

Academic Network Policy

1.0 Purpose

The purpose of this policy is to define standards for creating and managing a BYU-Idaho academic network. These standards are designed to maximize teaching of network and computer technology and minimize the potential exposure of the campus network to damages which may result from the teaching environment. Damages include disruption of the campus network, introduction of viruses or worms, hacking of campus systems, inappropriate activity on the Internet, interference of address or air space, etc.

2.0 Scope

This policy applies to all BYU-Idaho employees, students, and guests with a BYU-Idaho-owned or personally-owned computer or device used to connect to a BYU-Idaho academic network.

3.0 Policy

3.1 General

1. A request for an academic network should be reviewed by Telecommunications and must be approved by the Computer & Technology Council (CTC) prior to implementation.
2. Approved academic networks will be created by Telecommunications as an interface off of a firewall, giving granular capability to define ingress and egress access rules.
3. The requesting department will be responsible for specifying access needs, management of systems and services, trouble-shooting problems, and disciplining those responsible for inappropriate activity related to the academic network.
4. Lines of communication between departments and Information Technology (IT) must remain open to facilitate awareness of changes, needs, and new thrusts and to keep each other informed, encourage synergy, and discourage interference.
5. In the event that either the academic or campus network is causing problems to one another, the link between the networks will be severed until the problem is resolved.
6. Academic networks are owned by BYU-Idaho, not any particular department or person. The same responsibility for acceptable use, living the honor code, obeying copyright laws, and etc. that is required on the campus network is also expected on academic network.

3.2 Requirements

1. One point of contact from the department and one from IT will be appointed. All requests related to an approved academic network shall be filtered through the points of contact.
2. Firewall rules must be requested through a "Firewall Exception Request" form and must be approved by the department and IT point of contacts.
3. Departments are responsible for the services they provide on the academic network. Care must be taken to ensure the services do not interfere with services on the campus network.
4. Changes in the use of the academic network or use of new technologies will be disclosed between point of contacts as a professional courtesy and to promote trust. For example, the addition of a wireless network would require care be taken to avoid interfere with other campus wireless networks as well as taking appropriate security precautions.
5. An academic network shall not attempt to become a domain name service (DNS) for "byui.edu," although they may become a sub-domain to "byui.edu." Any need to become a non-"byui.edu" domain shall be requested and approved through CTC.
6. Externally advertised domain names will be administered by Telecommunications. Such a request shall be made in writing from the department point of contact to the IT point of contact.
7. Academic networks will use the campus Internet for legitimate educational purposes and not frivolously, since the entire campus shares this limited and expensive resource.
8. Requests for access to the academic network from off campus must be approved by CTC.

4.0 Enforcement

Any employee or student found to have violated this policy may be subject to disciplinary action, up to and including separation from the university.

5.0 Related References

1. *Acceptable Use Policy*
2. *Honor Code*
3. *University Guidelines for Copying*
4. *Copyright Policy*
5. *Wireless Network Policy*

6.0 Definitions

<u>Term</u>	<u>Definition</u>
-------------	-------------------

Academic Network	A network managed by an academic department for the purpose of teaching network and computer technology. The academic network is subject to experimentation and could be up and down often. An academic network is a DMZ-like interface off of a firewall.
Campus Network	This is the network used by BYU-Idaho as a business tool to fulfill its mission. This network is not subject to experimentation and must stay up 24 hours a day, 7 days a week.
CTC	Computer Technology Council. This council is made up of representatives of each Vice President, is chaired by the Academic Vice President, and has extra representation from Information Technology.
DMZ	Demilitarization Zone. A DMZ is an interface in a firewall separate from the internal campus network. The DMZ is a network where servers are kept that are available to the world through the Internet. In theory, if a system in the DMZ is compromised, the campus network will not be in jeopardy.
DNS	Domain Name Service. Internet addresses, which are numbers, are translated into names, such as smith.byui.edu, by this service. The campus has an internal DNS that gives names to every network device. The campus external DNS advertises to the world only the names we wish them to know, such as www.byui.edu . Academic networks could have their own DNS servers in order to teach students what they are and how to create and manage them. Care has to be taken so academic DNS servers do not interfere with campus DNS servers.
Firewall	A firewall is a system which, for security reasons, separates and protects the campus network from the Internet. Typically, a firewall has an additional interface called a DMZ. At BYU-Idaho, an academic network is created by adding another DMZ-like interface to the firewall.

6.0 Revision History

Policy approved by President's Council on August 11, 2003.