin Magner, Dean of Operations.

CRIME STATISTICS

The following statistics are provided for your information in compliance with the Jeanne Clery Disclosure of Campus Security Act and Campus Crime Statistics Act. South Coast College prepares the crime statistic policies annually by gathering all reported data and preparing a report for its employees and students. Set forth in the first box below are statistics available to the College concerning the occurrence on the College's campus which were reported to local police agencies. The second box below sets forth available statistics concerning the number of criminal offenses in relation to hate crimes on the College's campus, non-campus buildings and property, and public property. Finally, in the third box arrests and "referrals for campus disciplinary action" for liquor law violations, drug law violations, and illegal weapons possession are listed. Victims or witnesses may report crimes on a voluntary, confidential basis for inclusion in the annual disclosure of crime statistics.

CAMPUS CRIME STATISTICS

1. General Crime Statistics

Criminal Homicide

Murder & non-negligent manslaughter

On Campus			Non-Campus			Public Property		
2018	2019	2020	2018	2019	2020	2018	2019	2020
0	0	0	0	0	0	0	0	0

Negligent manslaughter

On Campus			Non-Campus			Public Property		
2018	2019	2020	2018	2019	2020	2018	2019	2020
0	0	0	0	0	0	0	0	0

Sex Offenses

Forcible sex offenses

On Campus			Non-Campus			Public Property		
2018	2019	2020	2018	2019	2020	2018	2019	2020
0	0	0	0	0	0	1	0	0

Non-forcible sex offenses

On Campus			Non-Campus			Public Property		
2018	2019	2020	2018	2019	2020	2018	2019	2020
0	0	0	0	0	0	0	0	0

Robbery

On Campus			Non-Campus			Public Property		
2018	2019	2020	2018	2019	2020	2018	2019	2020
0	0	0	0	0	4	0	0	0

Aggravated Assault

On Campus			Non-Campus			Public Property		
2018	2019	2020	2018	2019	2020	2018	2019	2020
0	0	0	0	0	0	0	3	0

Burglary

On Campus			Non-Campus			Public Property		
2018	2019	2020	2018	2019	2020	2018	2019	2020
0	0	0	0	0	0	1	0	0

Motor Vehicle Theft

On Campus			Non-Campus			Public Property		
2018	2019	2020	2018	2019	2020	2018	2019	2020
0	0	0	0	0	0	0	0	1

Arson

On Campus			Non-Campus			Public Property		
2018	2019	2020	2018	2019	2020	2018	2019	2020
0	0	0	0	0	0	0	0	0

Vandalism

On Campus			Non-Campus			Public Property		
2018	2019	2020	2018	2019	2020	2018	2019	2020
0	0	0	0	0	1	0	0	0

Arrests

Liquor Law Violations*

On Campus			Non-Campus			Public Property		
2018	2019	2020	2018	2019	2020	2018	2019	2020
0	0	0	0	0	0	0	0	0

Drug Abuse Violations*

On Campus			Non-Campus			Public Property		
2018	2019	2020	2018	2019	2020	2018	2019	2020
0	0	0	0	3	0	5	8	8

Weapons Violations*

On Campus			Non-Campus			Public Property		
2018	2019	2020	2018	2019	2020	2018	2019	2020
0	0	0	0	0	0	1	1	0

1. Arrests for, and persons referred for campus disciplinary action for liquor law violations, drug violations, and illegal weapons possession. This category does not include students referred for disciplinary action unless the violation(s) was also a violation of law.

Arrests by specific category is listed below.

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Drug Abuse Violations	0	0	0	0	0	0	5	5	8
Liquor Law Violations	0	0	0	0	0	0	0	0	1
Weapons Violations	0	0	0	0	0	0	0	1	1

Arrests by specific category is listed below.

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Drug Abuse Violations	0	0	0	0	0	0	5	5	8
Liquor Law Violations	0	0	0	0	0	0	0	0	0
Weapons Violations	0	0	0	0	0	0	0	1	1

2. Hate Crimes by category of prejudice, and any other crime involving bodily injury reported to local police agencies or to a campus security authority that show evidence of prejudice based on race, gender, religion, sexual orientation, ethnicity or disability.

Murder/Non-negligent man slaughter

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Race	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0
Sexual Orientation	0	0	0	0	0	0	0	0	0
Gender	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0
Ethnicity	0	0	0	0	0	0	0	0	0

Negligent manslaughter

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Race	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0
Sexual Orientation	0	0	0	0	0	0	0	0	0
Gender	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0
Ethnicity	0	0	0	0	0	0	0	0	0

Sex Offenses – Forcible

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Race	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0
Sexual Orientation	0	0	0	0	0	0	0	0	0
Gender	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0
Ethnicity	0	0	0	0	0	0	0	0	0

Sex Offenses – Non-forcible

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Race	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0
Sexual Orientation	0	0	0	0	0	0	0	0	0
Gender	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0
Ethnicity	0	0	0	0	0	0	0	0	0

Robbery

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Race	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0
Sexual Orientation	0	0	0	0	0	0	0	0	0
Gender	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0
Ethnicity	0	0	0	0	0	0	0	0	0

Aggravated Assault

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Race	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0
Sexual Orientation	0	0	0	0	0	0	0	0	0
Gender	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0
Ethnicity	0	0	0	0	0	0	0	0	0

Burglary

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Race	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0
Sexual Orientation	0	0	0	0	0	0	0	0	0
Gender	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0
Ethnicity	0	0	0	0	0	0	0	0	0

Motor Vehicle Theft

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Race	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0
Sexual Orientation	0	0	0	0	0	0	0	0	0
Gender	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0
Ethnicity	0	0	0	0	0	0	0	0	0

Arson

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Race	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0
Sexual Orientation	0	0	0	0	0	0	0	0	0
Gender	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0
Ethnicity	0	0	0	0	0	0	0	0	0

Simple Assault

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Race	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0
Sexual Orientation	0	0	0	0	0	0	0	0	0
Gender	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0
Ethnicity	0	0	0	0	0	0	0	0	0

Larceny – Theft

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Race	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0
Sexual Orientation	0	0	0	0	0	0	0	0	0
Gender	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0
Ethnicity	0	0	0	0	0	0	0	0	0

Intimidation

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Race	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0
Sexual Orientation	0	0	0	0	0	0	0	0	0
Gender	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0
Ethnicity	0	0	0	0	0	0	0	0	0

Destruction/Damage/Vandalism of Property

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Race	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0
Sexual Orientation	0	0	0	0	0	0	0	0	0
Gender	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0
Ethnicity	0	0	0	0	0	0	0	0	0

Violence Against Women

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2018	2020
Domestic Violence	0	0	0	0	0	0	0	0	0

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Dating Violence	0	0	0	0	0	0	0	0	0

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Sexual Assault	0	0	0	0	0	0	0	0	0

	On Campus			Non-Campus			Public Property		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Stalking	0	0	0	0	0	0	0	0	0

VIOLENCE AGAINST WOMEN ACT POLICY

INTRODUCTION

The South Coast College is dedicated to fostering a campus learning environment that is free from any forms of sexual misconduct and gender-based discrimination. Students, who are victims of sexual misconduct including; sexual harassment, sexual assault, stalking, domestic violence, dating violence, or other gender-based harassment or discrimination are encouraged to report these actions to the appropriate administrator. Sexual harassment, sexual violence and other gender-based harassment occurring in the
college setting implicates a federal law called Title IX of the Higher Education Amendments of 1972, which prohibits discrimination on the basis of gender in education programs or activities. Reports of any allegations of this nature trigger certain responsibilities on the part of the College. This policy and its accompanying procedures are intended to ensure safe non-discriminatory campus environments among the College locations where academic success is paramount. Furthermore, it is the unwavering goal of the South Coast College to deter gender-based misconduct through:

1. Education and preventative programs;
2. Accessible services for victims and others affected by sexual or gender-based misconduct;
3. Fundamentally fair methods of investigation and resolution on any report of misconduct; and
4. Safeguards to ensure that recurrence is prevented and the acts of misconduct do not persist.

REFERENCES

Education Code § 66281.5, 67382 and 67385;
California Penal Code § 242, 243, 245, and 261 et seq.;
California SB 967; 20 U.S. Code § 1092(f); 34
Code of Federal Regulations § 668.46(b)(11);
Government Code § 12950.1; Title 5 § 59320, 59324, 59326, 59328, and 59300 et seq.; 34
Code of Federal Regulations § 106.8(b)
U.S. Department of Education, “Dear Colleague Letter:”
http://www2.ed.gov/about/offices/list/ocr/letters/colleague-201104.pdf

SCOPE OF THE POLICY AND PROCEDURES

The College-Student Correspondence

South Coast College institution’s primary correspondence and notification mechanism with students shall be through the student email account provided by the student. At the College’s discretion, students may be notified via U.S. certified mail, delivery in person, or by an alternate email on record from the student.

Jurisdiction

The College's jurisdiction concerning alleged Student Code of Conduct violations extends to The College or any of its college activities occurring on The College property. This jurisdiction may also apply to student-to-student or student-to employee off-campus conduct and/or actions, including electronic activity (such as e-mail, texting, 4 telephone contact, social media), when the College administrator, or designee, determines that the off campus conduct affects, disrupts, or interferes with the educational mission of the campus.

SEXUAL MISCONDUCT POLICY (FOR STUDENTS)

Sexual and Other Sexual Assaults on Campus

I. Any sexual assault or physical abuse, including, but not limited to rape as defined by California law, whether committed by an employee, student or member of the public, that occurs on the College property, is a violation of the College policies and procedures, and is subject to all applicable punishment, including criminal procedures and employee or student discipline procedures. Students, faculty, and staff who may be victims of sexual and other assaults shall be treated with dignity and provided comprehensive assistance. The President shall establish administrative procedures that ensure that students, faculty, and staff who are victims of sexual and other assaults receive appropriate information and treatment, and that educational information about preventing sexual violence is provided and publicized as required by law.

II. Reference: Education Code Section 67382, 67385; 20 US.C. § 1092(f); 34 C.F.R. § 668.46(b)(11) (CCLC)

Other Misconduct Offenses (Will Fall under Title IX When Sex or Gender-Based)

1. Threatening or causing physical harm, extreme verbal abuse, or other conduct which threatens or endangers the health or safety of any person;
2. Discrimination, defined as actions that deprive other members of the community of educational or employment access, benefits or opportunities on the basis of gender;
3. Intimidation, defined as implied threats or acts that cause an unreasonable fear of harm in another;
4. Hazing, defined as acts likely to cause physical or psychological harm or social ostracism to any person within the college community, when related to the admission, initiation, pledging, joining, or any other group-affiliation activity;
5. Bullying, defined as repeated and/or severe aggressive behavior likely to intimidate or intentionally hurt, control or diminish another person, physically or mentally (that is not speech or conduct otherwise protected by the 1st Amendment).
6. Violence between those in an intimate relationship to each other; and
7. Stalking, defined as repetitive and/or menacing pursuit, following, harassment and/or interference with the peace and/or safety of a member of the community; or the safety of any of the immediate family of members of the community.

RESOURCES FOR STUDENTS

South Coast College is committed to maintaining a positive learning, working and living environment. The College will not tolerate acts of sexual harassment or sexual violence or related retaliation against or by any employee or student. When sexual harassment or sexual violence has occurred and is brought to the attention of a responsible administrator, steps will be taken to end the harassment or violence, prevent its reoccurrence, and address its effects. The following resources list the confidentiality obligations of South Coast College personnel at South Coast College with respect to reports of sexual misconduct:

Student Counseling and Health Services (Confidential Reporting)
South Coast College has available confidential counseling for all registered students attending these institutions. Whether you are seeking support after a sexual assault or another form of sexual misconduct, contact Rebecca Remsen, Title IX coordinator, to obtain referrals to services..

Title IX Coordinator (Non-Confidential Reporting)
The Title IX Coordinator, Dean of Operations, is responsible for promoting an institutional environment that is free of gender bias, sexual harassment, and other forms of sexual misconduct. In addition, the Title IX Coordinator's role is to monitor and evaluate the institution's Title IX compliance efforts and make recommendations for any appropriate changes and improvements. The Title IX Coordinator oversees the administration of this policy and procedures in a neutral and equitable manner.

Campus Security (Non-Confidential Reporting)
Students may report sexual misconduct to Rebecca Remsen, Title IX coordinator, or a local law enforcement agency where the misconduct occurred. To submit a campus security report involving sexual misconduct, contact the Dean of Operations at (714) 867-5009.

South Coast College Faculty and Staff (Non-Confidential Reporting)
Students who report sexual misconduct behaviors to faculty and staff should not expect confidentiality. As mandated reporters, faculty and staff are obligated to report all statements of sexual misconduct to Rebecca Remsen, Title IX coordinator.

REPORTING SEXUAL MISCONDUCT

Time of Reporting a Complaint

South Coast College does not limit the time for filing a complaint of sexual misconduct. Due to the passage of time, the College's ability to investigate and respond effectively may be reduced substantially; however, this will not hinder offering remedies and oncampus/off-campus services to the complainant.

