Treasure Valley Community College

Code: IIBGA
Adopted: 10/20/98
Readopted: 10/14/09; 2/15/11; 6/15/21
Orig. Code: BP 401-5; AR 300-13; IIBGA/EGAD

Acceptable Use of IT Resources

Purpose:

TVCC provides many technology products and services to support the academic and administrative needs of the College. Individuals who use the College's IT resources are expected to follow certain defined behaviors in order to minimize information security risk and protect the College and its constituents.

Protecting students, faculty, and staff from the risk of identity theft or unauthorized disclosure of personal information is the primary goal of adopting the best practices described in this policy.

In addition, this policy seeks to ensure that, in using College IT resources individuals:

1. Respect the rights of all TVCC students, faculty, and staff.

2. Ensure that TVCC technology services are available when needed.

3. Protect TVCC from harm that may result in misuse.

As a public institution, the College has a legal obligation to comply with federal and state regulations that dictate the acceptable use of our IT resources, as well as to demonstrate appropriate due diligence to our accrediting body.

Accordingly, this policy supports the following goals:

1. Ensure the integrity, reliability, availability, and optimal performance of IT resources.

2. Minimize the risk of data breach and cybercrime.

3. Ensure that use of IT resources is consistent with the principles and values that govern the use of other College facilities and services.

4. Prevent unauthorized disclosure of controlled sensitive data.

5. Prevent disruption of the learning experience.

6. Ensure the College is protected from financial, legal, regulatory, and reputational harm.

7. Ensure that IT resources are used for their intended purpose.

Scope Statement

All Treasure Valley Community College (TVCC) employees, students, and affiliates or other third parties that create, use, maintain, or handle TVCC IT resources are subject to this policy. This policy applies to use of all TVCC owned and managed IT resources, use of any computer or mobile device connected to a TVCC network, all controlled sensitive data stored or transmitted using TVCC IT resources and all users of such data.

Policy Summary

TVCC technology resources shall be used to support the academic and administrative needs of the College in accordance with information security industry and TVCC Information Security Department best practices.

Policy and Acceptable Use

1. Users may use only the computers, computer accounts, and computer files for which you have authorization.

2. Users may not use another individual's account or attempt to capture or guess other users' passwords.

3. Users are individually responsible for appropriate use of your computer, account and all resources assigned to you.

4. Users college is bound by its contractual and license agreements respecting certain third party resources; you are expected to comply with all such agreements when using such resources.

5. Users should make a diligent effort to protect your passwords and to secure resources against unauthorized use or access.

6. Users must not attempt to access restricted portions of the network, individual computers, or attempt to monitor network traffic without approval of Computer Services.

7. Users must not develop or use programs, software, or processes that disrupt other computer or network users, or that damage or degrade performance, software, or hardware components of a system.

Unacceptable Use

The following information is provided for additional clarification of the Acceptable Use Policy, but should not be interpreted as an exhaustive list of prohibited uses:

1. Users may not use the campus computing or network services to transmit or display information which:

    a. Violates or infringes on the rights of another person, including the right of privacy.
    b. Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material.
    c. Violates TVCC policy prohibiting sexual harassment.
    d. Restricts or inhibits other users from using the system or the efficiency of the computer systems.
    e. Uses the system for any illegal purpose.

2. Users may not illegally share or obtain copyrighted material.

3. Users may not use computing and network services for uses that are inconsistent, incompatible, or in conflict with state or federal law or TVCC policy.

4. Users must respect the privacy of other users, including others digital property.

5. Users may not share their password with others or let others use their account.

6. Users must respect the intellectual property of others and adhere to College standards of academic honesty.

7. Users must not intentionally disrupt the campus computing system or obstruct the work of other users such as by interfering with the accounts of others, introducing or spreading viruses or other destructive programs on computers or the network, sending chain letters or blanket e-mail messages, or knowingly consuming inordinately large amounts of system resources.

Exemptions

1. Faculty and staff are permitted incidental personal use of IT resources, provided that such use does not violate other policies.

2. Students may use IT resources for unrestricted personal use, provided such use does not violate other policies.

3. Programmatic evaluation of connected devices is for security purposes only in order to protect against potential threats such devices may introduce into the TVCC network.

   NOTE: TVCC will not (and cannot) scan, or otherwise inspect user data, user-installed programs, user activity, or any other personal/user information on personal devices connected to the TVCC network.

   Example 1: A faculty member connects to the TVCC wireless network and sends an email using their personal email account. This is not discoverable by TVCC IT.

   Example 2: A student connects their smart phone to the TVCC wireless network and performs a banking transaction. This is not discoverable by TVCC IT.

   Example 3: TVCC is required to perform eDiscovery for a legal matter. Data stored on personal devices connected to the TVCC wireless network (e.g.: personal laptops, smart phones, etc.) or data stored in third party sites (e.g.: Dropbox) are not discoverable by TVCC IT.

Exceptions

Exceptions to this policy must be pre-approved in writing by the Chief Information Officer (CIO)

Policy Violation

1. Violation of this policy may result in disciplinary action in accordance with TVCC Human Resources and/or Student Conduct guidelines.

2. TVCC reserves the right to report security violations or compromises to the appropriate authorities. This may include reporting violations of Federal, State, and local laws and regulations governing computer and network use, or required accreditation reporting.

