GOVERNING BOARD POLICY

Antelope Valley Air Quality Management District

Policy No: 04-02 Adopted: August 17, 2004
Effective Date: August 17, 2004

Last Review: February 17, 2015

SUBJECT: DISTRICT COUNSEL - ELECTRONIC COMMUNICATION, ELECTRONIC DOCUMENTS, ATTORNEY CLIENT PRIVILEGE, AND WORK PRODUCT PRIVILEGE.

POLICY:

Electronic Communication: It is the policy of the Governing Board of the Antelope Valley Air Quality Management District (District) to preserve the privilege of its electronic communication in the Office of District Counsel, including but not limited to its privilege of confidentiality where applicable, and prevent any inadvertent waiver regardless of the electronic medium of communication.

Electronic Document: It is the policy of the District to preserve the dignity of its electronic documents in the Office of District Counsel and to prevent any loss of dignity regardless of the electronic form of document or manner of storage.

Attorney Client Privilege: It is the policy of the District to preserve the confidentiality of the attorney client privilege and prevent any inadvertent waiver regardless of the electronic medium of communication.

Attorney Work Product Privilege: It is the policy of the District to preserve the confidentiality of the attorney work product and prevent any inadvertent waiver of the privilege regardless of the electronic form or storage of work product.

AMPLIFICATION OF POLICY:

Statement of Law: California Penal Code §502 provides, with very limited exceptions, that persons who knowingly and without permission tamper with, view or copy data from a computer, computer system or computer network is guilty of a public offense punishable as either a misdemeanor or a felony depending upon the circumstances. Penal Code §502 is attached hereto as Exhibit "A" and incorporated herein by reference with the intent that it shall be deemed to have been automatically amended to conform to California Penal Code §502 as hereafter amended.

"Electronic" is defined as having the meaning provided in California Civil Code § 1633.2 specifically, "related to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities." Civil Code §1633.2 is attached hereto as Exhibit "B"

and incorporated herein by reference with the intent that it shall be deemed to be automatically amended to conform to California Civil Code §1633.2 as hereafter amended.

Reasonable Precaution: In order to claim attorney client or attorney work product privilege in the event of inadvertent waiver, the District and the Office of District Counsel are required to take reasonable precautions to protect the security of electronic communication and electronic document produced by the Office of District Counsel.

Declarations: The District computer network is, and shall continue to be, set up in such a manner as to protect the Office of District Counsel from unauthorized access to its electronic communication and document from internal and external disclosure.

The Governing Board declares that employees are not acting within the course and scope of their employment with the District if and when any employees access the communication or document of the Office of District Counsel absent one or more of the following:

1. Action of the Governing Board;
2. Order of a Court of Competent Jurisdiction; or
3. Consent of the District Counsel

Any employee who knowingly and without permission accesses the electronic communication or document of the Office of District Counsel outside the course or scope of employment will be subject to disciplinary or other adverse action up to and including termination of employment. In addition, such a person can be independently prosecuted under California Penal Code §502 or other applicable statutes.

Notwithstanding the previous paragraphs, during the performance of their duties, network and computer operations personnel and system administrators need from time to time to observe certain transactional addressing information to ensure proper functioning of email services, and on these and other occasions may inadvertently see the contents of email messages. They are not permitted to see or read the contents intentionally; to read transactional information where not germane to the foregoing purpose; or disclose or otherwise use what they have seen. One exception is that of systems personnel (such as "postmasters") who may need to inspect email when re-routing or disposing of otherwise undeliverable email. This exception is limited to the least invasive level of inspection required to perform such duties. Furthermore, this exception does not exempt postmasters from the prohibition against disclosure of personal and confidential information, except insofar as such disclosure equates with good faith attempts to route the otherwise undeliverable email to the intended recipient. Re-routed mail normally should be accompanied by notification to the recipient that the email has been inspected for such purposes.

Attachments:

Exhibit A, Penal Code §502
Exhibit B, Civil Code §1633.2

Exhibit A

WEST'S ANNOTATED CALIFORNIA CODES
PENAL CODE
PART 1. OF CRIMES AND PUNISHMENTS
TITLE 13. OF CRIMES AGAINST PROPERTY
CHAPTER 5. LARCENY [THEFT]

§ 502. Unauthorized access to computers, computer systems and computer data

(a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.

(b) For the purposes of this section, the following terms have the following meanings:

(1) "Access" means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

(2) "Computer network" means any system that provides communications between one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities.

(3) "Computer program or software" means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

(4) "Computer services" includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network.

(5) "Computer system" means a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(6) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.

(7) "Supporting documentation" includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.

(8) "Injury" means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or the denial of access to legitimate users of a computer system, network, or program.

(9) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access.

(10) "Computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self- replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

(11) "Internet domain name" means a globally unique, hierarchical reference to an Internet host or service, assigned through centralized Internet naming authorities, comprising a series of character strings separated by periods, with the rightmost character string specifying the top of the hierarchy.

(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

(d)(1) Any person who violates any of the provisions of paragraph (1), (2), (4), or (5) of subdivision (c) is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(2) Any person who violates paragraph (3) of subdivision (c) is punishable as follows:

(A) For the first violation that does not result in injury, and where the value of the computer services used does not exceed four hundred dollars ($400), by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000) or in an injury, or if the value of the computer services used exceeds four hundred dollars ($400), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(3) Any person who violates paragraph (6) or (7) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars ($1, 000).