Requesting Confidentiality in Connection with a Report to the College

When the College becomes aware of sexual violence, the College may have an obligation to proceed with an investigation, regardless of a complainant's wishes, in order to ensure campus safety. You are not required to participate if you choose not to; however, this may limit the College's ability to respond to the incident. If you request that your name or other identifying information not be used in an investigation, the College will consider your request in light of the context of its responsibility to provide a safe and nondiscriminatory environment. In most cases, information including your name may be shared with the respondent, witnesses and with college officials who have a legitimate need to know. Beyond that, the College will take steps to protect your identity and the identity of all individuals involved. Anonymous allegations directed at anyone cannot be addressed.

Confidentiality

Any Information provided to The College employees may be shared with other The College employees, law enforcement, and other parties consistent with law, and only on a "need to know" basis. The College employees shall endeavor to honor any complainant's or victim's request for confidentiality; however, confidentiality cannot always be assured. The College may weigh requests for confidentiality against its duty to provide a safe and nondiscriminatory environment for all members of the campus community. Interim

Accommodations

The Title IX Coordinator, or designee, will work with the students affected by the sexual misconduct report to ensure safety and promote their well-being. Sometimes this assistance will take the form of immediate interim actions or accommodations to support and protect the involved students in the immediate aftermath of an incident and while an investigation or disciplinary action is pending. The Title IX Coordinator, or designee, may assign a victim's advisor to the person who reported the complaint or the complainant may choose his/her own. Likewise, the Title IX Coordinator may determine other remedies, such as, but not limited to, accommodations relating to changing academic schedules, restrictions on the alleged perpetrator pending investigation, and other remedies to promote the well-being, safety, and restoration of alleged victim.

Related Alcohol and Drug Violations

The institution understands that students are reluctant to file complaints of sexual misconduct when alcohol and/or drugs were illegally used. The severity of the infraction will determine the nature of the college's response, but whenever possible the college will respond educationally rather than punitively to the illegal use of drugs and/or alcohol associated with a report of sexual misconduct.

Unknown/Non-College Offenders

South Coast College will investigate reports of incidences affecting college students that are committed by individuals who are not members of the college community or whose identity is not known to the extent it is able, and take appropriate actions designed to protect affected students and others in the college. The College will offer appropriate remedies and on-campus/off-campus services to the complainant.

Campus Awareness Events and Programs

As a committed entity on educating our campus community of the impact that sexual misconduct has on an individual and the campus community, South Coast College supports public awareness events and programs surrounding these issues. The disclosure of incidents of sexual misconduct at such events is not considered a report to the campus for purposes of triggering an investigation of a particular incident.

Anti-Retaliation/Anti-Intimidation Policy

Any form of retaliation or intimidation against anyone who has complained of or formally reported discrimination, harassment, or sexual misconduct, or has participated in an investigation of such a complaint, regardless of whether the complaint relates to the complaining person or someone else, will not be tolerated, and violates both this policy and applicable law.

PROCEDURES FOR RESPONDING TO STUDENT SEXUAL MISCONDUCT

Rights of the Complainant and Respondent

South Coast College does not discriminate based upon age, race, ethnicity, sexual orientation, gender, national origin, veteran's status, gender identification, or genetic information in administering The College educational policies and procedures. The College complies with the American with Disabilities Act of 1990 (ADA) and Section 504 of the Rehabilitation Act of 1973. Students are entitled to a fundamentally fair process, including reasonable notice of allegations of violations of sexual misconduct, the opportunity for the student to be heard and to afford the student the opportunity to present evidence prior to the administrative determination of the alleged violations, except when immediate interim suspensions or restrictions are deemed necessary pending an investigation and determination of the matter. Any Sanctions imposed under this policy shall be appropriate to the nature of the violations, as determined by the College designee or panel.

Throughout this process, both the complainant and respondent have the following rights:

- To be treated with respect by The College officials
- To take advantage of campus support resources to help remedy and restore
- To experience a safe living, education, and work environment

- To have an advisor during an adjudication process
- To refuse to have an allegation resolved through conflict resolution procedures
- To be free of retaliation
- To have complaints heard in substantial accordance with procedures To fully participate in any process whether the injured party is serving as the complainant or the institution is serving as complainant
- To be informed in writing of the outcome/resolution of the complaint, any sanctions imposed, and the rationale for the outcome, when permissible. Special Requests/Accommodations

The Student may have an interpreter attend the investigation meeting and the proceeding before the College Disciplinary Committee or Panel. An interpreter accompanying a Student to the proceeding before the investigator, College Disciplinary Committee, or Panel must provide evidence of his/her certification as a certified interpreter to the investigator and/or College Disciplinary Committee at least five days prior to the commencement of the proceeding. The interpreter may only interpret for the student, and shall not expand or enhance the student's testimony. Likewise, the use of assistive technology must be reviewed and approved at least five days prior to the commencement of the proceeding.

Student Right to Review Records

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

Parents or eligible students have the right to inspect and review the student's education records maintained by the college. Colleges are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.

Advisors

Student conduct proceedings are not formal court hearings but are administrative actions imposed by the College. Although The College-related sanctions may be imposed, the process is intended to provide an opportunity of learning. Both the complainant and the respondent (student charged) may elect to be accompanied by an advisor to any meeting(s) or interview(s). The advisor's role is limited to observing and consulting with and providing support to the complainant or respondent. An advisor may not participate (speak) in the investigation and hearing processes on the student's/complainant's behalf. The advisor should also maintain confidentiality.

Presence of Legal Counsel (Not an Advisor)

An attorney duly licensed to practice in the State of California may accompany the student to any proceeding. The attorney shall not make any statements or presentations to the judicial panel, examine or cross-examine any witnesses, or present evidence or any written material to the panel. An attorney may not in any way disrupt or interfere with the panel's process. Any violation of this section shall result in the immediate removal of the attorney. An attorney shall provide the College Disciplinary Committee with a retention letter confirming that he/she has been retained by the student at least five (5) days before the proceeding so that the necessary arrangements can be made for an attorney for the College to be present at the proceeding. The attorney's retention letter shall include the attorney's State Bar number and telephone number.

Declining to Participate

A complainant and/or respondent may decline to participate in the investigation and proceeding. In these cases, the investigation and adjudication process will continue and a determination of "responsible" or "not responsible" will be made without the benefit of the complainant's and/or respondent's input.

Reluctant to Make a Formal Complaint

As a complainant/victim of an incident of sexual misconduct, you may want to inform the college of the alleged violation and unwilling to participate further in any investigation and/or disciplinary action against the student(s) who has been accused. The College has an obligation to investigate to the extent of the information that is available and known. If during the investigation the investigator finds corroborating information, it may be determined that is necessary to move forward with the student conduct process without the involvement to the complainant or to implement other appropriate remedies. If a complainant does not wish to participate in the student conduct process, there is an obligation to document the incident. When a report is being documented, there will be no personally identifying information about the complainant. The complainant will be notified of any actions by the College, coupled with a letter stating the choice to participate in the investigation and/or student conduct process.

Written Submissions

Impact Statements

The purpose of impact statements is to allow the complainant and respondent, during the sanctioning process, to describe to the panel how this violation has had an impact on them. The panel only may use information from these statements to help determine an appropriate sanction(s). Impact statements may provide information about damage to complainant/respondent that would otherwise have been unavailable to the panel. A complainant is not required to appear before a panel but is empowered by the panel to convey their experience(s) in the case in written form.

Time Frames

The Title IX Officer, or designee, shall use best efforts to seek and resolve sexual misconduct reports within 60 calendar days of an initial report, not including appeals.
The general timeline is as follows:

- Review and investigation process begins within 7 calendar days after the date of the initial report.
- Investigation is completed within 25 calendar days after the investigation begins.
- Hearing (if any) is held within 20 calendar days after the conclusion of the investigation.
- Determination of the hearing is issued within 7 calendar days after the completion of the hearing.
- Notice of Sanction(s) issued within 7 calendar days after the completion of the hearing.
- Notice of appeals filed by either or both complainant and respondent to the College Disciplinary Committee within 7 calendar days after the notice of determination and sanction(s).
- Appeal hearing is held within 20 calendar days after complainant and/or respondent's notice of appeal was received.
- Determination of appeal hearing by the President, or designee, is issued within 7 days after the completion of the appeal hearing.

Notice

The Title IX Officer, or designee, will provide electronic mail notice to the involved parties with the following information:

- A description of the alleged violation(s);
- A description of the applicable policies;
- A statement of the potential sanctions/responsive actions that could result; and
- A required date, time, and location of the hearing, superseding all other campus and work activities.

If any party does not appear at the scheduled review, investigation, or proceeding, the meeting will be held in his/her absence. For compelling reasons, the Title IX Officer, or designee, may reschedule the meeting.
Time frames for reviews, investigations, and hearings may vary depending on the details of a case and at certain times of the academic year for possible violations that occur near, during, or after The College holidays, breaks, or the end of an academic term, in which meetings will be held immediately after the end of the term or during the summer, as needed, to meet the resolution timeline followed by this policy and procedures.

Investigation

South Coast College, through a trained Title IX Team, will investigate any and all reports of alleged violations of sexual misconduct. Anyone who believes the Student Code of Conduct on sexual misconduct has been violated should contact a mandated reporter at each The College campus. The investigators will interview the complainant, respondent, and any witnesses (if appropriate).

The investigator will also gather information, documents, and materials (if any) that is relevant to the case.
The College Disciplinary Committee makes a determination based on the investigation's evidence. After the investigation, the investigator refers the findings of the case to the College Disciplinary Committee, or designee, and may recommend or impose a "responsible" or "not responsible" determination. The investigator may also recommend appropriate sanctions.

Informal Resolution Options

If appropriate, the South Coast College Title IX Office may seek to resolve certain sexual misconduct cases through an informal process involving both the complainant and respondent:
Informal Resolution
The Respondent accepts the findings of the investigation and, if appropriate, sanctions by the Title IX Officer or designee.

Mediation

As mutually agreed upon by the Title IX Officer, complainant, and respondent, a participatory mediation between all parties involved may occur to resolve the alleged violation. Sanctions may be determined in mediation, as outlined in the U.S. Department of Education's "Dear Colleague Letter" (2011):
https://www2.ed.gov/about/offices/list/ocr/letters/colleague-201104.html

Administrative Resolution

The Title IX Officer, the respondent, and/or when appropriate, the complainant, may request an administrative hearing through a single College designated administrator, typically a Title IX Officer or designee.

Proceedings

If an informal resolution process is not available, the College will convene a trained formal judicial panel to conduct and to make a determination of the alleged violation and to impose possible sanctions. The College shall make reasonable efforts to give the student(s) an opportunity to refute the accusation or otherwise provide relevant information to the panel regarding the incident(s) which led to the belief by the investigator, or designee, that the student(s) violated the Student Code of Conduct in a proceeding format.

Construct of the Judicial Panel

The proceeding is closed to all persons except the: 1) College Disciplinary Committee; 2) student charged; 3) advisor; an attorney or other professional, expert, or consultant retained by the College; 4) witness(es) (while testifying); 5) a court-certified interpreter at the student's own

expense; 6) selected members of the panel; and 7) any person to assist the hearing officer. Likewise, the Title IX Coordinator, or designee, may be present to ensure a fundamentally fair process and compliance. Panel members for an appeal hearing will consist of South Coast College employees only. No students will be asked to serve on a hearing panel due to the sensitive nature of the subject matter.

If the student is a minor, the student's parent or legal guardian must be present during the hearing.

Selection of the Judicial Panel

The following process determines possible members of a judicial panel. Members come from the South Coast College. All members participating on a judicial panel are oriented and trained to adjudicate a sexual misconduct case. The College Disciplinary Committee, in consultation with the Title IX Coordinator, or designee, will devise the panel. The panel will consist of 3 or 5 members. a. Within thirty days of the beginning of the fall Semester, the College shall send a list of at least six faculty members who will be eligible to serve on a hearing panel to the College Disciplinary Committee. The list shall remain on file and in effect until a new list is provided. B. Managers and Classified personnel members of the panel will be chosen upon interest and availability.

Members of the Panel and a Conflict of Interest

The panel shall be chosen by the Dean of Operations except that the panel shall not include any person who was a participant in the event, out of which the disciplinary action arose, nor shall it include any person who has had a past association with the student or any other party to the hearing which could impede the individual's ability to act in a fair and impartial manner. A panel member who is chosen must disclose any potential or actual conflict of interest.

Parallel Student Conduct Proceedings

Student Conduct Code proceedings are independent from court or other administrative proceedings. Discipline may be instituted against a student also charged in civil or criminal courts based on the same facts that constitutes the alleged violation of the Student Code of Conduct. The College may proceed before, concurrently with, or after any judicial or other administrative proceedings, except in cases involving sexual misconduct. In sexual misconduct cases, the College shall proceed without undue delay in accordance with federal and state law requirements, and The College policies and procedures.

Proceeding Procedures

1. The chair will call the proceeding to order, explain the procedures of the proceeding, and have all parties introduce themselves.
2. The chair will present the guiding principles/norms of behavior in the proceeding to guarantee control of the proceeding, make certain that all parties respect the right of others to make statements, and to ensure confidentiality.