3. Anyone who violates this policy may be held liable for damages to TVCC assets, including but not limited to the loss of information, computer software and hardware, lost revenue due to disruption of normal business activities or system down time, and fines and judgments imposed as a direct result of the violation.

4. TVCC reserves the right to deactivate any User's access rights (whether or not the User is suspected of any violation of this policy) when necessary to preserve the integrity of IT Resources.

Complaint Procedures

Report non-security-related violations (such as receipt of inappropriate content, other Human Resource policy violations, general college policy violations, or regulatory compliance violations) to a supervisor, HR, or the IT Department.

Report information security and general technical policy violations to Human Resources or the TVCC's Chief Information Officer.

Definitions

Affiliate: Any person or entity that has been sponsored by a TVCC manager to receive controlled temporary access to TVCC services. This is generally as a result of a contractual relationship with TVCC. For example, an air conditioning vendor may require affiliate access to test the HVAC system. A consultant project manager may require affiliate access to access project plans on a TVCC system.

Chief Information Officer (CIO): Senior manager of the Information Technology (IT) Department and a member of TVCC's Administrative Team.

Controlled Sensitive Data (CSD): A general categorization that is used in TVCC's Information Technology (IT) policies (primarily the Information Security Policy and the Acceptable Use Policy) to represent all confidential and private information governed by those policies. CSD includes: PII, PHI, HIPAA, FERPA, regulated, private, personal, or sensitive information for which TVCC is liable if publicly disclosed.

Cybercrime: Criminal activity or a crime that involves the Internet, a computer system, or computer technology.
Data Breach: Generally, an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. Note: Although "breach" is a commonly used term in the information security community, legally, the term "breach" tends to only be used when a security event reaches the threshold of regulatory reporting. TVCC will use the terms "incident" or "compromise" until it can be determined whether an event satisfies the legal definition of a breach.

Hardware: The collection of physical components that constitute a computer system (a desktop computer, a server in a datacenter, a network switch, a printer, etc.)

IT Resource: (At TVCC) All Information Technology (IT) resources that are the property of TVCC and include, but are not limited to, all network-related systems; business applications; network and application accounts; administrative, academic and library computing facilities; college-wide data, video and voice networks; electronic mail; video and web conferencing systems; access to the Internet; voicemail, fax machines and photocopiers; classroom audio/video; computer equipment; software and operating systems; storage media; Intranet, VPN, and FTP.

IT Resources include resources administered by IT, as well as those administered by individual departments, college laboratories, and other college-based entities.

Network: (In IT) The technology that carries messages between one computer and another.

A network is a primary component of technology infrastructure and consists of hardware (e.g. routers, switches) that control and direct traffic; transport technologies (e.g. cables, fiber, wireless radio waves) that transport messages from Point A to Point B; and standards (e.g. Internet Protocol, Ethernet) that facilitate a common understanding of the messages being sent and how they are to be processed.

End points (or nodes) on a network are the senders and receivers of the messages and are usually computers (e.g. servers, desktops, laptops) – but can also be technology such as machine controllers, audio/visual devices, etc.

The Internet of Things (IoT) largely replaces people interacting across a network with machines and other technology devices interacting across a network, often using artificial intelligence (AI).

Software: A set of instructions that tells a computer what to do.

Computer software is generally constructed as programs (applications) written in a specific language designed to run on computer hardware. Most common softwares are applications for business and personal use. More specialized computer software runs the operating systems of computers, operates machinery, creates artificial intelligence in robots, controls scientific instruments, etc.

Third Party: (In Information Technology [IT]) A vendor. Can be applied to any vendor ("third party provider"), but mostly used regarding "vendor software" to distinguish it from software developed "in house."

User: Any person who makes any use of any TVCC IT resource from any location (whether authorized or not).

END OF POLICY

Legal Reference(s):

ORS 167.060 - 167.100
ORS Chapter 192
ORS 260.432
ORS 339.250
ORS 339.270
ORS 341.290
OAR 581-021-0050
OAR 581-021-0055
OAR 584-020-0040
OAR 584-020-0041

Children's Internet Protection Act, 47 U.S.C.§§ 254 (h) and (l) (2018); 47 C.F.R. Section 54.520 (2019).
Copyrights, 17, U.S.C. §§ 101-1332 (2018); 19 C.F.R. Part 133 (2020).
Every Student Succeeds Act, 20 U.S.C. 20 U.S.C. § 7131 (2018).
Americans with Disabilities Act of 1990, 42 U.S.C. §§ 12101-12213 (2018); 29 C.F.R. Part 1630 (2020); 28 C.F.R. Part 35 (2020).
Americans with Disabilities Act Amendments Act of 2008, 42 U.S.C. §§ 12101-12133 (2018).Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2018); 34 C.F.R. Part 99 (2020).
Safe and Drug-Free Schools and Communities Act, 20 U.S.C. §§ 7101-7117 (2018).

Cross Reference(s):

GBN/JBA - Sexual Harassment and Sexual Violence
GBNAA/JFCFA - Cyberbullying

JFCFA/GBNAA - Cyberbullying
JHFE - Reporting of Suspected Abuse of a Child JFCFA/GBNAA - Cyberbullying
JHFE - Reporting of Suspected Abuse of a Child