CHAPTER 10: INFORMATION SYSTEMS (1000)

CHAPTER 10: INFORMATION SYSTEMS (1000)

10.P.01 Information Technology Policy.

Lake Washington Institute of Technology (LWIT) provides and maintains, within available resources:

1. Access for its community to local, national, and international sources of information.

2. A comprehensive range of appropriate technologies to support the college's administrative functions, instruction, and learning.

College community members must use college information systems resources in line with these policies and procedures and with related state policies, rules, and regulations of the:

1. Information Services Board (ISB).

2. Executive Ethics Board.

3. State Board for Community and Technical Colleges (SBCTC).

The president or designee will ensure that these policies, rules, regulations, and procedures followed and enforced.

10.P.03 Definitions.

A reasonable list of definitions of selected policy and procedure terminology will help college community members understand IT policies and procedures.

1. Computing and communications systems: computing, networking, teleconferencing, and voice phone systems for instructional and administrative functions.

2. Computing and communications facilities: the computers and computing software, terminals, printers, network and telecommunications equipment, modems, phones, fax devices and related equipment, as well as data files or documents managed or maintained by authorized college employees and that reside on disk, tape, or other electronic or magnetic media.

3. Computing and communications users: anyone, authorized or not, who uses a computing and communications facility from any location, whether using a college or a personal ID. For example, this definition includes people who:
   A. Access these facilities by an electronic network, such as email.
   B. Work with computing devices in classrooms, labs, offices or any other college location.
   C. Use an electronic network to connect a personal computing device to any other system, service, or location.

4. The "college's information": any information within the college's purview, including information it may not own but which is governed by laws and regulations to which the college is held accountable. It includes all:
   A. Student data.
   B. Personnel data.
   C. College financial data.
   D. Departmental administrative data.
   E. Alumni and donor data.
   F. Other data that relates to or supports the administration of the college.

This data may include facts, records, reports, planning assumptions, or any information meant only for internal use.

10.P.05. Acceptable Use**.**
The college is a leader in the use of information technology (IT) for teaching, learning, and higher education administration. To maintain that position, the college expects regular and proficient use of IT and further encourages individual and group innovation and experimentation. The college supports easy access to IT, technology choices, and academic freedom. Acceptable use includes compliance with all laws, regulations, licenses, contracts, security standards and procedure protocols, and use that does not impede or deny IT access to others.

1. Information technology (IT) includes all college owned, leased, or controlled hardware and software, devices and peripherals, networks, cabling, software, applications ("apps"), domain names, subscriptions, and bandwidth.

2. People may only use college IT for teaching, learning, and to conduct college business.

3. Personal use of IT by employees is limited to "de minimus" use as defined by the state of Washington.

4. Certain IT assets are designated as public use, including the "LWIT" wireless network and computers designated by the library, and are available for personal use but not for commercial or illegal purposes.

5. Students may use IT designated as public use in addition to those attached to the courses in which they are registered, departments to which they belong, and other technology related to their status or group membership in the college.

6. The public may use IT assets designated as public use and also use those designated for conference services ("ConfServ" network) if they participate in a sponsored activity on campus. Commercial activity is only permitted by clients of conference services who use designated IT assets.

7. College departments, programs, and service areas can create and enforce local acceptable use rules for IT assets under their control, as long as they do not conflict with college or state policies.

8. All users must comply with IT security requirements, standards, and operational protocols. Key among these is use of individual security credentials and following all laws, regulations, licenses, and contracts, and use that does not impede or deny IT access to others.

9. College administration can monitor and review the use of IT to ensure appropriate use. Users who violate the acceptable use policy and procedures are subject to discipline and penalties that may result in losing access privileges, as well as other penalties related to the inappropriate use. Unlawful

acts that involve IT may also subject violators to penalties by the Washington State Executive Ethics Board or prosecution by local, state, or federal authorities.

10.P.07 Responsibilities of Information Technology Services.
Information technology services will:
1. Provide support for IT resources, including technical support for its campus network, workstations, systems, and approved software.
2. Provide investment plans and budgets for future technologies.
3. Create and maintain procedures, forms, and standards to develop, manage, and protect the college's electronic resources and systems.

10.P.09 Training for Information Technology.
LWIT will provide, as resources allow, training for students and employees as needed to provide for the efficient, effective use of IT resources.

10.P.11 Information Technology Security.
The college will assign staff to manage a security program with security controls over IT resources that is proportionate with the level of risk. IT services will follow the ISB IT security policy and standards. The college will comply with ISB audit and review requirements and submit the signed security compliance memo.

10.P.13 Privacy.
Employees have no personal privacy rights in any file, message, or communication they place, send, or receive using college computing or communications systems. Employees must:
1. Guard information that is protected from disclosure by law.

2. Follow federal regulations and state laws related to protected information.

College records, stored electronically or in another format, may be subject to disclosure under:
1. State and federal public records laws.