3. The Dean of Operations, and if applicable her/his witness(es), shall have up to forty-five (45) minutes to present relevant evidence conducted by the investigator and witnesses (if 11 applicable) to support the determination by the College Disciplinary Committee that a violation of the Student Code of Conduct has occurred.
4. The respondent may question any witnesses presented by the College Disciplinary Committee. Members of the panel may also question any witness(es) presented by the College Disciplinary Committee. Questioning by the student or the committee shall not be considered part of the time allotted for presentation of the College Disciplinary Committee's evidence. It is the discretion of the chair to impose a timeline on questioning.
5. The student charged, and if applicable her/his witness(es), shall have up to forty-five (45) minutes, if necessary, to present relevant evidence bearing on the accusation. The

College Disciplinary Committee may question any witnesses represented by the student. Members of the panel may also question witnesses. Questioning by the panel shall not be considered part of the time allotted for presentation of the student's evidence. It is the discretion of the chair to impose a timeline on questioning.

6. The College Disciplinary Committee, and then the student charged may make a closing statement to the panel. These closing statements shall be limited to a maximum of ten minutes each. The chair shall have the authority to extend the time limits, but must ensure equal time.

Once all information has been collected, the chair, or designee, will:

7. Reiterate the alleged policy violation(s);
8. Remind all parties involved of the Standard of Proof (Preponderance of Evidence);
9. Remind all parties of confidentiality and of all imposed interim sanctions that are active and must be adhered to;
10. Remind all parties to review South Coast College's Student Code of Conduct to understand their student rights and responsibilities;
11. Inform all parties of the deliberation process and the projected timeline for notification; and
12. Remind the respondent and the complainant, if applicable, that notification and all communication are via The College email accounts.

Additional proceeding rules include:

- Information Regarding Romantic or Sexual History. The panel will not consider the romantic or sexual history of either the complainant or the respondent in cases involving allegations of sexual misconduct, except for testimony offered by one or the other about the complainant's and respondent's shared sexual history that the panel deems relevant. The existence of a sexual relationship between the complainant and respondent does not support the inference of consent to alleged sexual misconduct.

- Prior Conduct Violation. The hearing panel will not consider the respondent's prior conduct violations, unless:

1. The respondent was previously found to be responsible, and
2. The previous incident was substantially similar to the present allegation(s) and/or the information indicates a pattern of behavior by the respondent.

Use of Cell Phones and Recording Devices. Cell phones and recording devices may not be used in the investigation meetings and hearings.

Panel Determination/Standard of Proof

The panel will find a student either "responsible" or "not responsible" based on a majority vote. If a panel determines a student is "responsible" for violating the Student Code of Conduct, the matter will advance to the sanctioning stage. In all cases involving alleged violations of the Student Code of Conduct, the standard of proof is the "preponderance of the evidence" standard as set forth in the definitions herein (e.g., more likely than not). This standard is also employed when making determinations regarding interim restrictions/actions.

Sanctions

How Sanctions are Determined

It is the commitment from the College that respondents found "responsible" for violating sexual misconduct policies are imposed of sanctions that are:

- Fair and appropriate given the facts of the particular case;
- Consistent with the College's handling of similar cases;
- Adequate to protect the safety of the campus community; and
- Reflective of the seriousness of the sexual misconduct.

The relevant factors that are considered when imposing sanctions are:

1. The specific sexual misconduct at issue (such as penetration, touching, unauthorized recording, and so on;
2. The circumstances accompanying the lack of consent (such as force, threat, coercion, incapacitation, and so on);
3. The respondent's state of mind (intentional, knowing, bias-motivated, reckless, and so on);
4. The impact of the offense on the complainant;
5. The respondent's disciplinary history;
6. The safety of the campus community; and
7. The conduct respondent's conduct during the disciplinary process.

Non-Appealable Sanctions

The following sanctions may be imposed for violation of this Student Code of Conduct. These sanctions are not exclusive and may not be appealed:

- Disciplinary Probation consists of written notice to the student by the College

Disciplinary Committee that the student has violated this Student Code of Conduct (including a specified period of time) with conditions as imposed by the College Disciplinary Committee. Any subsequent violations of this policy by the student during the term of the probation or the student's failure to comply with any condition of probation imposed by the College Disciplinary Committee will result in additional sanctions under this policy.

- The College Restriction. The College Disciplinary Committee may for a specified period of time restrict the student's access to parts or areas of the College and/or The College property.

- Exclusion From The College Activities prohibits the student from participating in any The College co-curricular and/or extra-curricular activity(ies) for a period to be determined by the College Disciplinary Committee.

- Mental Health Clearance. Mental Health Clearance may be required before a student is readmitted to a particular class or allowed to come onto The College property. The College Disciplinary Committee must receive a letter from a licensed mental health professional stating that in his/her professional judgment the student will no longer continue the behavior which gave rise to the College Disciplinary Committee taking disciplinary action against him/her or that the student's continued presence on campus is not a threat to himself/herself or others. The mental health professional must be licensed by the State of California and the College The College Administrator must verify that the mental health professional is credentialed to render a professional opinion. The student shall bear the cost and expense of obtaining mental health clearance.

- Restitution requires the student to repay the College or any person for the cost of replacing or repairing any property taken, destroyed or damaged by the student. This student may also be charged a service charge and/or collection fee under the College policy regarding service charges and collection fees.

- Restriction from Attendance at The College Events. The College Disciplinary Committee may restrict the student from attending some or all The College events for a specified period of time.

- Short Term Removal From Class for a period not to exceed four class meetings, may be imposed by any instructor on a student who is disrupting the class or otherwise interfering with the ability of other students in the class to learn. Before removing a student from class, an 13 instructor shall first give or make reasonable efforts to give the student notice of his/her intent to remove the student and a reasonable opportunity for the student to modify his/her behavior. The instructor or program supervisor shall notify the College Disciplinary Committee, in writing, immediately following his/her removal of a student under this section, with a copy to the Dean of the academic division. The student may not return to the class until the student has met with the College Disciplinary Committee. The College Disciplinary Committee shall contact the student to arrange such a meeting.

- Short Term Suspension prohibits the student from attending classes or entering onto any The College Property for a period of one (1) to ten (10) days as determined by the College Disciplinary Committee.

- Hold on Records which consists of the withholding of transcripts and/or other student records. This is imposed when a student fails to repay debts to the College, return The College equipment or make restitution to the College. A hold on records may also be asserted if a student does not comply with requests such as, but not limited to, required meeting or appointments.

- Administrative Withdrawal from Class prohibits a student's continued presence in the class if his/her behavior is disruptive of the class and interferes with the ability of other students in the class to learn or in any way endangers himself/herself or others. When this sanction is applied the student will be administratively withdrawn by College Disciplinary Committee.

- Grade Change from a "Withdraw" to a letter grade may be imposed where the College Disciplinary Committee, together with the instructor, determine this is an appropriate sanction.

- Written Warning is a written reprimand and warning to the student by the College Disciplinary Committee that he/she has determined that the student has violated this Student Code of Conduct and is on notice.

Appealable Sanctions

The following sanctions imposed by the College Disciplinary Committee or panel may be appealed:

- Expulsion prohibits the student from attending any classes or registering as a student in the College for an indefinite period of time. Expulsion prohibits the student from entering onto any The College property without written permission of the College. Expulsion will be imposed immediately. When expulsion has been recommended, the student shall be immediately suspended pending Committee action.

- Long Term Suspension prohibits the student from attending classes, registering as a student or entering onto any The College property without written permission of the College Disciplinary Committee for a period from eleven (11) days to three (3) years as determined by the College Disciplinary Committee and/or the College President. Long term suspension may be imposed immediately or at the end of the current term at the discretion of the College Disciplinary Committee.
  A student may be required to attend classes at their own expense to further educate the student in the severity of the exhibited behavior.

Ongoing Accommodations for Complainant

Whatever the outcome of the informal resolution or hearing process, a complainant may request ongoing or additional accommodations. In consultation with other campus entities, a determination will be made on whether such measures are appropriate.

Potential ongoing accommodations include:

- Providing an escort to vehicle.
- Changing the complainant's academic schedule.
- Adjusting the complainant's on campus work schedule.
- Allowing the complainant to withdraw from or retake a class without penalty. Providing access to tutoring or other academic support, such as extra time to complete or retake a class.

Additional Responses

The College may also determine that additional measures are appropriate to respond to the effects of the incident. Additional responses for the benefit of the College community may include:

- Revision of the College's policies and procedures regarding sexual misconduct.
- Additional training and education materials for students, faculty, and staff.
- Increased monitoring, supervision, or security at locations or events where the sexual misconduct occurred.
- Ensuring relevant climate surveys that focus on safety, security, inclusion are gathered to improve on developing a culture that is intolerant of sexual misconduct. Appeals

Either the complainant or the respondent or both may appeal the determination of the judicial panel and/or sanctions. Disagreeing with the finding of the sanction is not, by itself, grounds for appeals. Students are allowed one appeal. The decision of the appeal panel is final.

Specific Grounds for Appeal:

1. A procedural error or omission occurred that significantly impacted the outcome of the hearing (for example, substantiated bias, material deviation from established procedures, and so on).
2. The sanction is excessive, insufficient, or significantly disproportionate to the violation.

DEFINITIONS

Sexual Misconduct

- An umbrella term for offenses that are sexual or gender-based, which include, but are not limited:
- Sexual Harassment
- Non-Consensual Sexual Contact (or attempts to commit same)
- Non-Consensual Sexual Intercourse (or attempts to commit same)
- Sexual Exploitation

Non-Consensual Sexual Contact

Non-consensual sexual contact is any intentional sexual touching, however slight, with any object, by a man or a woman upon a man or a woman that is without consent and/or by force. The determination of whether an environment is "hostile" must be based on all of the circumstances. These circumstances could include:

- The frequency of the conduct;
- The nature and severity of the conduct;
- Whether the conduct was physically threatening;
- Whether the conduct was humiliating;
- The effect of the conduct on the alleged victim's mental or emotional state; Whether the conduct was directed at more than one person;
- Whether the conduct arose in the context of other discriminatory conduct;
- Whether the conduct unreasonably interfered with the alleged victim's educational or work performance;
- Whether the statement is a mere utterance of an epithet which engenders offense in an employee or student, or offends by mere discourtesy or rudeness
- Whether the speech or conduct deserves the protections of academic freedom or the 1st Amendment.

Sexual Contact

Includes Intentional contact with the breasts, buttock, groin, or genitals, or touching another with any of these body parts, or making another touch you or themselves with or on any of these body parts; any intentional bodily contact in a sexual manner, though not involving contact with/of/by breasts, buttocks, groin, genitals, mouth or other orifice.

Non-Consensual Sexual Intercourse

Non-Consensual Sexual Intercourse is any sexual intercourse however slight, with any object, by a man or woman upon a man or a woman that is without consent and/or by force. Intercourse includes: vaginal penetration by a penis, object, tongue or finger, anal penetration by a penis, object, tongue, or finger, and oral copulation (mouth to genital contact or genital to mouth contact), no matter how slight the penetration or contact.

Sexual Harassment

Sexual Harassment is unwelcome, gender-based verbal or physical conduct that is, sufficiently severe, persistent or pervasive that it, unreasonably interferes with, denies or limits someone's ability to participate in or benefit from the college's educational program and/or activities, and is based on power differentials (quid pro quo), the creation of a hostile environment, or retaliation. Examples include: an attempt to coerce an unwilling person into a sexual relationship; to repeatedly subject a person to egregious, unwelcome sexual attention; to punish a refusal to

comply with a sexual based request; to condition a benefit on submitting to sexual advances; sexual violence; intimate partner violence, stalking; gender-based bullying.

Sexual Exploitation

Occurs when a student takes non-consensual or abusive sexual advantage of another for his/her own advantage or benefit, or to benefit or advantage anyone other than the one being exploited, and that behavior does not otherwise constitute one of other sexual misconduct offenses. Examples of sexual exploitation include, but are not limited to:

- Invasion of sexual privacy;
- Prostituting another student;
- Non-consensual video or audio-taping of sexual activity;
- Going beyond the boundaries of consent (such as letting your friends hide in the closet to watch you having consensual sex);
- Engaging in voyeurism;
- Knowingly transmitting an STI or HIV to another student;
- Exposing one's genitals in non-consensual circumstances; inducing another to expose their genitals;
- Sexually-based stalking and/or bullying may also be forms of sexual exploitation

Force

Force is the use of physical violence and/or imposing on someone physically to gain sexual access. Elements of force also includes physical force, threats, intimidation (implied threats) and coercion that overcome resistance or produce consent ("Have sex with me or I'll hit you. Okay, don't hit me. I'll do what you want.").

Physical Force (violence, abuse, compulsion) – Physical force is the classic construct, equated with violence or the use of a weapon. No matter how slight, any intentional physical impact upon another, use of physical restraint or the presence of a weapon constitutes the use of force.

Threats (harassment) – Any threat that causes someone to do something they would not have done absent the threat is enough to prove forcible compulsion. For example, if I threaten you with a negative consequence and that threat causes you to acquiesce in sexual activity, forcible compulsion is present, and sexual misconduct has occurred. - If you don't have sex with me, I will harm someone close to you - If you don't have sex with me, I will tell people you raped me
- If you do not have sex with me, I will spread a rumor you are gay
- If you don't sleep with me, I will fail you

Intimidation (implied threats, abuse) – Intimidation is defined as an implied threat, whereas threats are clear and overt. It is a situation where someone uses their power or authority to influence someone else.

