CASCADIA COMMUNITY COLLEGE

Administrative Procedures (AP)

Administrative Procedure: **Connecting Non-College Owned Technology to the College Infrastructure**	***Procedure Number:*** **AP1:4.10.21**
Board Policy	**Adopted by President's Cabinet 3/3/04**
Applicable WAC/RCW:	**Page 1 of 2**

Purpose
To maintain a technical environment which is secure, supportable, cost-effective and stable, only those technologies that have been tested and certified by the Information Technology staff may be connected to the college's infrastructure.

Technology Scope
These technologies include, but are not limited to the following categories: desktop hardware; portable computers; networked Personal Digital Assistants (PDAs) or handheld computers; wireless access points; and network bridging technologies. Technologies excluded from this administrative procedure include USB, parallel, serial, firewire, blue tooth and IR peripherals which are connected and supported solely by the user. These latter technologies are not directly supported by the IT team. Only technologies that have been evaluated, tested and deployed by the IT team have IT support on campus.

Process/Actions
Prior to connecting any foreign network-capable technology to the college network, the technology owner will need to schedule time to have the technology certified by a member of the college's Information Technology team. Students are referred to workers in the college's Open Learning Center which is located in room CC060. Employees should submit a Help Desk ticket for an analyst's review.

Students: The Open Learning Center employee will then perform a cursory inspection of the technology. They will be looking for updated anti-virus software and current operating system security patches.

If the Open Learning Center employee thinks the hardware meets the above criteria, the technology owner will be provided with a "Short Term Network Access Release" form to complete. The technology owner will then be directed to one of the system administrators for a higher level inspection. If the technology passes this inspection, a temporary network identity for the device will be created. The temporary

network identity will be active for the duration of the current academic quarter. Renewals are performed on a quarterly basis. If the technology fails the inspection, suggestions for remediation will be provided to the student. It is the owner's responsibility to bring their technology up to the college's standards.

Employees: Once the Help Desk ticket has been assigned, an analyst will make an appointment with the employee to certify the technology. The technology owner will complete a "Short Term Network Access Release" form. The analyst will check for current anti-virus coverage, operating system updates and patches as well as perform higher level inspection. If the technology passes the inspection, a temporary network identity for the device will be created. Given our architecture and limited network resources, the temporary network identity will be valid only in the home sub-net of that employee. Roaming outside of the sub-net is currently not feasible. If the technology fails the inspection, suggestions for remediation will be provided to the employee. It is the owner's responsibility to bring their technology up to the college's standards.

The completed "Short Term Network Access Release" forms are kept on file by the Open Learning Center (OLC). Hardwired network connectivity on campus is dependent upon the availability of an unused live network port. Existing computers, printers and other currently networked technologies can not be unplugged in order for non-college owned technologies to be connected to our network.

Students can access banks of available ports located on the north end of the Lower Level (LL) and First (1st) floors of the Cascadia building. These ports are available on a first come basis. Employee access to available ports within their sub-net must be preauthorized by their appropriate supervisor.