Reference: *15 US Code Sections 6801 et seq.;*
17 US Code Sections 101 et seq.
Penal Code Section 502, California Constitution, Article 1 Section 1;
Government Code Section 3543.1(b);
16 Code of Federal Regulations Parts 314.1 et seq.;
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45
California Community Colleges Information Security Standard

The District computer and network systems are the sole property of the West Hills Community College District. They may not be used by any person without the proper authorization of the District. The computer and network systems are for District instructional and work related purposes only.

This procedure applies to all District students, faculty, and staff and to others granted use of District information resources. This procedure refers to all District information resources whether individually controlled or shared, stand-alone, or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the District. This includes personal computers, workstations, mainframes, minicomputers and associated peripherals, software and information resources, regardless of whether used for administration, research, teaching, or other purposes.

Conditions of Use

Individual units within the District may define additional conditions of use for information resources under their control. These statements must be consistent with this overall procedure but may provide additional detail, guidelines and/or restrictions. Access to District services is a privilege that may be wholly or partially restricted by the District without prior notice and without the consent of the user.

All suspected violations of the Computer and Network Use Policy by any District student shall be reported to the appropriate District or college administrator in keeping with legal obligation and Board policies.

All suspected violations of the Computer and Network Use Policy by any District employee shall be reported to the employee's supervisor in keeping with legal obligation and Board policies.

Legal Process

This procedure exists within the framework of the Board Policy and state and federal laws. A user of District information resources who is found to have violated any of these policies will be subject to disciplinary action up to and including, but not limited to, loss

of information resources privileges; disciplinary suspension or termination from employment or expulsion; and/or civil or criminal legal action.

Copyrights and Licenses

Computer users must respect copyrights and licenses to software and other online information.

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

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

- Copyrights – In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is prohibited in the same way that plagiarism of any other protected work is prohibited.

Integrity of Information Resources

Computer users must respect the integrity of computer-based information resources.

- Modification, Relocation, or Removal of Equipment – Computer users must not attempt to modify, relocate, or remove computer equipment, software, or peripherals that are owned by others without proper authorization.

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

- Unauthorized Programs – Computer users must not intentionally develop or use programs which disrupt other computer users or which access private or restricted portions of the system, or which damage the software or hardware components of the system. Computer users must ensure that they do not use programs or utilities that interfere with other computer users or that modify

normally protected or restricted portions of the system or user accounts. The use of any unauthorized or destructive program will result in disciplinary action as provided in this procedure, and may further lead to civil or criminal legal proceedings.

- Unauthorized Access – Computer users must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access. Contact Information Technology Services immediately upon suspicion or discovery of any security issue.

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

- Reporting Problems – Any defects discovered in system accounting or system security must be reported promptly to the appropriate system administrator so that steps can be taken to investigate and solve the problem. Additionally, any physical damage to assets and equipment must be promptly reported to the Information Technology department.

- Password Protection – A computer user who has been authorized to use a password protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the system administrator.

- Usage – Computer users must respect the rights of other computer users. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of district procedure and may violate applicable law.

- Two-Factor Authentication – All student and employee accounts are required to enroll in Two-Factor Authentication, and it will be enabled on all systems where it is technically feasible.

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

- Commercial Usage – Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations, or promotions (see Commercial Use, below). Some public discussion groups (Associated Student Body and related college clubs) have been designated for selling items and electronic communication may be used appropriately, according to the stated purpose of the group.

- Information Belonging to Others – Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users, without the permission of those other users and the system administrator.

- Rights of Individuals – Users must not release any individual's (student or employee) personal information to anyone without proper authorization.

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

- Political, Personal and Commercial Use – The District is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property and similar matters.

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

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

    - Commercial Use – District information resources should not be used for commercial purposes. Users also are reminded that the ".cc" and ".edu" domains on the Internet have rules restricting or prohibiting commercial use, and users may not conduct activities not appropriate within those domains.