Coercion (pressure, duress, cajoling, compulsion, abuse) – Coercion is unreasonable pressure for sexual activity. Coercive behavior differs from seductive behavior based on the type of pressure someone uses to get consent from another. When someone makes clear to you that they do not want sex, that they want to stop, or that they do not want to go past a certain point of sexual interaction, continued pressure beyond that point can be coercive.
- Cases will be investigated regardless of whether the accuser resisted the sexual advance or request, but resistance is a clear demonstration of non-consent. The presence of force is not demonstrated by the absence of resistance. Sexual activity that is forced is by definition non-consensual, but non-consensual sexual activity is not by definition forced.
- In order to give effective consent, one must be of legal age (18 years or older). - Sexual activity with someone who one should know to be—or based on the circumstances should reasonably have known to be—mentally or physically incapacitated (by alcohol or other drug use, unconsciousness or blackout), constitutes a violation.

Stalking

A course of conduct directed at a specific person that would cause a reasonable person to feel fear or suffer substantial emotional distress. Stalking involves repeated and continued harassment against the expressed wishes of another individual, which causes the targeted individual to feel emotional distress, including fear or apprehension. Stalking behaviors may include: pursuing or following; unwanted communication or contact—including face-to-face, telephone calls, voice messages, electronic messages, web-based messages, text messages, unwanted gifts, and so on; trespassing; and surveillance or other types of observation.

Domestic Violence

The use of physical violence, coercion, threats, intimidation, isolation, stalking, or other forms of emotional, sexual or economic abuse directed towards (a) a current or former spouse or intimate partner; (b) a person with whom one shares a child; or (c) anyone who is protected from the respondent's acts under the domestic or family violence laws of California. This includes any behaviors that intimidate, manipulate, humiliate, isolate, frighten, terrorize, coerce, threaten, blame, hurt, injure, or wound someone. Domestic violence can be a single act or a pattern of behavior in relationships.

Dating Violence

The use of physical violence, coercion, threats, intimidation, isolation, stalking, or other forms of emotional, sexual or economic abuse directed towards a person who is or has been in a social relationship of a romantic or sexually intimate nature with the victim. This includes any behaviors that intimidate, manipulate, humiliate, isolate, frighten, terrorize, coerce, threaten, blame, hurt, injure, or wound someone. Dating violence can be a single act or a pattern of behavior in relationships.

Consent

Consent is informed. Consent is an affirmative, unambiguous, and conscious decision by each 17 participant to engage in mutually agreed-upon sexual activity.

Consent is voluntary. It must be given without coercion, force, threats, or intimidation. Consent means positive cooperation in the act or expression of intent to engage in the act pursuant to an exercise of free will.

Consent is revocable. Consent to some form of sexual activity does not imply consent to other forms of sexual activity. Consent to sexual activity on one occasion is not consent to engage in sexual activity on another occasion. A current or previous dating or sexual relationship, by itself, is not sufficient to constitute consent. Even in the context of the relationship, there must be mutual consent to engage in sexual activity. Consent must be ongoing throughout a sexual encounter and can be revoked at any time. Once consent is withdrawn, the sexual activity must stop immediately.

- Consent cannot be given when a person is incapacitated. A person cannot consent if she/he is unconscious or coming in and out of consciousness. A person cannot consent if she/he is under the threat of violence, bodily injury or other forms of coercion. A person cannot consent if her/his understanding of the act is affected by a physical or mental impairment.

Retaliation

Any act of reprisal is a violation of policy. Examples of actions that might be retaliation against a complainant, witness, or other participant in the complaint process include:

- Singling the person out for harsher treatment;
- Lowering a grade or evaluation;
- Failing to hire, failing to promote, withholding pay increase, demotion, or discharge; Providing negative information about the person in order to interfere with his or her prospects for employment, admission, or academic program.

Hostile Environment

A hostile environment may arise when unwelcome conduct of a sexual or gender-based nature affects a student's ability to participate in or benefit from an education program or activity, or creates an intimidating, threatening or abusive educational and/or living environment. A single, isolated incident of sexual or gender-based harassment may, based on the facts and circumstances, create a hostile environment.

Incapacitation

Incapacitation is a state where someone cannot make rational, reasonable decisions because they lack the capacity to give knowing consent (e.g., to understand the "who, what, when, where, why, or how" of their sexual interaction).

The College policy also covers a person whose incapacity results from mental disability, sleep, involuntary physical restraint, or from the taking of rape drugs. Possession, use and/or distribution of any of these substances, including but not limited to Rohypnol, Ketamine, GHB, Burundanga, and so on, is prohibited, and administering one of these drugs to another student is a violation. More information on these drugs can be found at 911 Rape Information.

Complainant "Complainant" means the person(s) reporting alleged violations of this Student Code of Conduct.
Respondent "Respondent" means the person(s) who are alleged to have violated the Student Code of Conduct.

Requirements

In order to develop, implement, and maintain your information security program, you shall:
Designate an employee or employees to coordinate your information security program.
Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
Employee training and management;
Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
Detecting, preventing and responding to attacks, intrusions, or other systems failures.
Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
Oversee service providers, by:
Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
Requiring your service providers by contract to implement and maintain such safeguards.
Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.
Cybersecurity Compliance – General Overview
As the number and severity of cyberattacks increases, industry standards organizations and governments seek to enforce cybersecurity by establishing more stringent compliance requirements. However, compliance requirements often lag behind cybersecurity risk. Therefore, to prepare for changing compliance requirements, organizations need to create an approach to cybersecurity so that they can stay ahead of the evolving requirements.

What are the data breach risks?
The **2019 Data Breach Investigation Report** noted several trends.
43% of data breaches involved small businesses
69% of breaches were perpetrated by outsiders
53% of breaches featured hacking
33% of breaches included social engineering
71% of breaches were financially motivated
56% of breaches took months or more to discover

The newest statistics indicate that cybercriminals target small businesses to gain unauthorized access to data that they can sell on the dark web. Hacking and social engineering attacks focus on exploiting weaknesses in systems, networks, software, and people to gain entry.

Many small businesses currently lack the appropriate resources necessary to defend against these attacks, which increases the likelihood that cybercriminals will continue to target them.

What is compliance?

In general, compliance is defined as following rules and meeting requirements. In cybersecurity, compliance means creating a program that establishes risk-based controls to protect the integrity, confidentiality, and accessibility of information stored, processed, or transferred.

However, cybersecurity compliance is not based in a stand-alone standard or regulation. Depending on the industry, different standards may overlap, which can create confusion and excess work for organizations using a checklist-based approach.

For example, the healthcare industry needs to meet Health Insurance Portability and Accountability Act (HIPAA) compliance requirements, but if a provider also accepts payments through a point-of-service (POS) device, then it also needs to meet Payment Card Industry Data Security Standard (PCI DSS) requirements.

Moreover, as compliance requirements shift from control-based to risk-based, the landscape of cybersecurity compliance also shifts.

Steps to Creating a Cybersecurity Compliance Program

Create a Compliance Team

Even in small to mid-sized businesses, a compliance team is necessary. Cybersecurity does not exist in a vacuum. As organizations continue to move their business critical operations to the cloud, they need to create an interdepartmental workflow and communicate across business and IT departments.

Establish a Risk Analysis

As more standards and regulations focus on taking a risk-based approach to compliance, organizations of all sizes need to engage in the risk analysis process.

Identify

Identify all information assets and information systems, networks, and data that they access.

Assess Risk

Review the risk level of each data type. Determine where high risk information is stored, transmitted, and collected and rate the risk of those locations accordingly.

Analyze Risk

After assessing risk, you need to analyze risk. Traditionally, organizations use the following formula: Risk = (Likelihood of Breach x Impact)/Cost

Set Risk Tolerance

After analyzing the risk, you need to determine whether to transfer, refuse, accept, or mitigate the risk.

Set Controls

Based on your risk tolerance, you need to determine how to mitigate or transfer risk. Controls can include:

Firewalls

Encryption

Password policies

Vendor risk management program

Employee training

Insurance

Create Policies

Policies document your compliance activities and controls. These policies serve as the foundation for any internal or external audits necessary.

Continuously Monitor and Respond

All compliance requirements focus on the way in which threats evolve. Cybercriminals continuously work to find new ways to obtain data. Rather than working to find new vulnerabilities, called Zero Day Attacks, they prefer to rework existing strategies. For example, they may combine two different types of known ransomware programs to create a new one.

Continuous monitoring only detects new threats. The key to a compliance program is to respond to these threats before they lead to a data breach. Without responding to an identified threat, the monitoring leaves you open to negligence arising from lack of security.

Why you need continuous documentation for continuous assurance Security is the act of protecting your information. Compliance is the documentation of those actions. While you may be protecting your systems, networks, and software, you cannot prove control effectiveness without documentation.

Documenting your continuous monitoring and response activities provides your internal or external auditors with the information necessary to prove governance. Moreover, the documentation process eases conversations with business leadership and enables the Board of Directors to better review cybersecurity risk. Since compliance requirements focus on Board governance over the cybersecurity program, documenting risk, monitoring, and remediation in an easy-to-digest way enables you to meet these compliance requirements.

Why you need a single-source-of-information. With the number of stakeholders involved in cybersecurity compliance activities, maintaining shared documents leads to a variety of potential compliance risks. Shared documents can be updated without the document owner's knowledge. People can make copies which leads to multiple versions which leads to lack of visibility.

A single-source-of-information allows all stakeholders to track and review compliance activities while maintaining compliance data integrity.

PURPOSE

This policy defines security requirements that apply to all information assets of South Coast College. All departments of South Coast College must meet South Coast College security of business needs or satisfy specific legal requirements listed below which exceed the security requirements instituted in this document; but all departments must, at a minimum, achieve the security levels required by this policy.
The primary objectives of this policy and security programs are to:

Manage the risk of security exposure or compromise of South Coast College information assets;
Designate responsibilities for the protection of South Coast College information;
Optimize the integrity and reliability of South Coast College information assets;
Reduce opportunities for the introduction of errors in information assets supporting South Coast College business processes;
Protect South Coast College senior management and staff, and preserve senior management's options in the event of an information asset misuse, loss or unauthorized disclosure;
Promote and increase the awareness of information security at South Coast College.
Support the Mission Statement of South Coast College.

SCOPE

This policy is applicable to entities, staff and all others who have access to or manage South Coast College information. This policy encompasses all information systems for which South Coast College has administrative responsibility. It addresses all digital information which is created or used in support of South Coast College business activities. Where conflicts exist between this policy and a South Coast College departmental policy, the more restrictive policy will take precedence.

Information security refers to the protection of information from accidental or unauthorized access, destruction, modification or disclosure. Digital information is defined as the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by computer automated means. Digital information is relayed in a variety of methods, including through computer networks and portable media, such as jump drives, CD‟s and DVD‟s. Digital information is also stored and retrieved in several formats, including but not limited to computer databases or transmissions, tapes, CD ROMs, diskettes, computer generated reports, hard copy documentation, e-mail messages, and voice mail.

This policy must be communicated by supervisors to all employees and all others who have access to or manage South Coast College digital information. This security policy is technology independent and does not include implementation standards, processes or procedures.

DEFINITIONS

Authorized User refers to any individual granted credentials to access South Coast College Information Technology Resources.

Credentials refer to the unique username and password provided each authorized user to access South Coast College resources.

Database Administration - The function of applying formal guidelines and tools to manage the College's information resource and specifying, implementing, and maintaining access control to assure that Data Users have the appropriate authorized access needed to perform assigned duties or to fulfill College roles is termed database administration. Responsibility for database administration activities is shared among the Data Stewards, Data Experts/ and ITS Database Administrators.

Data Definition - Data Stewards and Data Experts provide data descriptions so Data Users know what shareable data are available, what the data mean, and how to access and process the data. These data about the data are referred to as data definitions and sometimes called metadata. Data definitions may be stored in an integrated or complementary database known as a *Metadata Repository*.

Digital Information is defined as the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by computer automated means.

Digital Systems refers to the computer platform on which digital information is stored and used.

Highly Sensitive Information refers to information that is considered confidential.

Information Assets refers to the data and resources owned and protected by South Coast College.

Metadata Repository refers to a database system that contains descriptive information about the College's enterprise data and administrative systems. The repository is a complementary facet of the Data Warehouse.

Moderately Sensitive Internal Business-Use Data refers to those elements of the COLLEGE DATABASE that may be accessed by all employees of the College, with authorization, for the conduct of College business.

Non-sensitive Public Data refers to the elements of the COLLEGE DATABASE that are available to the general public, including people outside of South Coast College.

Open-port facilities refer to the communication end point in computer networking configured to accept units of data.

Portable Computing Devices and Information Media refers to any mobile computing device such as a laptop, smart phone, personal data assistant, flash drive or other storage media.

Sensitive (or critical) systems and applications refer to systems such as the Student Information System and Human Resource system that house confidential student and employee data.

South Coast College Application Owners refers to the users of software

South Coast College Electronic Resources refers to information available online via the South Coast College network or the World Wide Web.

