

*Duke University Auxiliary Services*  
**POLICY STATEMENT**

*POLICY#: GENL-007.AUX    REVISION#:1    Date:12-12-2002    EFFECTIVE DATE: 1-7-2003*

**SUBJECT: Acceptable Computer Use Policy**

**OBJECTIVE**

*This policy deals with security, privacy and acceptable use issues associated with computers in Auxiliary Services. Special requirements for credit card processing systems are addressed in a separate document.*

**GUIDING PRINCIPLES**

The computers and computing infrastructure (“computers”) provided to Auxiliaries Services (AuxSvc) employees are for the purpose of supporting and executing the mission and individual tasks of AuxSvc and Duke University at large. Secondary to this function, AuxSvc computers offer opportunities for self-expression, improving skill levels and relaxation during break times. This secondary function of AuxSvc computers is not to interfere with their primary function.

Privacy of information stored on AuxSvc computers cannot be guaranteed although it will be supported whenever possible subject to the limitations described below. Protecting confidentiality of information required by legal statute, departmental regulation or ethical/social strictures is a primary factor in determining acceptable computer use policies.

**PERSONAL DATA PRIVACY**

Personal data stored on AuxSvc computers is generally secure if certain precautions are taken, however there is no absolute guarantee that any information stored on AuxSvc computers will be kept private, “for the owner’s eyes only.” AuxSvc management is committed to respecting the privacy of such information so long as (1) such information is not illegal, illegally obtained or of use in an illegal activity, (2) such information is in conformity with Duke University’s acceptable use policies for computers and (3) such information is neither important to the business of AuxSvc or to Duke University at large.

AuxSvc systems personnel may access information stored on AuxSvc computers as a result of (1) a subpoena or other legal instruments authorizing such access, (2) an explicit request from the Director of the department in question (or the Director’s explicit delegate), (3) certain systems procedures. The last conditions refer to such things as examining file backup logs to insure proper backup completion, migrating files for a user to a new computer, diagnosing system problems or recovering from such problems. AuxSvc systems personnel are prohibited from examining other employee’s personal data on AuxSvc computers without a legitimate systems-based need to do so.

**APPROVAL SIGNATURES:**

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

## **CONFIDENTIAL DATA PRIVACY**

AuxSvc personnel frequently handle data whose confidentiality is protected by legal, ethical/social strictures or AuxSvc regulations. Student data, for example, are protected by FERPA statutes (this includes student addresses, academic and financial records, etc.). Social security numbers, payroll information, credit card information and medical history information (including insurance claims) are all protected by one or more regulatory statutes. It is the responsibility of every AuxSvc employee to protect the confidentiality of data in their care and to be aware of possible confidentiality requirements. Specifically, AuxSvc personnel should not exchange data in their care except on a need to know basis and should consult their supervisors if there is any uncertainty regarding privacy requirements of their data. They must show due diligence by not carelessly exposing this data to theft or public exposure. Ensuring proper physical security to computers and data media as well as exercising care in distributing and securing reports containing confidential data are some of the primary duties of AuxSvc staff using computers.

## **SECURITY—PASSWORDS**

AuxSvc computer systems are networked and highly distributed which makes any action that compromises security very serious. Therefore all AuxSvc users must observe the following rules:

- Passwords are a key security component. Unless otherwise restricted by the particular computer system in question, all passwords are to be at least eight characters in length and must not match any word in the dictionary. Password characteristics, such as minimum password length, will be set by the computer system in question where possible. In addition, passwords are not to be constructed from any easily guessed pattern, such as 12345678, aaaaaaaa, etc.
- Where possible, passwords will be set to expire every 90 days.
- Where possible, passwords will have to meet complexity requirements by employing both upper and lower case characters, numbers and punctuation symbols.
- Password reuse will be limited by denying reuse of the last five passwords, where possible.
- Passwords will not be shared nor will they be written down or displayed in any manner that allows other individuals to find or see them.
- As a security measure, AuxSvc system personnel will attempt to crack passwords (where possible) as a method for insuring their quality. Any staff member repeatedly found creating bad passwords, as described above, will be subject to disciplinary action.

## **SECURITY—DATA AND PHYSICAL**

- AuxSvc personnel are responsible for the data they create and manipulate. They are responsible to see that all critical data are adequately backed up to tape or disk and stored in a secure location. Backups of critical data should never be stored in the same location as the computer itself.
- Prudent measures shall be taken so that uninvited persons or hackers cannot access AuxSvc computers. This means that indiscriminate sharing of hard disks (e.g., using programs like Napster with hard disk sharing turned on) is prohibited. Likewise, AuxSvc personnel should never share their login accounts with others.
- Likewise, downloading programs, screen savers and files from unknown sites is strongly discouraged. This practice exposes personnel to viruses and trojan programs.

- Physical access to computers should be properly controlled. Computers containing confidential data should never be left unattended while logged in without being locked with a password protected screen saver.

## **COMPUTER USE**

AuxSvc computer systems are provided to support the functions of AuxSvc and Duke University. Any unrelated commercial use is forbidden. Any unrelated non-commercial use is to be limited as follows:

- “Break-time” use is acceptable within guidelines set out by the individual AuxSvc departments.
- “Break-time” activities shall not result in the use of significant amounts of networking capacity or hard disk storage. For example, storing hundreds of megabytes of songs and transferring these files repeatedly is prohibited.
- All legal requirements, such as copyrights and software license agreements shall be obeyed.
- All Duke University computer regulations are applicable.
- Display of racist, pornographic and other inappropriate materials in a Duke University environment is prohibited.
- Display of materials offensive to co-workers will be adjudicated by the department Director and AuxSvc Personnel Director.

## **ATTACHING NETWORKED DEVICES TO THE PUBLIC NETWORK**

Publicly networked devices represent a security hazard if not properly secured. Furthermore, it is important to record, in a central location, the location, ip address and hardware address of all such devices. This facilitates identifying and locating these devices in case they become compromised or malfunction in a manner that causes interference to the rest of the network.

- All Auxiliary Services departments are to notify AIS when attaching a networked device to the public network. Any AIS staff member may be contacted, preferably before attaching the device. However, if circumstances do not permit early notification, then notification should occur no later than one business day later.

Exceptions: DukeCard Office and Computer Repair. DukeCard is exempted from the one business day requirement. They must notify AIS in a timely fashion. Computer Repair is exempted from all networked equipment they are servicing, but not from their own equipment.