2. Per a subpoena, discovery request, or court order as a result of criminal or civil legal actions.

10.P.15 User Identification.
The college must adequately protect against unauthorized modification, disclosure, or destruction of information handled by college computer and communications systems. The college maintains effective controls for access to minimize inadvertent user error and negligence and reduce potential systems misuse. Each user of a college automated system must have a unique personal identifier for user identification. The college will authenticate the user's ID before the computer or communications system grants access to electronic information. The college will end access for user IDs not in use.

10.P.17 Password Security.
Passwords authenticate a user's identity and create accountability while protecting vital assets. IT services creates and maintains a system of procedures to assign, authenticate, revise, and protect the secrecy of user passwords in line with applicable SBCTC and ISB policies, standards and procedures. IT

services will inform employees and students of these procedures and will use diligence in following them.

10.P.19 Electronic Messaging.
Employees must follow the governor's executive order EO 91-10 on electronic messaging systems and related state statute when using electronic messaging such as email and fax. Violating the electronic messaging policy can result in losing access or disciplinary actions. Employees have no personal privacy rights in any electronic message they create on, receive by, or send from the college's electronic messaging systems.

Employees must follow the state public records law to determine archival, record retention and disposition requirements. Electronic records an employee retains are subject to the state's public records law.

10.P.21 Internet Use.
Employees cannot use the internet for non-college business except for minimal (de minimis) use as given in the college's acceptable use policy.

10.P.23 College Website.
The college maintains a set of websites. All content of the websites must follow copyright and trademark rules and meet the same guidelines for quality and accuracy as other college publications. The college can disable and/or remove, after appropriate review and warning, website links and publishing capability on college-managed servers (or internet accessibility to such by college-supplied network components) of anyone who uses the internet to violate college policy or state and federal laws.

10.P.25 Software Copyright.
No college community member may engage in any activity that violates these copyright laws:
1. Intellectual property rights.

2. The terms of software license agreements.

3. Other college policies on computer and communications systems software.

10.P.27 Software Site License and Volume Purchases.
Employees must ensure they acquire software and hardware using site licenses and volume purchases the college establishes to most efficiently use college resources.

10.P.29 Computer Lab, Classroom, and Other Instructional Facilities Access and Use.
Employees and students must follow all college policies, state, and federal laws when using all college computing resources.

10.P.31 Penalties for Policy Violations.
Violating applicable law or college policy may result in penalties including, but not limited to withdrawing use privileges. Additional penalties may also arise under local, state, or federal law and college policies.

CHAPTER 10: INFORMATION SYSTEMS (1000)

10.P.33 Computing and Communications Systems Management Responsibilities.
College department administrators are responsible to manage the use of computer and communications systems resources, including hardware, software, and data installed within their facilities. IT services :

1. Manages the college's networks, including the electronics, hardware, software, and the infrastructure (e.g., wiring closets, cabling).

2. Manages and maintains the computer and communications servers and infrastructure used for college-wide applications.

Each department administrator, with IT services, will develop a comprehensive computer and communications systems plan and business continuity plan that:

1. Supports, tests, and recovers computer and communications operations for the department's business functions.

2. Covers troubleshooting, maintaining, and replacing hardware and software needed to process the department's critical business functions, restoring data files, and inventory special supplies needed to process the applications.

When others in the department have custodial responsibilities for computer and communications devices delegated to them, the department administrators have responsibility to ensure employees and students understand the procedures to follow on protecting and using these college assets.

10.P.35 Security for the shared SBCTC Administrative Processors.
SBCTC-IT manages the college's administrative application systems processor. The "Shared Expectations for Operation Security" agreement between LWIT and SBCTC outlines roles and responsibilities.

10.P.37 Networked Server and User Data Backup.
IT Services will:

1. Perform regular back-ups of the college network servers that support college-wide applications.

2. Back up any data loaded and stored on the network servers so it is available to restore the next day.

3. Perform regular back-ups of the college's employee data stored on the campus network.

4. Conduct periodic tests of backup procedures.

10.P.39 Supported and Unsupported Hardware and Software.
IT services staff will:

1. Support hardware and software established as the college's standard.

2. Consider any hardware or software not designated as a college standard as unsupported.

If a college department determines it must have an unsupported computer and/or communications hardware and software, IT services will consider adding the new software to the standard hardware and/or software listing. IT services will create a procedure to amend the list of standard hardware and software and to accommodate unique installations designated as central to the college's operations.

CHAPTER 10: INFORMATION SYSTEMS (1000)

Resources:

1. Executive Order EO 91-10
   http://www.governor.wa.gov/execorders/eoarchive/eo91-10.htm
2. Office of Financial Management (State Administrative and Accounting Manual)
   http://www.ofm.wa.gov/policy/default.asp
3. Revised Code of Washington
   http://apps.leg.wa.gov/rcw/
4. Washington Administrative Code
   http://apps.leg.wa.gov/wac/

Chapter Reviewed and Revised: February 2009 through November 2010
Board of Trustees Adoption: April 2011
10.P.05 Revised May 5, 2014