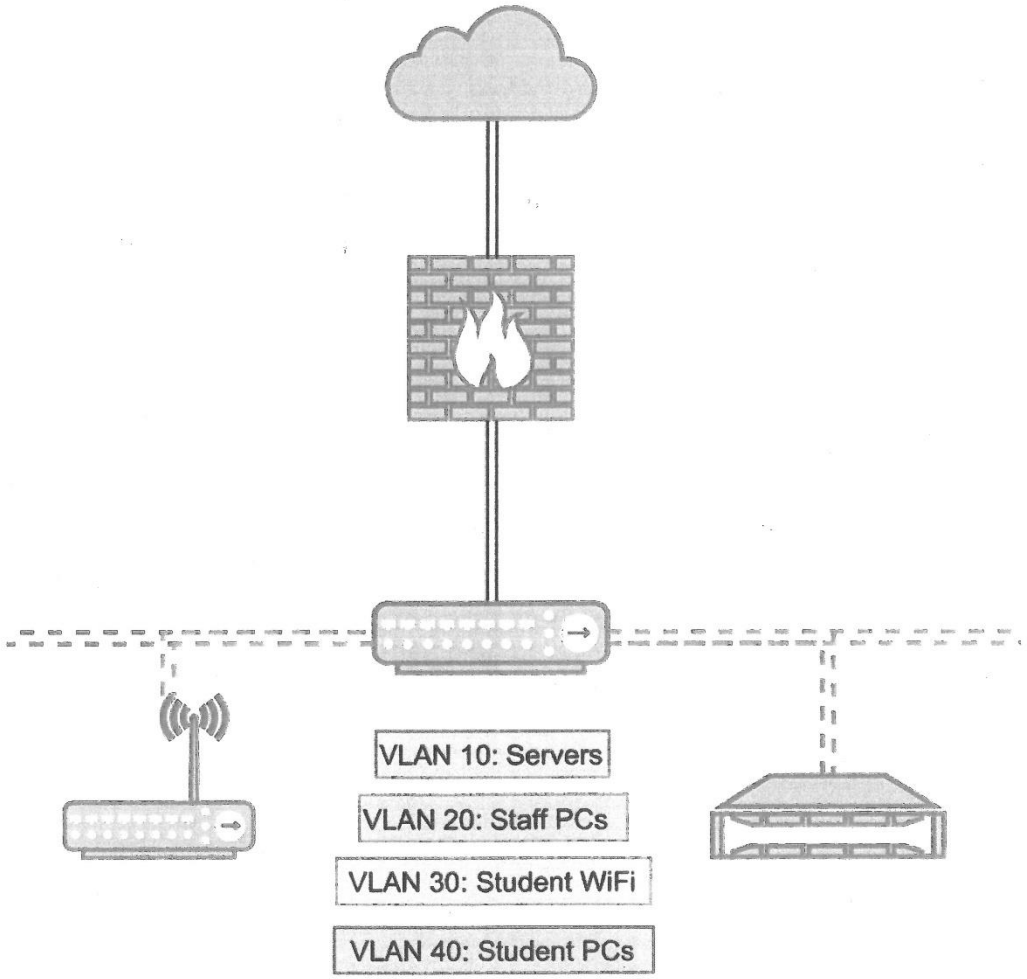
System Administration - The function of maintaining and operating hardware and software platforms is termed system administration. Responsibility for system administration activities belongs to the Computing Services unit of ITS.

COLLEGE DATABASE (College Enterprise Database) is a conceptual term used to identify that body of data critical to College planning, management, and business operations of both administrative and academic units. This data may reside in different database management systems and on different machines, but in aggregate may be thought of as forming one logical College resource, which is called the COLLEGE DATABASE. The COLLEGE DATABASE contains data from multiple operational areas that need to be integrated in order to support institutional research, business analysis, reporting, and decision making.

College Information System is a conceptual term used to identify the collection of computer hardware, software, and network connections, which together form the integrated system underlying the logical College Enterprise Database (COLLEGE DATABASE).

Network Layout (Map) is a physical representation of how each computer is connected to the server(s). Below is the drawing of the South Coast College network layout.

South Coast College (SCC) Building Layout (Figure 1)


VLAN 10: Servers
VLAN 20: Staff PCs
VLAN 30: Student WiFi
VLAN 40: Student PCs

POLICY

Part 1. Preface

This policy is a statement of the goals, ethics, responsibilities and accepted behaviors required to establish and maintain South Coast College's information security objectives; it sets the direction, offers broad guidance and defines senior management's requirements for digital information security related processes and actions. Compliance is mandatory. *This policy follows the framework of safeguard requirements of GLBA in audits of postsecondary institutions or third-party services under the regulations in 16 C.F.R. Part 314* for Security Policy guidelines and is consistent with existing South Coast College policies, rules and standards. This policy documents many of the security practices already in place. Senior management is fully committed to information security and agrees that every person employed by or on behalf of South Coast College has important responsibilities to continuously maintain the security and privacy of South Coast College data.

Part 2. Document Change Management

Requests for changes to this policy should be presented by the South Coast College Chief Information Officer (CIO) to Senior Management. If senior management agrees to the change(s), the Chief Information Officer (CIO) will be responsible for communicating the approved change(s) to the South Coast College community.

This policy and supporting policies and standards will be reviewed on an annual basis.

Part 3. Data Management Roles and Responsibilities

Authorized User refers to any individual granted credentials to access South Coast College Information Technology Resources.

Chief Information Officer, CIO: The College official responsible for overseeing the management of College-wide data systems.

Database Administrators (DBAs): Data administration involves the application for formal guidelines and the appropriate tools to manage South Coast College's information resources (provide a secure infrastructure in support of data including, but not limited to, providing physical security, backup and recovery processes, granting and terminating access privileges as authorized by data stewards, and implementing and administering controls over the information).

Data Stewards: Data Stewards are College officials (e.g. Directors, Managers, or their designees) having direct operational level responsibility for information management (capture, maintenance, and dissemination of data). Data stewards are responsible for: working with Data Trustee/Owner to classify data, approving data access on behalf of Data Trustee/Owner, determining/specifying user access level(s), securing paper infrastructure and implementing and enforcing departmental policy and procedures.

Data Trustees/Owners: Data Trustees/Owners are senior College officials (e.g. Deans, VPs, AVPs, or their designees) responsible for overseeing the establishment of data management policies and procedures, the assignment of data management responsibility (assigning data stewards) and promoting data resource management for the good of the entire College.
Data Users: Data users are individuals who need and use South Coast College data as part of their assigned duties or in fulfillment of assigned roles or functions within the College community. Individuals who are given access to sensitive data have a position of special trust, and as such, are responsible for protecting the security and integrity of those data. Anyone who has intentionally breached the confidentiality and/or compromised the integrity of protected data/information may be subject to disciplinary action and/or sanctions up to, and including discharge or dismissal in accordance with South Coast College policy and procedures. Additionally, breach of confidentiality and/or compromising integrity of data/information that are protected by law, acts, or regulations, will result in criminal prosecution.

Information Security Program Team (ISec): The Information Security Program Team, appointed by the South Coast College President, will coordinate and oversee implementation of information security awareness program activities, will approve and support major initiatives to enhance information security, and will develop a process to measure compliance with policy. The Information Security Program Team is responsible for investigating (and responding to) all alleged security violations.

Information Technology Services (ITS): ITS is responsible for the *data* processing infrastructure and computing network which support *information owners*. It is the responsibility of ITS to support this policy and provide resources needed to enhance and maintain the required level of digital *information security*.

Non-South Coast College Employees: Employees such as Contractors, Consultants, Vendors and other persons, to the extent of their present or past access to South Coast College information assets, are also covered by this policy.

Senior Management: Senior Management includes the President and Vice Presidents (known as members of the South Coast College President's Cabinet).
South Coast College Employees: It is the responsibility of all employees to protect South Coast College information and resources, to note variances from established procedures, and to report such variances for suspected security incidents to the appropriate supervisor(s) and to the Director of Internal Control, co-chair of the Information Security Program Team.
Supervisors: Supervisors will be responsible for the implementation of this and other information security policies and the compliance of their employees. Supervisors must educate their employees with regard to information security issues, including information retention policies. Supervisors will explain the issues, the rationale for the policies, the role(s) individuals have in safeguarding information assets, as well as the consequences of non-compliance. It is the

responsibility of the supervisor to notify DBA and System Administrators when staff members terminate employment.

System Administrators: System Administrators are the staff members responsible for administering security tools, auditing security practices, identifying and analyzing security *threats* and solutions, implementing specific security *controls* and responding to security violations. They have administrative control over *user*-IDs and passwords and the associated processes for reviewing, logging, implementing access rights, emergency privileges, exception handling, and reporting requirements.

Part 4. Information Security Policy

Information is among South Coast College's most valuable assets and South Coast College relies upon that information to support its mission of teaching, research and service as well as its business activities. Information must be protected from the time it is created, through its useful life, and authorized disposal since quality and availability of that information is key to South Coast College's ability to carry out these missions. Therefore, the security of South Coast College's information, and of the technologies and systems that support it, is the responsibility of everyone concerned. Each authorized user of South Coast College information has an obligation to preserve and protect said information assets in a consistent and reliable manner. Information must be classified and protected based on its importance to business activities, risks and security practices as defined in 16 C.F.R. 314.4(b), a Code of Practice for Information Security Management, and as implemented by this policy. Security controls provide the necessary physical, logical and procedural safeguards to accomplish those goals. Information security management enables information to be shared while protecting the information and its associated computer assets including the network over which the information travels. South Coast College Data Trustees and Stewards are responsible for ensuring that appropriate physical, logical and procedural controls are in place on these assets to preserve the confidentiality, integrity, availability and privacy of South Coast College information.

Individual Accountability

Individual accountability is the cornerstone of any security program. Without it, there can be no security. Individual accountability is required when accessing all South Coast College electronic resources or when terminating employment. Access to South Coast College computer systems and networks is provided through the use of individually assigned unique computer identifiers known as user-ID and password. Individuals who use South Coast College computer resources must only access resources to which they are authorized. Passwords must be treated as confidential information and must not be disclosed. All individuals are responsible for all activities performed under their user-ID. For the user's protection and for the protection of South Coast College resources, passwords (or other tokens or mechanisms used to uniquely identify an individual) must not be shared. Upon termination of employment, individuals are required to archive or delete information according to record retention policy.

Confidentiality/Integrity/Availability

All South Coast College information will be protected from unauthorized access to help maintain information's confidentiality and integrity. The information owner will classify and secure information within their jurisdiction based on the data classification guidelines in the "Information Management and Security Procedural Document" according to the information's value, sensitivity to disclosure, consequences of loss or compromise and ease of recovery.

Information will be readily available for authorized use as needed by the user in the normal performance of their duties. Appropriate processes will be implemented to ensure the reasonable and timely recovery of all South Coast College information, applications and systems, regardless of computing platform, should that information become corrupted, destroyed, or unavailable for a defined period.

Business impact analysis will be performed periodically to determine the criticality of South Coast College processes and establish a schedule for backup and recovery of those systems and data to ensure their timely recovery in the event of an extended outage. When performing a business impact analysis, the data stewards as charged by senior management, will:

Identify all key business processes and assess their criticality to the operation of South Coast College. The information owners (data trustees and stewards) will determine maximum acceptable time to recover each key business process in the event of a disruption;

For each critical process, an inventory will be developed of all of the assets required to perform the process or to resume the process in the event of a disaster. Considerations of assets will include but are not limited to staff, accommodations, communications, IT assets, networking and data;

Perform a threat analysis to determine the threats the organization and its data are subject to. These threats could include natural disasters or man- made events;

Perform a risk assessment to determine the likelihood that a threat would or could occur;

Develop and test plans to recover the assets within the time frame required to meet the requirements of the lines of business.

Policy and Standards Relationship

South Coast College will develop standards that support the implementation of this policy for systems and technologies being used within their domains. These security standards will be produced and implemented to ensure uniformity of information protection and security management across the different technologies deployed within South Coast College. The standards can be used as a basis for policy compliance measurement.

Part 5. Security Organization Policy

Chief Information Officer (CIO) is responsible for researching and managing information security issues. Chief Information Officer (CIO) reports to the President who is responsible for its organization and leadership.

The mission of the Chief Information Officer (CIO) is to:
Develop, deploy and maintain an information security architecture that will provide security policies, mechanisms, processes, standards and procedures that meet current and future business needs of South Coast College;
Provide information security consulting to South Coast College regarding security threats that could affect South Coast College computing and business operations and make recommendations to mitigate the risks associated with these threats; Assist senior management in the implementation of security measures that meet the business and academic needs of South Coast College;
Develop and implement security training and awareness programs that educate South Coast College students, employees, contractors and vendors with regard to South Coast College's information security requirements;
Investigate and report to senior management breaches of security controls, and implement additional compensatory measures when necessary to help ensure security safeguards are maintained;
Assist with the development, implementation and maintenance of disaster recovery processes and techniques to maintain South Coast College business continuity in the event of a disaster or extended period of computer resource unavailability.

Part 6. Asset Classification and Control Policy Information Management

Information, like other assets, must be properly managed from its creation, through authorized use, to proper disposal. As with other assets, not all information has the same use or value, and therefore information requires different levels of protection. Information will be classified based on the classification guidelines in the "Information Management and Security Procedural Document" according to its value, sensitivity, consequences of loss or compromise, and/or legal and retention requirements.
All information will have the information or data steward established within South Coast College's lines of business that will be responsible for assigning the initial information classification and make all decisions regarding controls, access privileges of users, and daily decisions regarding information management. Periodic high-level business impact analyses will be performed on the information to determine its relative value, risk of compromise, etc. Based on the results of the assessment, information will be classified into one of South Coast College's information classifications, where appropriate.
Each classification will have a set or range of controls, designed to provide the appropriate level of protection of the information and its associated application software commensurate with the value of the information in that classification.

