NETWORK STANDARDS	
Policy Number: IT-130	**Responsible Department: Information Technology**
Effective Date: 12/01/2016	**Last Revision Date: 12/22/2016**

PURPOSE:

To provide the standards for the establishment of CWI's networking infrastructure.

SCOPE:

Applies to CWI's networking infrastructure in all buildings owned and/or operated by CWI, CWI's networking infrastructure that provides connectivity between all CWI buildings, and any vendors used in support of the infrastructure.

DEFINITIONS:

Data Center: The infrastructure provided by a third party to house mission critical applications and hardware. This infrastructure is for facilities leased by CWI and should always be in a facility or building not owned or operated by CWI. The Data Center provides high availability for power and carrier access to be able to provide redundant and highly available infrastructure for CWI's mission critical applications.

Independent Distribution Facility (IDF): The IDF is the Telco room in a building that contains the switching and cabling termination points for a LAN. There can be multiple IDF's in one building. A Data Center cannot reside in an IDF.

Information Technology (IT) Resources: An array of products and services that collect, transform, transmit, display, present, and otherwise make data into usable, meaningful and accessible information. IT Resources include but are not limited to: desktop computers, laptops, and tablet PC's; handheld devices including but not limited to, cell phones; e-mail, voicemail, servers, central computers, and networks; cloud storage systems; network access systems including wireless systems; portable hard drives and databases; computer software; printers and FAX machines and lines; campus, classroom and office audio and visual display devices and switching, camcorders, televisions, physical media; telephone equipment and switches including local and long-distance services; satellite equipment and any other current or future IT resource adopted by CWI as new technologies are developed.

Local Area Network (LAN): The infrastructure used to provide connectivity within a single building or portion of a building owned and/or operated by CWI. This can be physical infrastructure, such as cabling or switches, or can be a wireless network.

Main Distribution Facility (MDF): The MDF is the Telco room that houses the network core for a particular building and is the focal point for the WAN entering the building and the LAN servicing the building. The Data Center would be considered an MDF.

Telecommunications Rooms (Telco): The secure room that houses the electronics and network cabling for the LAN at each building. Telco rooms can be centrally located, or can be dispersed throughout a building depending on the layout of the building. Multiple floor buildings will typically have an MDF and several IDF rooms. The WAN connection for a building will be in the MDF. IDFs will typically only have switching and cabling for the LAN in a particular section of a building.

User: Anyone who uses CWI's IT Resources, even if they have no responsibility for managing the resources. This includes students, faculty, staff, contractors, consultants, and temporary employees.

Wide Area Network (WAN): The infrastructure used to provide connectivity between all of the buildings owned and operated by CWI. This can be a mix of several technologies and is usually provided by or leased from a third party or carrier.

POLICY

CWI supports centralized network services to offer the most advanced technology available while ensuring stable and reliable services are maintained for the benefit of the CWI community. These standards are subject to change based on newly available technology, changes in the makeup of the CWI footprint and any change in the direction of technology support.

GUIDELINES

I. The Information Technology Department (IT) is directly responsible for the network infrastructure
II. IT is responsible for every aspect of the networking infrastructure which includes:
    a. All cabling, copper and/or fiber, installed at the College
    b. All hardware installed in the data center(s), MDFs and IDFs
    c. Monitoring all data connections and hardware for possible trouble or failures
    d. Maintenance of all hardware installed
    e. Managing the budget used to operate the infrastructure
III. Redundancy
    a. Wherever possible and practical, the design of the network infrastructure will have redundancy in mind. Some examples of a redundant design are:
        i. Separate internet providers for the internet bandwidth at the Data Center
        ii. Multiple routers and switches in the core network at the Data Center
        iii. Multiple sources of power for the equipment at the Data Center
        iv. Uninterruptable Power Systems (UPS) at the MDFs and IDFs for each building
        v. Multiple connections between devices using technology such as line aggregation, port channeling, and VPC.
IV. Telecommunications Rooms
    a. IT exclusively manages CWI's Data Center(s), MDFs and IDFs in all buildings.
    Access to MDFs and IDFs is limited to IT staff only. Any exception to this must be coordinated with CWI's Chief Information Officer (CIO).
    b. MDFs and IDFs will not be used for any storage other than equipment used in the operation of the network infrastructure.
V. Best Practices

a. IT shall seek and adopt whenever possible best practices with regards to the acquisition, implementation, management and replacement of network infrastructure resources.
b. IT will review and adopt appropriate standards and procedures that represent best practices.

