

6.04 ACCEPTABLE USE OF YVC NETWORK AND DATA MANAGEMENT SYSTEMS

Approved by Administrative Council on August 8, 2006

Yakima Valley College (YVC) owns the YVC network systems and applications. This procedure is intended to provide YVC network users with guidelines for responsible and appropriate utilization of this resource. This procedure supplements the [YVC Administrative Procedure 6.02 Acceptable Use of Technology Resources](#); all of its tenets, and any other applicable YVC policies, procedures, and/or standards that apply to the use of the assets defined in this procedure as well. YVC reserves the right to determine at any time what constitutes appropriate use of the YVC network and any computing access and services provided by YVC. This procedure also complies with the Washington State Department of Information Services (DIS) IT Security Audit Process.

Applicability

This procedure applies to all YVC employees, students and non-employees who may be authorized to use the YVC network as defined by this procedure. They shall be notified in writing of these procedures before being granted permission to access this resource. No part of this document supersedes [YVC Administrative Procedure 6.02 Acceptable Use of Technology Resources](#). This document shall also apply to the use of all technology resources at YVC facilities as defined by policy, procedure, and/or as defined by state or federal law. Its principles extend to and include any use or attempted use of the YVC network, regardless of point of origin. YVC users shall also apply this procedure when using the YVC network to navigate thorough networks beyond the local systems.

Use of the YVC Network and Data Management Systems

Use of the YVC network and data management systems shall be for the purpose of facilitating the exchange and storage of information, including information on students and/or employees, and compliance with, and furtherance of, the education, and administrative missions of the college. The use of the YVC network and data management systems will be consistent with the purposes and objectives of YVC, the community and Technical College system (see [Washington State Executive Order 91-10, Sec. III \[A\]](#)) and [RCW 42.52](#)).

Goals

The goals of this procedure are to:

1. Help assure the integrity and reliability of the YVC internal networks, hosts on those networks, the YVC databases, legacy systems, web-accessible resources, and any computing resource connected to them.
2. Ensure the security and privacy of YVC computer systems, networks and data.
3. Ensure the protection and retention of sensitive college data.
4. Establish appropriate guidelines for the use of the YVC network and YVC-owned data, whether accessed on or off-campus.

Permission

It is not the intent of this document to limit academic freedom, but to provide an appropriate framework for proper exercise of those freedoms. Furthermore, it is not the intent of this document to impinge on the intellectual property rights of authorized users.

YVC employees, students and non-employees who are authorized to use the YVC network may:

1. Use YVC-owned networks, computers, programs and data to which each individual has authorized access;
2. Use YVC provided networking, including access to the internet;
3. Use these computing and networking facilities and resources in a manner that is consistent with the mission and educational purpose of YVC.

Prohibitions

Utilizing the YVC network and data management systems for uses and/or communications that are specifically proscribed in the [YVC Administrative Procedure 6.02 Acceptable Use of Technology Resources](#) or which violate any other YVC policy, procedure, standard, and/or State and Federal rule or law is strictly prohibited.

Specifically prohibited uses of the YVC network and data management systems include:

1. Subverting, attempting to subvert, or assisting others to subvert or breach the security of any YVC data, network, or technology resource, or to facilitate unauthorized access;
2. Use of any YVC network and data management systems to create, disseminate or execute self-replicating or destructive programs (e.g., viruses, worms, Trojan horses);
3. Participating in activities involving disclosure or masquerading;
4. Viewing, copying, altering or destroying data, software, documentation or data communications belonging to YVC or to another individual without permission;
5. Individuals allowing another individual (whether they might otherwise be authorized to use the YVC network and data management systems or not) to use their login account password.
6. Accessing data for any purpose other than to perform the official duties of a YVC position.
7. Unauthorized disclosure of information to a third party.
8. Bypassing the YVC data management systems "time-out" feature, unless specifically authorized by the Director of Technology Services.

Personal Use

YVC allows de minimus personal use of the YVC network by employees consistent with [WAC 292-110-010 \(3\)](#) and [WAC 292-110-010 \(6\)](#), unless such use is specifically prohibited by this procedure. This personal use is defined in the [YVC Administrative Procedure 6.02 Acceptable Use of Technology Resources](#).