Privacy and Handling of Private Information

Privacy of an individual's information must be respected throughout its lifetime.
South Coast College's systems hold personal identifiable information (i.e., any information that is unique to any individual) to carry out the business of South Coast College.

The protection of the privacy of personal information is of utmost importance and South Coast College must conduct business so as to protect the rights of privacy of all members of the public, business partners, and South Coast College community.
All South Coast College employees with access to personal information are required to respect the confidentiality of that personal information.
Personal data, including information about students, employees, members of the public, organizations and business partners, collected and maintained by South Coast College must:
Be used only for the stated purpose for which it was gathered;
Be gathered in lawful and fair circumstance;
Be kept for the amount of time required by law or regulations or as long as it remains relevant for its primary purpose;
Not be disclosed without specific consent or as authorized by law;
Be available for review by authorized individuals;
Be corrected if errors are known to exist or if the individual identifies errors;
Be erased where appropriate if the individual requests consistent with applicable laws; and
Be protected using system access controls, or be stored in a locked cabinet or office. (If this information is stored by a third-party, the third-party must contractually abide by these rules.)
Be destroyed in a manner consistent with that required by law or regulations.

Release of Private Information to Third Party Consultants
"Private information which is part of the "Internet Security and Privacy Act and considered "Highly Sensitive Information" by South Coast College definition must not be released as storable data to third party consultants without security procedures that demonstrate South Coast College's third party diligence in protecting the data and ensuring its proper distribution when no longer needed. "Private or highly sensitive information" shall mean personal information (e.g., information concerning an individual which, because of name, number, symbol, mark or other identifier, can be used to identify an individual) in combination with any one or more of the following data elements:
social security number;
driver's license number or non-driver identification card number;
account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.
It does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Campus procedures must include:
Data Trustee approval of the need for the release;
South Coast College approved mechanism for encrypting the data;
Approval by the third party for receiving the data;
Third party assurance of proper security for the stored data and its subsequent destruction;
Logging of the transfer to record the date, type of sensitive data, type of security, location of written approval, and parties to the transfer on both sides;

Recording of the third party's written statement of subsequent secure destruction of the data.

Protection of Third Party Information

Confidentiality of any third party confidential information must be respected throughout its lifetime.

South Coast College's systems hold confidential information from third party entities to carry out the business of the organization. The protection of the confidentiality of this information is of utmost importance and South Coast College conducts business so as to protect the rights of all partners including constituents, governments and vendors. All employees with access to such information are required to respect the confidentiality of that business information and not disclose the information to other third parties. Confidential information obtained from relationships with third parties must:

Be used only for the stated purpose it was gathered;

Be gathered in lawful and fair circumstance;

Be kept for the amount of time required by law or regulations or as long as it remains relevant for its primary purpose;

Not be disclosed without specific consent or as authorized by law;

Be available for review by authorized third parties;

Be corrected if errors are known to exist or if the third party identifies errors;

Be erased where appropriate if the third party requests consistent with applicable laws; and

Be protected using system access controls, or be stored in a locked cabinet or office. (If this information is stored by a third-party, the third-party must contractually abide by these rules.)

Be destroyed in a manner consistent with that required by law or regulations.

Part 7. Personnel Security Policy

The Human Resources Information Security Program is intended to reduce the risks of human error, theft or misuse of South Coast College information and facilities. Security responsibilities must be defined and addressed at the employee hiring stage, included in contracts with third parties, and monitored by the employee's direct supervisor during an individual's employment.

Including Security in Job Responsibilities

Security roles and responsibilities as defined in this must be documented where appropriate. They will include any general responsibilities for implementing or maintaining the security policy as well as any specific responsibilities for the protection of particular assets, or for the execution of specific security processes.

Personnel Screening

South Coast College will follow specific guidelines with regard to pre-employment screening. South Coast College may perform, or have performed, additional screening for sensitive positions. These additional checks could include but are not limited to the following:

Previous employment;

Criminal records as authorized by Federal and State laws;
A check (for completeness and accuracy) of the applicant's curriculum vitae;
Confirmation of claimed academic and professional qualifications;
Independent identity check (passport, visa or similar documents) consistent with Federal and State laws; and

Licensing requirements, etc.

User Training

CyberSecurity awareness training is developed, implemented, and maintained to address security education for South Coast College employees. The CyberSecurity awareness Training will review information security policy, threats and concerns, and the proper use of information processing facilities (e.g. logon procedures and use of software packages) to minimize possible security risks. The program will additionally include the procedure to follow to report incidents (security breach, threat, weakness or malfunction) that might have an impact on the security of South Coast College information.

Reporting Security Weaknesses

Users of South Coast College Information Technology resources will be required to note and report any observed or suspected security weaknesses or threats to Chief Information Officer (CIO). They must report these weaknesses as soon as possible. *Users must not attempt under any circumstances to prove a suspected weakness.* This is for their own protection, as testing weaknesses could be perceived as a potential misuse of the system.

Information Technologies established specifically to research Information Assurance as a legitimate academic pursuit are not restricted by this reporting policy.

Procedures must be established for reporting security software malfunctions. The following should be considered:
The symptoms of the problem and any messages appearing on the screen should be noted;
The computer must be isolated, if possible, and use of it stopped until the problem has been resolved;
The matter should be reported immediately to the Chief Information Officer (CIO), for appropriate investigation

Part 8. Physical and Environmental Security

Critical or sensitive South Coast College business information processing facilities are housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls to protect from unauthorized access, damage and interference. Physical security perimeters are established in South Coast College environments where servers are stored or operational in wiring closets for network and telephonic connections, where printers used for printing confidential or sensitive information, and any other location where critical or sensitive

South Coast College computer equipment may be in use or stored. The purpose of the security perimeter is to prevent unauthorized access to the computer resource, or to prevent theft of the resource.

The Chief Information Officer (CIO) will perform periodic threat and risk analysis to determine the extent of the perimeter vulnerabilities.

Clean Desk and Clear Screen

Sensitive information must be removed from view and physically secured when not in use. Measures must be taken to insure that such information cannot be read or copied by unauthorized persons. Physical security for the machine when unattended is one approach. The use of computer screen savers or similar technology is required to ensure that sensitive information is not displayed after a specified period of inactivity. When unattended or physically unsecured for more than a few minutes, all computers must be screen locked.

Part 9. Communications and Network Management

South Coast College network monitoring follows best practice to the extent appropriate resources are available for staffing and monitoring tools.

Third party connections to any portion of the South Coast College network could compromise the integrity and confidentiality of data on the South Coast College network. Third party network connections are only allowed with prior approval by the Network Security Administrator to ensure that security measures are in place to maintain the current level of security on South Coast College networks.

The South Coast College Computer and Network Usage policy can be obtained from Chief Information Officer (CIO) or by attending the CyberSecurity Awareness Training. The policy/training includes information on user responsibilities and policies on connecting computer systems to the South Coast College network and the temporary removal or blocking of vulnerable or compromised systems from the network.

Network Management

South Coast College implements a range of network controls to maintain security in its trusted, internal network, and to protect connected services and networks. The "network" includes any device that is attached via a wired or wireless connection with an IP (Internet Protocol) address.

Host Scanning

SCC reserves the right to scan any device attached to the South Coast College network on a periodic and tiered basis to ensure optimal configuration to protect against known vulnerabilities and to advise Data Trustees of unencrypted storage of highly sensitive and confidential data (e.g. SS#). For example, a system integrity check, using an appropriate tool, may be run as frequently as SCC's current standards recommend checking for system integrity. Sensitive or critical systems will be scanned as frequently as current standards recommend. Due to the complex nature of various vulnerabilities, central scanning will be used where possible, and a notification

mechanism developed to propagate vulnerability information to data trustees/owners and ITS staff for appropriate remediation.

Network Security Checking

Network vulnerability scans are conducted periodically on systems that are essential to supporting a process that is critical to South Coast College business and annually on all other systems. Appropriate tools to scan the network and to report vulnerabilities will be identified by Chief Information Officer (CIO) and will be updated periodically to ensure that recently discovered vulnerabilities are included in any scans.

The vulnerability scanning process is followed and tested at all times to minimize the possibility of disruption to South Coast College networks by such reviews. Reports of exposures to vulnerabilities will be forwarded to Chief Information Officer (CIO) for review.

The use of network vulnerability scanning tools by anyone other than, or authorized by, Chief Information Officer (CIO) and his IT team is prohibited. Researchers and students performing vulnerability testing as a function of their research or coursework must receive authorization from Chief Information Officer (CIO) and make arrangements to ensure that scans are limited to their own systems or systems that have been assigned to them. Any vulnerability scanning from the Internet must be conducted exclusively by appropriately authorized and trained organizations.

Penetration and Intrusion Testing

All production computing systems that provide college campus information to external parties, either directly or through another service that provides information externally (such as the World Wide Web), may be subjected to penetration analysis and testing. It may be necessary for another campus organization, a suitably qualified evaluation team or authorized third party to attempt a live test to validate potential vulnerabilities. Such analysis and testing will be used to determine if:

The application may be changed by anyone while in production;

An authorized user may access the application and cause it to perform unauthorized tasks;

An unauthorized user may access, destroy or change any data; or

An unauthorized user may access the application and cause it to take inappropriate action.

Only authorized administrators may perform penetration testing and the system owner or her/his designate must approve each test. Any other attempts to perform such tests or to determine how a system may change or behaves under abnormal circumstances, whether successful or not, will be deemed an unauthorized access attempt and will result in disciplinary or legal action.

Internet and Electronic Mail Acceptable Use

All uses of the South Coast College network and of South Coast College electronic mail facilities must be within the boundary of South Coast College's Computer and Network Authorization and Use of Computer and Network policy.

External Internet and VPN Connections

South Coast College acts as an Internet Service Provider for its faculty, staff and students in support of its teaching, research and service missions. This mission is best served by minimizing controls on network traffic while ensuring that the network facilities are not abused.

Virtual Private Network (VPN), wireless and open-port facilities attached to the college campus network must provide for authenticated access to insure proper use and the ability to attribute responsibility for actions. If a specific implementation does not allow for authentication, reasonable steps must be taken to ensure that access to the facility is controlled by other means. All other permanent connections intended to route traffic from the South Coast College network to other networks must be approved by Chief Information Officer (CIO) in order to insure that they:

Do not interfere with campus operations

Address appropriate security concerns

Insure proper use of South Coast College's resources.

Transmission of sensitive data over the Internet must be done in such a manner that the data is not compromised in regard to privacy or integrity. Encryption of such data is required. This can be accomplished by encrypting the data prior to transmission or by using VPN technology to encrypt the data flow over the network.

Connections to Third Party Networks

Any permanent connection intended to route traffic from the South Coast College private network to a third party private network must have a business case documented and approved by Chief Information Officer (CIO) or designee. A risk analysis may be performed to ensure that the connection to the third party network will not compromise South Coast College's network. Controls, such as the establishment of firewalls, may be implemented between the third party and South Coast College to protect South Coast College's trusted networks. These connections may be periodically reviewed or tested by Chief Information Officer (CIO) or her/his designee to ensure:

The business case for the connection is still valid and the connection is still required;

The security controls in place (filters, rules, access control lists, etc.) are current and functioning correctly.

This policy requires that connection to the South Coast College network be done in a secure manner to preserve the integrity of the South Coast College network, data transmitted over that network, and the availability of the network. The security requirements for each connection will be assessed individually, and be driven by the business needs of the parties involved. Only

authorized Information Security or IT network staff will be permitted to use “sniffers” or similar technology on the network to monitor operational data and security events.
Third parties requesting permanent access to the South Coast College network must be approved by Chief Information Officer (CIO) to have an internal network connection. A South Coast College non-disclosure/non-access agreement must be signed by an authorized South Coast College representative and a duly appointed representative from the third party organization who is legally authorized to sign such an agreement. This document, describing the business nature and network connection requirements, must be submitted to the South Coast College and Chief Information Officer (CIO). Chief Information Officer (CIO) or her/his designee has final approval authority. Failure to sign this document by either party will result in the connection being disapproved.
If a VPN connection is to be provided, refer to the section above, “External Internet and VPN Connections” for security requirements.

Security of Electronic Mail

Electronic mail is inherently not secure and should not be used to transmit highly sensitive/confidential information, due to the security risks which include but are not limited to:
Vulnerability of messages to unauthorized access or modification or denial of service;
Vulnerability to error, e.g. incorrect addressing or misdirection, and the general reliability and availability of the service;
Impact of a change of communication media on business processes, e.g. the effect of increased speed of dispatch or the effect of sending formal messages from person to person rather than company to company;
Legal considerations, such as the potential need for proof of origin, dispatch, delivery and acceptance;
Implications of publishing externally accessible staff lists;
Controlling remote user access to electronic mail accounts.

Messaging and Conferencing

When making use of commercial communications facilities or services, methods of authorization and encryption should be employed, when appropriate, to ensure that information is not disclosed to unauthorized individuals.

Portable Computing Devices and Information Media

Highly sensitive (confidential) data should never be in unencrypted format on portable computing devices and information media. Individuals requiring remote access to secure information should do so only via the VPN services provided by Chief Information Officer (CIO) or her/his designee with completion of VPN use agreement. Storage media used to backup and archive information must be secured to prevent compromise of confidentiality or integrity.
When using portable computing devices (e.g. laptops, smart phones) to access information special care must be taken to ensure that device and information accessed by that device is not compromised (i.e.: unauthorized persons viewing information on the screen).When accessing

databases containing confidential information the mobile device user must be careful to never save data to the local hard- drive or other mobile storage device.