VI. Documentation
a. IT will maintain documentation of the network infrastructure data including:
    i. IP addressing
    ii. Network layout drawings
    iii. Software levels
    iv. Services provided
    v. Contact information
    vi. Backup schedule

VII. Availability
a. IT will strive to ensure that all network resources are available to CWI 24 hours a day, 7 days a week. This includes all internet connectivity and wireless, telephone and data access.
b. IT will monitor all aspects of the network so that a failure may be detected quickly.
c. In the event of a failure of any system, hardware, software or connectivity, IT will work to repair and restore service as quickly as possible.
d. IT will notify staff and management of any failure along with an estimated time for return of service.

VIII. Wireless Networks
a. IT will work with campus leadership to educate users on the shared responsibility of wireless access.
b. CWI provides wireless access to computing and IT resources for users as part of the services offered to enhance productivity in the workplace. Wireless networks operate within a shared and finite radio spectrum. IT will maintain administrative rights over this spectrum on campus and remote CWI buildings to ensure fair and efficient allocation of resources.
c. IT will manage the RF spectrum and reserve specific 20 MHz wide 5 GHz channels for use by non-IT departments and vendors. Departments and vendors shall only use the assigned channels.
d. The spectrum usage applies to all device traffic and interference occurring in the following frequencies ranges:
    i. 800 and 900 MHz, industrial, scientific, and medical (IS) bands, all modes
    ii. 2.21920-1930 MHz, all modes
    iii. 2.4-5 GHz, all modes
    iv. 4.9-6 GHz, all modes
e. IT will grant, limit, or restrict access to the wireless spectrum within the physical spaces and on grounds owned and operated by CWI.
f. IT will monitor the spectrum on a continuous basis, and may regulate all wireless activities at all institution sites, including remote offices and common areas.
g. Should any device create harmful interference, IT may request or cause immediate deactivation of the device until such time as it can be reactivated without causing harmful interference.
h. Access to wireless networks owned or operated by CWI imposes certain responsibilities and obligations and is granted subject to CWI polices, and local, state, and federal laws. Acceptable use of wireless networks includes, but is not limited to the following:
    i. Respecting system security mechanisms, and not taking measures designed to circumvent, ignore, or break these mechanisms;
    ii. Showing consideration for the consumption and utilization of IT resources; and
    iii. Assisting in the performance of remediation steps in the event of a detected vulnerability or compromise.

IX. Privacy Expectations

a. While CWI respects Users' rights to privacy, the institution cannot assure any level of privacy while using the CWI network infrastructure. Users are responsible for taking reasonable measures to ensure their own privacy on the wireless network.

b. IT Resources must be available to support CWI's mission. IT staff may need to inspect the resources to maintain or improve the function, if there is a suspicion of misconduct or if there may be a violation of federal, state, local law or evidence of violation of CWI policy.

c. Offenders may be prosecuted under all applicable laws including but not limited to the Communications Act of 1934 (as amended), the Family Educational Rights and Privacy Act of 1974, the Computer Fraud and Abuse Act of 1986, the Computer Virus Eradication Act of 1989, the Idaho Computer Crimes statute, and the Electronic Communications Privacy Act.

d. Individuals using wireless networks owned by CWI do so subject to applicable laws and CWI policies. Users assume all associated risks and agree to hold CWI and its employees harmless for: (1) the compromise of any personal information (e.g., credit card numbers); (2) any damage caused to Users' hardware or software due to security issues; or (3) any other harm caused by viruses or hacking while on CWI wireless networks.

e. CWI disclaims any responsibility and/or warranties for information and materials residing on non-CWI systems or available over publicly-accessible networks. Such materials do not necessarily reflect the attitudes, opinions, or values of CWI, its employees or students.