RESPONSIBILITIES

All users of the YVC network and data management systems have a responsibility to comply with this procedure and to understand their responsibilities and all expectations as spelled out in the [YVC Administrative Procedure 6.02 Acceptable Use of Technology Resources](#). This includes the requirement for confidentiality, retention, and access to public records detailed there.

Yakima Valley College and its representatives also have responsibilities under this policy. These include the responsibilities for logging and monitoring, for the monitoring of data management systems and for the monitoring of electronic messaging systems as enumerated in the [YVC Administrative Procedure 6.02 Acceptable Use of Technology Resources](#).

Additional specific responsibilities include:

Policy Maintenance

1. Technology Services (TS)

The primary responsibility for maintenance and administration of this procedure rests with the Director of Technology Services. TS is responsible for drafting any updates and changes to this procedure. After appropriate campus review and final approval by the college president. TS will announce the new or revised procedure to the campus providing a brief description of the procedure and its implications for employees and other affected individuals or groups.

2. Human Resources (HR)

The Director of Human Resources is responsible for reviewing any updates and changes to this procedure in light of current policies and procedures, providing input on the procedure and its implications for employees and other affected individuals or groups.

Procedures

Network Use

This procedure applies to all YVC employees, students and non-employees who may be authorized to use the YVC network and who wish to have an account created to access this resource. In the event of changes to YVC policies, standards, or procedures, the Director of Technology Services may require YVC account holders to periodically submit an updated Network Account and E-mail Request Form (see Appendix A).

1. Employee and Non-Employee Permission for Network Use

- a. Before using the YVC network, employees or authorized non-employees must formally request permission for a login/e-mail/voice mail account. This request must be approved by the administrator to whom the individual reports. This is accomplished by completing and signing a YVC [Network/Email/Phone Request Form](#) (see Appendix A), providing the applicable information.
- b. After the requestor agrees by signature to the goals and requirements of this policy, the form must be routed to Technology Services (TS) for processing by the TS staff authorized to create and maintain accounts on the YVC network.
- c. Once the account has been created by TS, the individual will be notified of their login name and password.
- d. The completed YVC [Network/Email/Phone Request Form](#) (see Appendix A) will be maintained on file in a secure location in TS. When requesting initial creation of accounts, both forms may be submitted simultaneously to TS by individuals and/or departments.

2. Student Permission for Network Use

- a. Student accounts will not have sufficient privileges to access the

YVC_NT administrative networking domain or administrative computers. Because of this, a formal written request and approval process for creating student accounts is not required.

- b. The method for creation of student user login/e-mail accounts for use on the YVC LABS network will be at the discretion of the YVC Network Administrator, with the approval of the Director of Technology Services. Accounts may be requested by students and processed strictly by electronic means, if feasible.
- c. However, students are expected to abide by all expectations, responsibilities and guidelines of this procedure, any other applicable YVC policies, procedures, and standards as well as applicable State and Federal laws and rules. Because of this, a student account may not be created on the YVC LABS network until the YVC Network Administrator has ensured that the student has read and agreed with this procedure.
- d. This may be done with the use of a web form requiring electronic acknowledgement by the student when requesting an account (using the information contained in the YVC Acceptable Use Agreement Form). Login banners that must be acknowledged before use of YVC LABS network or computing resources, containing the same textual information, may also be used.
- e. Technology Services will also maintain an electronically accessible copy of this procedure and any related procedures and standards on the YVC support web.

Data Management Systems Use

These procedures apply to all YVC employees, students and non-employees who may be authorized to use the YVC Data Management Systems. Compliance with this procedure will assure the integrity and reliability of these resources.