(B) For any violation that results in a victim expenditure in an amount not greater than five thousand dollars ($5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(C) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000), by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(4) Any person who violates paragraph (8) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, a misdemeanor punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in a county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.

(5) Any person who violates paragraph (9) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not one thousand dollars.

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(e)(1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor, pursuant to the provisions of Section 1714.1 of the Civil Code.

(2) In any action brought pursuant to this subdivision the court may award reasonable attorney's fees.

(3) A community college, state university, or academic institution accredited in this state is required to include computer-related crimes as a specific violation of college or university student conduct policies and regulations that may subject a student to disciplinary sanctions up to and including dismissal from the academic institution. This paragraph shall not apply to the University of California unless the Board of Regents adopts a resolution to that effect.

(4) In any action brought pursuant to this subdivision for a willful violation of the provisions of subdivision (c), where it is proved by clear and convincing evidence that a defendant has been guilty of oppression, fraud, or malice as defined in subdivision (c) of Section 3294 of the Civil Code, the court may additionally award punitive or exemplary damages.

(5) No action may be brought pursuant to this subdivision unless it is initiated within three years of the date of the act complained of, or the date of the discovery of the damage, whichever is later.

(f) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction, nor shall it make illegal any employee labor relations activities that are within the scope and protection of state or federal labor laws.

(g) Any computer, computer system, computer network, or any software or data, owned by the defendant, that is used during the commission of any public offense described in subdivision (c) or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of subdivision (c) shall be subject to forfeiture, as specified in Section 502.01.

(h)(1) Subdivision (c) does not apply to punish any acts which are committed by a person within the scope of his or her lawful employment. For purposes of this section, a person acts within the scope of his or her employment when he or she performs acts which are reasonably necessary to the performance of his or her work assignment.

(2) Paragraph (3) of subdivision (c) does not apply to penalize any acts committed by a person acting outside of his or her lawful employment, provided that the employee's activities do not cause an injury, as defined in paragraph (8) of subdivision (b), to the employer or another, or provided that the value of supplies or computer services, as defined in paragraph (4) of subdivision (b), which are used does not exceed an accumulated total of one hundred dollars ($100).

(i) No activity exempted from prosecution under paragraph (2) of subdivision (h) which incidentally violates paragraph (2), (4), or (7) of subdivision (c) shall be prosecuted under those paragraphs.

(j) For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

(k) In determining the terms and conditions applicable to a person convicted of a violation of this section the court shall consider the following:

(1) The court shall consider prohibitions on access to and use of computers.

(2) Except as otherwise required by law, the court shall consider alternate sentencing, including community service, if the defendant shows remorse and recognition of the wrongdoing, and an inclination not to repeat the offense.

CREDIT(S)

(Added by Stats.1987, c. 1499, § 3. Amended by Stats.1989, c. 1076, § 1; Stats.1989, c. 1110, § 1; Stats.1989, c. 1357, § 1.3; Stats.1998, c. 863 (A.B.1629), § 3; Stats.1999, c. 254 (A.B.451), § 3; Stats.2000, c. 634 (A.B.2232), § 1; Stats.2000, c. 635 (A.B.2727), § 2.)

Current through Chs. 1 to 10 & Res. Ch. 1 of 2004 Reg.Sess., Ch. 1 (end) of 3rd Ex.Sess., Chs. 1 & 2 (Prop. 57) & Res. Ch. 1 (Prop 58) of 5th Ex.Sess., & Props. 55 & 56

Exhibit B

WEST'S ANNOTATED CALIFORNIA CODES
CIVIL CODE
DIVISION 3. OBLIGATIONS
PART 2. CONTRACT
TITLE 2.5. ELECTRONIC TRANSACTIONS

§ 1633.2. Definitions

In this title the following terms have the following definitions:

(a) "Agreement" means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations, and procedures given the effect of agreements under laws otherwise applicable to a particular transaction.

(b) "Automated transaction" means a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction.

(c) "Computer program" means a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result.

(d) "Contract" means the total legal obligation resulting from the parties' agreement as affected by this title and other applicable law.

(e) "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(f) "Electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review by an individual.

(g) "Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means.

(h) "Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record.

(i) "Governmental agency" means an executive, legislative, or judicial agency, department, board, commission, authority, institution, or instrumentality of the federal government or of a state or of a county, municipality, or other political subdivision of a state.

(j) "Information" means data, text, images, sounds, codes, computer programs, software, data bases, or the like.

(k) "Information processing system" means an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information.

(l) "Person" means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity.

(m) "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(n) "Security procedure" means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

(o) "Transaction" means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

CREDIT(S)

(Added by Stats.1999, c. 428 (S.B.820), § 1.)

Current through Chs. 1 to 10 & Res. Ch. 1 of 2004 Reg.Sess., Ch. 1 (end) of 3rd Ex.Sess., Chs. 1 & 2 (Prop. 57) & Res. Ch. 1 (Prop 58) of 5th Ex.Sess., & Props. 55 & 56