Remote Access

Remote connection to South Coast College's networks is allowed only through a Virtual Private Network (VPN) maintained by Chief Information Officer (CIO) or her/his designee for administrative business use access when remote work-related business is an absolute necessity. The VPN application and terms of agreement require data trustee authorization and data owner agreement and understanding of their responsibility to:

protect College information by ensuring unauthorized users are not allowed access to South Coast College internal networks via the VPN;

Maintain system security patches and anti-virus definitions;

secure the equipment used to access South Coast College information resources;

ensure no unencrypted highly sensitive (confidential) information resides on the device.

Modem Usage

Connecting dial-up modems to workstations that are stand-alone or simultaneously connected to South Coast College's local area network or to another internal communication network is prohibited. This technology is no longer supported by South Coast College.

Monitoring

South Coast College complies fully with Federal and State law. The appropriate Federal/State Information Technology (IT) personnel may inspect, monitor or search South Coast College information systems to comply with subpoenas and search warrants issued by appropriate authorities. Network traffic may be monitored for indications of system compromise or attack.

Part 10. Operations Management

Responsibilities, processes and procedures should be established and documented for the management and operation of all information processing facilities. This includes the development of appropriate operating instructions and incident response procedures.

Operating procedures for all South Coast College administrative systems and applications should be documented and maintained.

Operating procedures should be treated as formal documents with changes authorized by the supervisor.

Documented procedures should also be prepared for housekeeping activities associated with information processing and communication facilities such as computer startup and shut down procedures, back-up, equipment maintenance, and computer room management and safety.

Operational Change Control

Changes to South Coast College administrative information processing facilities and systems must be authorized and controlled through a change management process with appropriate checks and balances. Formal management responsibilities and procedures ensure satisfactory control of all changes to equipment, software or procedural documentation. Operational software will be

subject to strict change control. When programs are changed, an audit log containing all the relevant information will be created and maintained. The change control process will consider the following activities:
Identification and recording of significant changes;
Assessment of the potential impact of the change;
Formal approval process for proposed changes;
Communication of changes to all affected people and organizations; and
Procedures identifying responsibilities for aborting and recovering from unsuccessful changes.
Incident Management Procedures
An incident management process will be established to track the types, volumes and costs of security incidents and malfunctions. This information will be used to identify recurring or high impact incidents and to record lessons learned. This may indicate the need for additional controls to limit the frequency, damage and cost of future incidents, or to be taken into account in the policy review process.

All users of South Coast College systems should be made aware of the procedure for reporting security breaches, threats, weaknesses, or malfunctions that may have an impact on the security of South Coast College information. All South Coast College staff and contractors are required to report any observed or suspected incidents to local management as quickly as possible.
Incident management responsibilities and procedures will be clearly defined and documented to ensure a quick, effective and orderly response to security incidents. These procedures will address incidents such as:
Information system failures and loss of service;
Denial of service;
Errors resulting from incomplete or inaccurate business data;
Breaches of confidentiality;
Loss of integrity of the software or other system component.
In addition to normal contingency plans designed to recover systems or services, the incident response procedures will also cover:
Analysis and identification of the cause of the incident;
Planning and implementation of corrective actions to prevent reoccurrence;
Collection of audit log information;
Communication with those affected by or involved in the recovery from the incident.
Chief Information Officer (CIO) or her/his designee will investigate significant security incidents and implement corrective actions to reduce the risk of reoccurrence.

Segregation of Duties
Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Separating the management or execution of certain duties or areas of responsibility, in order to reduce opportunities for unauthorized modification or misuse of information or services, should be implemented wherever possible, especially in support of the College administrative systems.

At times, you may find this method of control difficult to achieve, but the principle must be applied as far as possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision must be implemented. It is important that security audit remains independent.

Care must be taken that no single person can perpetrate fraud in areas of single responsibility without being detected. The initiation of an event must be separated from its authorization. The following controls must be considered:

It is important to segregate activities which require collusion in order to defraud, e.g. raising a purchase order and verifying that the goods have been received;

If there is a danger of collusion, then controls need to be devised so that two or more people need to be involved, thereby lowering the possibility of conspiracy.

Separation of Test and Operational Facilities

Where possible, separating development, test and operational facilities is important to achieve segregation of the roles involved. Rules for the transfer of software from development to operational status must be defined and documented.

Development and test activities can cause serious problems, e.g. unwanted modification of files or system environment, or of system failure. The level of separation that is necessary, between operational, test and development environments, to prevent operational problems must be considered to ensure adequate protection of the production environment. Where possible, a similar separation must also be implemented between development and test functions. In this case, there is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access.

Where development and test staff have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational data. On some systems this capability could be misused to commit fraud, or introduce untested or malicious code. Untested or malicious code can cause serious operational problems. Developers and testers also pose a threat to the confidentiality of operational information.

Development and testing activities may cause unintended changes to software and information if they share the same computing environment. Separating development, test and operational facilities is therefore required to reduce the risk of accidental change or unauthorized access to operational software and business data. The following controls must be considered:

Development and operational software must, where possible, run on different computer processors, or in different domains or directories;

Development and testing activities must be separated as far as possible;

Compilers, editors and other system utilities must not be accessible from operational systems when not required;

Different log-on procedures are recommended for operational and test systems, to reduce the risk of error. Users will be encouraged to use different passwords for these systems, and menus should display appropriate identification messages;

In situations where separate development and production support staff exist, development staff will only have access to operational passwords where controls are in place for issuing passwords

for the support of operational systems. Controls must ensure that such passwords are changed after use.

System Planning and Acceptance

Because system and data availability is a security concern, advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. Requirements for new systems must be established, documented and tested prior to their acceptance and use. Capacity demands should be monitored and projections of future capacity requirements made to ensure that adequate processing capability and storage are available. This information will be used to identify and avoid potential bottlenecks that might present a threat to system security or user services.

Acceptance criteria based on best practices for new information systems, upgrades and new versions of existing systems must be will ensure that the requirements and criteria for acceptance are clearly defined, agreed, documented and tested.

Protection Against Code

Software and associated controls will be implemented across all South Coast College systems to prevent and detect the introduction of malicious software. The introduction of malicious software such as a computer virus, network worm programs and Trojan Horses can cause serious damage to networks, workstations and business data. User education will outline the dangers of unauthorized or malicious software. The types of controls and frequency of updating signature files, etc., is dependent on the value and sensitivity of the information that could be potentially at risk. For most South Coast College workstations, and all systems or servers, virus signature files are updated at least daily.

Information Back-up

Back-ups of critical South Coast College data and software are performed regularly. A threat and risk assessment is performed at least annually to determine the criticality of business systems, and the time frame required for recovery. Processes will be developed to back-up the data and software. Restoration of data is tested periodically. Formal disaster recovery plans for each critical South Coast College application will be developed, documented and tested periodically. Test results will inform changes to disaster recovery plans.

Inventory Requirements

An inventory will be maintained of all IT hosts and servers, together with an assessment of the criticality of the services provided and the sensitivity of the information held on these systems.

System Security Checking

Systems and services that process or store non-public information or provide support for critical processes will undergo technical security reviews to ensure compliance with implementation standards and for vulnerabilities to subsequently discovered threats. Reviews of systems and services that are essential to supporting a critical South Coast College function must be

conducted at least once every year. Reviews of a representative sample of all other systems and services must be conducted at least once every 24 months.
Any deviations from expected or required results that are detected by the security status review process must be reported to Chief Information Officer (CIO) or her/his designee and an IT staff and corrected immediately. In addition, South Coast College application owners should be advised of the deviations and must initiate investigation of the deviations (including the review of system activity log records if necessary).

Disposal of Media

Media such as tapes, diskettes, servers, and PC hard drives which contain sensitive data must be electronically erasure of data before disposal. Sensitive information could be leaked to outside persons through careless disposal of media. Formal processes must be established to minimize this risk. Media containing sensitive South Coast College data must be destroyed by incineration, shredding, or electronic erasure of data before disposal consistent with record retention policy.

Part 11. Access Control Philosophy

The value of data as a College resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, or unnecessary restrictions to its access. Furthermore, increased data access and use improves data integrity because discrepancies are identified and errors are subsequently corrected. As an educational institution with a mission to disseminate knowledge, South Coast College values ease of access to information, including administrative data. Permission to view or query data contained in the COLLEGE DATABASE should be granted to all Data Users for all legitimate business purposes. Update access should be restricted as necessary, but granted to College employees at the location where data are initially received or originate whenever this is feasible. Information specifically protected by law or regulation must be rigorously protected from inappropriate access. Examples include student grades or personnel evaluations that are identifiable with a specific person. To preserve the qualities of integrity, confidentiality and availability, South Coast College's information assets will be protected by logical and physical access control mechanisms commensurate with the value, sensitivity, consequences of loss or compromise, legal requirements and ease of recovery of these assets.

Data Categorization

As part of the data definition process, Data Stewards assign each data element and each data view in the COLLEGE DATABASE to one of three data access categories:
Non-sensitive (Public data)
Moderately sensitive (Internal Business use only data)
Highly sensitive (Confidential data)

Except as noted below, all data are designated as College-internal data for use within the College. Data users have access to these data by authorization of the Data Trustees and Stewards and by authentication for use in the conduct of College business. These data, while available within the

College, are not designated as open to the general public. Where appropriate, Data Stewards may identify elements or views of the COLLEGE DATABASE that have no access restriction whatsoever.

Designated Non-sensitive Public data may be released to the general public. Where necessary, Data Stewards may specify some data elements as limited-access.

Designated Highly sensitive confidential data includes those data for which Data Users must obtain individual authorization prior to access, or to which only on need based, access may be granted. When data are designated as highly sensitive, the Data Steward should provide the following to the ITS Database Administration (DBA) unit:

Specific reference to the legal, ethical, or externally imposed constraint which requires the restriction.

Description of Data User categories that are typically given access to the data, under what conditions, or with what limitations.

Documentation of the process for approving and implementing access.

Documentation of the process for maintaining security controls.

Note that a data view can possibly have more open access than that of the underlying data elements that comprise it. For example, removal of person-identifying data elements from a view may result in a view that contains some otherwise-restricted data elements but that the Data Steward may now designate as public or College-internal. The appropriate Data Steward in collaboration with ITS is responsible for determining and documenting data access procedures that are unique to a specific information resource, view, or set of data elements.

Data Access Control

Data Trustees and Stewards are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges will be (read, update, etc.).

Any Data User may request that a Data Steward review the restrictions placed on a data element or data view, or review a decision to deny access to limited-access data. The appropriate Data Trustee makes the final determination about restrictions and access rights for enterprise data.

Data Stewards and the ITS DBAs share security administration responsibilities (i.e., the functions of specifying, implementing, and managing system and data access control). To the extent possible, the Data Stewards work together and with the DBAs to define a single set of College procedures for requesting and authorizing access to limited-access data elements in the COLLEGE DATABASE. Data Stewards and DBAs are jointly responsible for documenting these access request and authorization procedures. Data Stewards, with the assistance of ITS, are responsible for monitoring and annually reviewing security implementation and authorized access. All Data Users who are cleared for the highly sensitive category of COLLEGE DATABASE data must acknowledge (by signed statement or other documented means) that they understand the level of access provided and accept responsibility to both protect their access privileges and to maintain the confidentiality of the data they access. Data Stewards are responsible for defining and implementing procedures to assure that data are backed up and recoverable in response to

events that could compromise data integrity. ITS or other College organizations may assist in this effort. Data Stewards may delegate specific security administration activities to operational staff. The Information Security Program Team is responsible for maintaining a plan for security policies and practices and for keeping abreast of security related issues internally within the College community and externally throughout the information technology marketplace.

College data may be stored on a variety of computing hardware platforms, and is considered part of the COLLEGE DATABASE. Every data storage platform must have a defined *System Administration* function with a designated system administrator whose responsibilities include:
Physical site security
Administration of security and authorization systems
Backup, recovery, and system restart procedures
Data archiving
Capacity planning
Performance monitoring

User Registration and Management
A process will be established to outline and identify all functions of user management, to include the generation, distribution, modification and deletion of user accounts for access to resources. The purpose of this process is to ensure that only authorized individuals or other entities have access to South Coast College applications and information and that these users only have access to the resources required for authorized purposes.
The User Management Process should include the following sub-processes:
Enrolling new users;
Removing user IDs;
Granting privileges to a user;
Removing privileges from a user;
Periodic reviewing of privileges of users;
Periodic reviewing of users enrolled to any system; and
Assigning a new authentication token (e.g. password reset processing).
The appropriate data trustee or steward or other authorized officer will make requests for the registration, granting, and revocation of access rights for all authorized users.
For applications that interact with individuals that are not employed, registered, or appointed by South Coast College, the information owner is responsible for ensuring an appropriate user management process is implemented where limitation of access is appropriate. Standards for the registration of such external users must be defined, to include the credentials that must be provided to prove the identity of the user requesting registration, validation of the request and the scope of access that may be provided.