Information Security Standards

The District collects, processes, and manipulates large amounts of data about students, its employees, and others. The District is committed to ensuring the highest level of privacy and security for these data sets in accordance with state and federal law and industry best practices. Local security procedures meet or exceed the standards established by the current California Community College Information Security Standard. All data sets are classified by security level and the appropriate security protocols are applied. Employees charged with managing data sets of any level of confidentiality shall adhere to District information security procedures and complete regular training in said procedures.

Storage of Protected Data

Protected data is defined as non-public data that is intended for internal use or is confidential. Unauthorized disclosure of protected data may violate regulations or standards such as PCI (Payment Card Industry), FERPA (Family Educational Rights and Privacy Act), or contractual agreements with third parties or service providers.

Protected data may exist in applications, databases, or files. Various access controls protect data when in its original location, but when copied, reproduced, or transmitted, the original protections are lost. However, the classification and level of protection for a data element must travel with it regardless of its location or format.

Storing protected data on personal devices, or various types of external storage may expose sensitive or confidential data to unauthorized disclosure and is prohibited. If sharing, transporting, or storing protected data must be facilitated, users must work with District IT to ensure the data is secure and meets regulatory compliance.

If protected data is copied from its original location (e.g., to other files, removable devices, or on backup media) it must be encrypted. If sent via e-mail or other transmission means on public networks, it must be encrypted.

Nondiscrimination

All users have the right to be free from any conduct connected with the use of the West Hills Community College District network and computer resources which discriminates against any person on the basis of national origin, religion, age, gender, gender identity, gender expression, race or ethnicity, color, medical condition, genetic information, ancestry, sexual orientation, marital status, physical or mental disability, pregnancy, or military and veteran status, or because a person is perceived to have one or more of the foregoing characteristics, or based on association with a person or group with one or more of these actual or perceived characteristics. No user shall use the District network and computer resources to transmit any message, create any communication of any kind, or store information which violates any District procedure regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

Disclosure

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

- Possibility of Disclosure – Users must be aware of the possibility of unintended disclosure of communications.

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

- Public Records – The California Public Records Act (Government Code Sections 6250 et seq.) includes computer transmissions in the definition of “public record” and nonexempt communications made on the District network or computers must be disclosed if requested by a member of the public.

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

Disclaimer

The District is not responsible for loss of information from computing misuse or malfunction. It cannot be guaranteed that copies of critical data will be retained for all systems.

The District cannot guarantee that users will not receive electronic communications they may find offensive, nor can the district guarantee the authenticity of electronic communications received, or that electronic communications received were in fact sent by the alleged sender. Users are solely responsible for materials they access and disseminate on the district computer and network system.

Dissemination and User Acknowledgment

All users shall have access to this procedure and be directed to familiarize themselves with it.

A “pop-up” screen shall appear prior to logging on to WHCCD computers and web-based single-sign on, which requires acknowledgement that the user has read and understands Board Policy and Administrative Procedure 3720, Computer and Network Use, and will comply with it.

Title IV Information Security Compliance

The District maintains an information security program that meets the following requirements in compliance with the Gramm-Leach-Bliley Act (GLBA). As part of this program, the District:

- Designates the Chief Technology Officer (CTO) to oversee the information security program.
- Performs assessments of information security to address the following items, at a minimum:
    - Employee training and management
    - Information systems, including network and software design, as well as information processing, storage, transmission, and disposal
    - Detecting, preventing, and responding to attacks, intrusions, or other systems failures
- Designs and implements information safeguards to control the risks the District identifies through risk assessments, and regularly tests or otherwise monitors the effectiveness of the safeguards' key controls, systems, and procedures.
- Oversees 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.

    - Requiring the District's service providers by contract to implement and maintain such safeguards.
- Evaluates and adjusts the information security program in light of:
    - The results of the testing and monitoring
    - Any material changes to the District's operations or business arrangements
    - Any other circumstances that may have a material impact on the District's information security program.

Board approval date: 4/22/08
Reviewed/Revised: 7/23/19; 4/18/23