1. Employee and Non-Employee Permission for Data Management System Use

- a. Before using a YVC data management system, employees or authorized non-employees must formally request permission for a user log on account. The administrator to whom the individual reports must approve this request. For access to student information, the supervisor must complete and submit electronically a Student Database Access Request Form (see the YVC IT Security Standard on Student Database Access Requests), providing the requested access. This form must be routed to the Family Education Rights and Privacy Act (FERPA) Officer for processing. The FERPA Officer will route the form to the appropriate TS staff authorized to create and maintain accounts on the administrative network.
- b. Once the account has been created by TS, the individual will be emailed their login instructions, user ID and generic password. The user is to immediately change the generic password. The completed Student Database Access Request Form will be maintained on file in a secure location in TS. When requesting changes to created accounts, supervisors may email the FERPA Officer the user ID and changes/additions requested.

Third-Party Access to Electronic Messages

Requests for third-party access to stored electronic messages will be handled

through the college's public record procedure (see also [YVC Administrative Procedure 2.08 Public Records Request](#)). YVC may be required to provide third parties with access in order to honor valid legal discovery and public records requests. Both the sender and the recipient will be provided notice of such requests prior to disclosure to the extent deemed feasible by college administrators, depending on the specific circumstance.

Right to Access

Given sufficient cause, the Director of Human Resources, or his/her authorized designee, has the right to obtain access to materials stored on the YVC network which are under the control of YVC employees in their administrative units or work areas when such access is necessary to conduct YVC business. The Director, or his/her designee, will identify the specific materials required and the employee will be given sufficient opportunity to provide YVC with the requested materials. In the case of an emergency, best efforts will be made to contact the employee prior to accessing the specific materials required.

Any individual's network use privileges may be suspended immediately upon the discovery of a possible violation of this procedure. Such suspected violations will be confidentially reported to the appropriate supervisors and/or administrators.

Sanctions

Violation of any of the provisions of this procedure will be dealt with in the same manner as violations of other college policies, procedures or standards, and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available, including:

1. Disciplinary action – Any disciplinary action will be taken in accordance with appropriate Human Resources procedures; and/or applicable collective bargaining agreements
2. Dismissal from the college; and/or
3. Referral to the Washington State Ethics Board; and/or
4. Legal action.

Some violations of this procedure may also constitute a state, local or federal criminal offense.

Definitions

All terms defined in the [YVC Administrative Procedure 6.02 Acceptable Use of Technology Resources](#) are applicable in this procedure. In addition, the following are defined:

Authorized User

This includes all YVC employees, students and non-employees who may be authorized to use the YVC network

YVC Data Management Systems

This includes the Student Management System (SMS), Personnel and Payroll Management System (PPMS) Finance Management System (FMS) Financial Aid (FAID), Facility Management (FM1), Scheduling (R25) and individual databases created by individual departments or the college.

YVC Network

This includes the YVC_NT and YVCLABS local area networks (LAN), the wide area networks (WAN) supporting sites separated from the main YVC campus, internet connectivity, networked infrastructure devices such as hubs, switches and servers, CTC-Net, and all other computers, networks and electronic messaging systems operated for the benefit of YVC employees and students.

De Minimis

The use of state resources is considered de minimis if:

1. The actual expenditure of state funds is so small as to be insignificant or negligible.
2. Any such use of the resource is brief in duration.
3. Occurs infrequently.
4. Is the most effective use of time or resources?
5. If the use does not disrupt or distract from the conduct of state business due to volume or frequency.
6. The use does not disrupt other state employees and does not obligate them to make a personal use of state resources.
7. The use does not compromise the security or integrity of state property, information, or software.

Disclosure

This occurs when an unauthorized user gains access to information. Disclosure often occurs when messages are forwarded to unauthorized users.

Masquerading

This is when a user presents him/herself to the system as another user. This may be done in order to gain unauthorized access to information or resources, to disseminate (mis)information in another's name, or to block or deny a system from operating correctly.

Unauthorized Access

Includes gaining access to accounts, resources, messages, or files to which one is not granted privilege by the owner or sender.