Privilege Management
The issuance and use of privileged accounts will be restricted and controlled. Inappropriate use of system privileges is often found to be a major contributing factor to the failure of systems that

have been breached. Processes must be developed to ensure that use of privileged accounts is monitored, and any suspected misuse of these accounts is promptly investigated.

User Password Management

Passwords are a common means of authenticating a user's identity to access an information system or service. Password standards are implemented and communicated to ensure all authorized individuals accessing South Coast College resources follow proven password management practices. These password rules must be mandated by automated system controls whenever possible.

Network Access Control

Access to South Coast College's trusted internal network must require all authorized users to authenticate themselves through use of an assigned user ID and an authentication mechanism, e.g., password, token or smart card, and/or digital certificate.

User Authentication for External Connections (Remote Access Control)

Individual accountability is required and must be maintained when South Coast College's resources are being accessed remotely. Identification and authentication of the entity or person attempting access must be performed across an encrypted connection using such technology as HTTPS and/or a secure VPN tool. Users who need a password reset must be authenticated before the request is granted.

For a vendor to access South Coast College computers or software, individual accountability is also required. For those systems (hardware or software) for which there is a built-in user ID for the vendor to perform maintenance, the account must be disabled until vendor access is required. The activity performed while this vendor user ID is in use must be logged. When the vendor has completed their work, the vendor user ID should be disabled, or the password changed to prevent unauthorized use of this privileged account.

Authentication of a user can be accomplished using three techniques: by providing something only the user knows; by providing something the user has; or by identifying the user by a physical characteristic of the user. "Strong authentication," refers to the use of two out of three of these methods to authenticate a user (i.e. password or PIN plus a token card).

To maintain information security, South Coast College requires that individual accountability be maintained at all times, including during remote access where sensitive information is exchanged. For example, remote access to generally available web content on South Coast College servers does not necessarily require individual accountability. For the purposes of this policy, "remote access" is defined as any access coming into South Coast College's network from off South Coast College's private, trusted network. This includes, but is not limited to:

Connecting a third party network to the South Coast College network;

VPN access (refer to Part 9, Communications and Network Management, External Internet and VPN Connections).

Segregation of Networks

When the South Coast College network is connected to another network, or becomes a segment on a larger network, controls are in place to prevent users from other connected networks from unauthorized access to sensitive areas of South Coast College's private network. Routers or other technologies are implemented to control access to secured resources on the trusted South Coast College network.

Operating System Access Control

Access to operating system code, services and commands must be restricted to only those individuals who need access in the normal performance of their College roles. Where possible, individuals will have a unique user ID for their use so that activities can be traced to the responsible person. Where avoidable, user IDs should not give any indication of the user's privilege level, e.g., supervisor, manager, administrator.

In certain circumstances, where there is a clear business requirement or system limitation, the use of a shared user ID for a group of users or a specific job can be used. Approval by management should be documented in these cases. Additional compensatory controls must be implemented to ensure accountability is maintained.

Application Access Control

Access to South Coast College applications must be restricted to those individuals who have a business need to access those applications or systems in the performance of their job responsibilities. Access to source code for applications and systems must be restricted. This access should be further restricted so that authorized South Coast College staff and contractors can access only those applications and systems they directly support.

Monitoring System Access and Use

Sensitive systems and applications are monitored to detect deviation from the access control policy and record events to provide evidence and reconstruct lost or damaged data. Depending on the nature of the events continuous and/or periodic monitoring may be appropriate. Audit logs recording exceptions and other security-relevant events that represent security incidents/deviations from policy are produced and kept to assist in future investigations and access control monitoring. Audit logs will include where technically feasible:

User IDs;

Dates and times for logon and logoff;

Terminal identity or location if possible;

Records of rejected system access attempts; and

Records of rejected data and other resource access attempts.

Part 12. Systems Development and Maintenance

Software applications are developed or acquired to support South Coast College in achievement of its mission. These applications generally store, manipulate, retrieve and display information used to conduct South Coast College activities. South Coast College departments and students

become dependent on these applications, and it is essential the data processed by these applications be accurate, and readily available for authorized use. It is also critical that the software that performs these activities be protected from unauthorized access or tampering.

To ensure that appropriate security is built into all South Coast College information systems, all security requirements, including the need for rollback arrangements, must be identified during the requirements phase of a project and justified, agreed to and documented as part of the overall business case for a South Coast College information system.

Security requirements and controls must reflect the value of the information assets involved, and the potential damage that might result from a failure or absence of security measures. This is especially critical for Web and other online applications. The framework for analyzing the security requirements and identifying controls to meet them is associated with threat assessment and risk management which must be performed by the information owner and technical support staff.

A process must be established and implemented for critical applications to:

Understand the business risks and develop a profile of the data to help to understand the risks;

Select security measures based on the risk profile and protection requirements;

Select and implement specific controls based on security requirements and technical architecture;

Provide a method to test the effectiveness of the security controls;

Develop processes and standards to support changes, ongoing management and to measure compliance.

Controls in systems and applications can be placed in many places and serve a variety of purposes. The specific control mechanisms must be documented at the application level. At a minimum, the security measures that are implemented must be based on the threat and risk assessments of the information being processed.

Input Data Validation

Data input must be validated. Checks will be applied to the input of business transactions, static data (names, addresses, employee numbers, etc.) and parameter tables. Where feasible the applications should apply the controls as part of the system to ensure consistent, complete, and accurate implementation of the controls in the most efficient manner. The following controls must be considered:

Dual input or other input checks to detect the following errors:

Out-of-range values;

Invalid characters in data fields;

Missing or incomplete data;

Exceeding upper and lower data volume limits;

Unauthorized or inconsistent control data.

Validation of the input's compliance with South Coast College policy, procedures and business rules.

Periodic review of the content of key fields or data files to confirm their validity and integrity;

Inspecting hard-copy input documents for any unauthorized changes to input data (all changes to input documents should be authorized);
Procedures for responding to validation errors;
Procedures for testing the plausibility of the input data;
Defining the responsibilities of all personnel involved in the data input process.

Control of Internal Processing

Data that has been correctly entered can be corrupted by processing errors or through deliberate acts. Validation checks and business rules must be incorporated into systems and automated where possible. The design of applications must ensure that restrictions are implemented to minimize the risk of processing failures leading to a loss of data or system integrity. Specific areas to consider include:
The use and location in programs of add and delete functions to implement change to data;
The procedures to prevent programs running in the wrong order or running after failure of prior processing;
The use of correction programs to recover from failures to ensure the correct processing of data.
Use of automated checking on the database (triggers) to ensure key validation rules are applied at the database level.

Cryptographic Controls

Use of cryptography for protection of high-risk information must be considered when other controls do not provide adequate protection. Encryption is a technique that can be used to protect the confidentiality of information. It must be considered for the protection of sensitive or critical information. Based on a risk assessment, the required level of protection will be identified taking into account the type and quality of the encryption algorithm used and the length of cryptographic keys employed. To the extent possible, consideration must also be given to the regulations and national restrictions that may apply to the use of cryptographic techniques in different parts of the world. In addition, and to the extent possible, consideration must be given to controls that apply to the export and import of cryptographic technology.

Key Management

Protection of cryptographic keys is essential if cryptographic techniques are going to be used. A secured environment must be established to protect the cryptographic keys used to encrypt and decrypt information. Access to these keys must be tightly controlled to only those individuals who have a business need to access the keys. Loss of confidentiality of a cryptographic key would cause all information encrypted with that key to be considered compromised.
Protection of System Test Data
Test data must be protected and controlled. Live operational data must never be connected to a testing environment. Acceptance testing usually requires large volumes of test data that closely resembles operational data. The use of test data populated from operational databases

containing sensitive information requires that those performing the tests are authorized by the appropriate data custodians to access such information.

Change Control Procedures

To minimize the possibility of corruption of administrative information systems, strict controls over changes to information systems must be implemented. Formal change control procedures must be enforced. They must ensure that security and control procedures are not compromised, that support programmers are given access only to those parts of a system necessary to perform their jobs, and that formal agreement and approval processes for changes are implemented. These change control procedures will apply to South Coast College applications as well as systems software used to maintain operating systems, network software, hardware, etc.

In addition, access to source code libraries for both South Coast College applications and operating systems must be restricted to ensure that only authorized individuals have access to these libraries and where practical that access is logged to ensure all activity can be monitored.

Part 13. Business Continuity Planning

The scope of this policy is limited to the IT infrastructure, and the data and applications of the South Coast College environment. To ensure interruptions to normal South Coast College business operations are minimized, and critical College business applications and processes are protected from the effects of major failures or disasters, each South Coast College business unit, in cooperation with the South Coast College IT organization, must develop, implement and periodically test a local business continuity plan that can meet the recovery requirements of all critical business processes and applications. These interruptions could be caused by natural disasters, accidents, equipment failures, or deliberate actions.

The consequences of an extended interruption due to a disaster or security failure must be analyzed to determine the impact on South Coast College's business, and to determine the recovery time necessary to restore normal business operations. Business continuity management must include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

Business continuity management begins with a business impact analysis and a threat analysis that identifies events that could cause an interruption of business operations and processes. Following the threat identification, a risk assessment must be performed to determine the impact of the threat on the business, likelihood of occurrence, and recovery time necessary for essential South Coast College business applications and processes. This assessment will consider only those business processes that are information technology related. These activities must be performed with the full involvement of the owners of the business data and business processes.

A business continuity plan must be developed by each South Coast College business unit that addresses each of the following key elements:

Understanding the risks South Coast College is facing in terms of their likelihood and impact on the business, including identification and prioritization of business processes and supporting applications;

Understanding the impact the interruptions are likely to have on South Coast College, and establishing the business objectives of information processing facilities;
Formulating and documenting a business continuity strategy and plans that are consistent with South Coast College's business objectives and priorities;
Regular testing and updating of the business continuity plans and processes that have been put in place;
Ensuring that the management of business continuity is built into South Coast College's processes and structure. Responsibility for coordinating the business continuity management process should be assigned to appropriate individuals.
For all instances where South Coast College is reliant upon the services of a third party for providing information services, South Coast College will define the requirements for information availability and recovery. These requirements must be made part of the agreement with the party providing services.
Although information security roles and responsibilities may be outsourced to third parties, it is the overall responsibility of each South Coast College business unit to maintain control of the security of the information assets that it owns.
The disaster recovery requirements for the Information Technology (IT) components are based on the business impact analysis performed by South Coast College business units and academic departments.

Part 14. Compliance

To avoid breaches of any criminal and civil law, statutory or State regulatory or contractual obligations, and security requirements, the design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements. Advice on specific legal or South Coast College requirements will be provided by South Coast College Legal Counsel.

Intellectual Property Rights

Appropriate procedures must be implemented to ensure compliance with legal restrictions on the use of copyrighted material, or material that may have design rights or trademarks. Proprietary software products are generally supplied with license agreements that limit the use of the product to a specific machine or number of users. Controls must be implemented to ensure all aspects of license agreements are met and can be audited. Copyright infringement can lead to legal action which may involve criminal proceedings.
For software or other intellectual property that South Coast College may create that it wants to protect, security measures and copyright procedures must be implemented to protect the SCC's intellectual property from unauthorized access and/or use.

Safeguarding of South Coast College Records

South Coast College records must be protected from loss, destruction or unauthorized modification. Some records may need to be retained in a secure manner for extended periods to meet State and Federal legal retention requirements, as well as to support essential business

operations. Records and information must be categorized into record types, e.g., accounting records, database records, transaction logs, audit logs, and operational procedures, each with details of retention periods and types of storage media.

The *General Retention and Disposition for South Coast College Records* contains guidelines for complying with legal, fiscal, and administrative requirements for records retention and disposition.

Prevention of Misuse of Information Technology Resources

The information technology resources and the data processed by these resources are provided for South Coast College business purposes. Management should authorize their use. Any use of ITS facilities for non-business or unauthorized purposes, without management's consent, should be considered a misuse of South Coast College facilities. Controls must be implemented to detect and report such activity to Chief Information Officer (CIO).

Compliance with Security Policy

South Coast College supervisors will ensure that all security processes and procedures within their areas or responsibility are followed. In addition, all business units within South Coast College will be subject to regular reviews to ensure compliance with security policies and standards.

Part 15. References

Data Administration Guidelines for Institutional Data, Indiana College Administrative Data Access Policy, College of Virginia
Standards, Practices, and Procedures, College of Arizona
Data Administration Mission, College of Maryland
Data Classification Policy, Columbia College
Fredonia State University of New York
Zeguro Cybersecurity Compliance

Part 16. Employee Acknowledgement Form

EMPLOYEE ACKNOWLEDGEMENT FORM

I acknowledge that I have received, read, and understand the CyberSecurity policies outlined in the South Coast College (SCC) Employee CyberSecurity Policy Handbook. I agree to conform to the rules and regulations of South Coast College (SCC) as described in the handbook which is intended as a guide to network security policies and procedures. I understand that the College has the right to change the handbook without notice. It is also understood that future changes in policies and procedures will supersede or eliminate those found in this book, and that employees will be notified of such changes through normal communication channels.

I also understand and agree that the information contained in these materials does not constitute an employment contract between South Coast College of (SCC) and me, and that either I or South Coast College (SCC) may terminate our employment relationship at any time, with or without cause.

_____

Employee Signature

_____

Employee Name (please print)

_____

Date

_____

Human Resource Signature

Information Management & CyberSecurity Policy HANDBOOK