RELEVANT LAWS AND OTHER RESOURCES

Revised Code of Washington <http://apps.leg.wa.gov/rcw/>

Washington Administrative Code <http://apps.leg.wa.gov/wac/>

Washington State DIS IT Security Policy <http://isb.wa.gov/policies/security.aspx>

Washington State DIS IT Security Audit Standards <http://isb.wa.gov/policies/security.aspx>

Washington State Ethics Board <http://www1.leg.wa.gov/LEB/>

APPENDICES

Appendix A (Network/Email/Phone Request Form)

Revision Log

Date	By	Notes

Procedure Contact: Director of Technology Services

YVC Network/Email/Phone Request Form

(YVC Admin Procedure 6.04 Acceptable Use of YVC Network & Data Management Systems - Appendix A)

STEP 1: NEW USER *This section is to be read and signed by the individual for whom the account is being created.*

Access to the YVC network and related internet services, electronic mail, and telephone/voicemail is requested. This is for a user who is one of the following: **Please ✓ one box.**

- | | | |
|---|---------------------------------------|--|
| <input type="checkbox"/> Administrator/Exempt | <input type="checkbox"/> Faculty (FT) | <input type="checkbox"/> PT Hourly Staff |
| <input type="checkbox"/> Classified Staff | <input type="checkbox"/> Faculty (PT) | <input type="checkbox"/> Other (specify) : |

Hiring Job Position/Title: _____

I have been given access to a copy of the following YVC Policies and Procedures by my supervisor or my administrator:

Employees can access these policies and procedures at <https://myyvc.net> under Policies & Procedures.

- | | |
|---|---|
| 6.00 Information Technology Security Policy | 6.04 Acceptable Use of YVC Network and Data Management System |
| 6.01 Information Technology Procedure | 6.05 Electronic Messaging and Retention |
| 6.02 Acceptable Use of Technology Resources | 6.06 Software Licensing Compliance |
| 6.03 Acceptable Use of YVC Computers | 6.09 Network Web Space Usage |

I have read and understand these policies and procedures, including my responsibilities and all processes identified in them, and agree to abide by their provisions. I also understand that I am required to protect the confidentiality of college data in accordance with the Family Education Rights and Privacy Act (FERPA), the Washington State Ethics Law (RCW 42.17), and YVC policies and procedures.

Name: PRINT clearly _____ Department: _____
 Home Email Address: PRINT clearly _____ Contact Number: _____
 Signature: _____ Date: _____

STEP 2: SUPERVISOR OR DEAN *To be completed by the SUPERVISOR detailing the privileges for the new user.*

Please ✓ the type of account (permanent or temporary) and then ✓ all boxes that apply for the new user; incomplete forms will result in account creation delays.

- | | | | |
|---|--|---|------------------------|
| <input type="checkbox"/> Permanent Account | or | <input type="checkbox"/> Temporary Account | Expiration date: _____ |
| <input type="checkbox"/> Network Log-In | <input type="checkbox"/> Access to server folders | List folders: _____ | |
| <input type="checkbox"/> Email account | <input type="checkbox"/> Access to email distribution groups | List groups: _____ | |
| <input type="checkbox"/> Telephone extension | <input type="checkbox"/> Voicemail account | Comments: _____ | |
| <input type="checkbox"/> CIS account | <input type="checkbox"/> FAID <input type="checkbox"/> FMS <input type="checkbox"/> SMS <input type="checkbox"/> PPMS <input type="checkbox"/> FAM | <input type="checkbox"/> ByRequest | _____ |
| <input type="checkbox"/> Website support access | <input type="checkbox"/> Approver <input type="checkbox"/> Contributor | Website requested: _____ | |
| <input type="checkbox"/> SSL VPN Remote access | Computer name: _____ | Server folder: _____ | |

Room/Office Location: _____ Other: _____

Please note that all account creation "communication" will be directed to the supervisor. The supervisor will be responsible for distributing the information to the new account holder.

Supervisor or Dean Name: PRINT clearly _____ Telephone: _____
 Signature: _____ Date: _____

STEP 3: ADMINISTRATOR-DIRECTOR OF TECHNOLOGY SERVICES *Required for YVC Resource Access.*

Director of Tech. Services: PRINT clearly _____ Telephone: _____
 Signature: _____ Date: _____

STEP 4: HELPDESK *Send the COMPLETED form to YVC Helpdesk, Prior Hall, P151, (509) 574-4717.*