BUENA VISTA
UNIVERSITY

# Information Technology Services

## Policy & Security Manual

## Procedures, Standards & Guidelines

*Revised October 2014*

## Table of Contents

## OVERVIEW

This Buena Vista University Information Technology Services (IT) Policies and Security Manual includes policies, standards, procedures and guidelines to ensure the integrity of BVU IT systems and reflect responsible stewardship of BVU IT resources. The IT department is primarily responsible for providing technology based services for all administrative, academic technology support, events and media services, mail and print services, the Help Desk (2Fix) and the Information Desk. Beginning in February 2013, the IT department will perform ongoing reviews of this document and recommend revised or new policies for approval by the President’s Cabinet.

# 1. COMPUTER PURCHASING POLICY FOR EMPLOYEES

Introduction

Prior to the enactment of this policy, the BVU ITS department absorbed a majority of the purchase costs for new computers, even when employees selected systems that cost significantly more than the standard Microsoft Windows-based systems. For example, in 2012, the Apple products such as the MacBooks actual cost to the institution is about $1,300. The IT department determined this funding model as unsustainable and on December 10, 2012 requested the President's Council approve a departmental charge-back funding model when Apple products are selected. The members of the President's Council agreed that a charge back funding model for more expensive computer systems was appropriate. On January 7, 2013, the President's Council committed to establishing the Windows-based PC as a standard for the institution. Requests for MacBooks (Apple products) may be approved on an exception basis if a business case is made (See Guidelines below). If approved, the full cost of the computer will be charged to the department of the requesting employee. Policy statements are below.

## **1.1.** Purpose

The purpose of the Computer Purchasing Policy is exercise judicious stewardship of BVU resources, standardize BVU technical equipment support, and ensure functionality of existing and new technology-based applications (such as the Jenzabar ERP and related products) on devices that attach to the BVU network.

## **1.2.** Audience

This Computer Purchasing Policy applies to all employees at BVU designated by the Vice President of the area as needing a PC to perform job duties.

## **1.3.** Definitions

1.3.1. PC - Personal Computer made by a manufacturer that is not Apple and has a Windows based operating system.

1.3.2. MacBook – a specific type of computer made by Apple.

## **1.4.** Computer Purchasing Policy

1.4.1. The IT department will supply one PC to each BVU employee as specified by the Vice President of that area.

1.4.2. The assigned PCs are BVU property.

1.4.3. The PC assigned to each employee will be selected by IT staff from an inventory pool, loaded with a standard BVU image.

1.4.4. The IT department will be responsible for the support of the PC. Employees are responsible for ensuring the safety, security, cleanliness of the PC and for contacting IT within 48 hours if the unit fails to function. Accidental damage to equipment is covered in a separate policy called *Equipment Repair* (in draft).

1.4.5. The IT department is responsible for periodic bulk purchasing of PCs to ensure an adequate supply is available for employees

1.4.6. The standard PC assigned to employees will not be charged to individual departments unless the computer system falls outside of the standard established by IT. In those cases, the department will be charged the full amount of the cost of the special system. Examples of special systems include Apple products and high-end computing systems running non-Windows operating systems. See the section on Guidelines below for determining if a special system is required. See the Standard Operating Procedures below for requesting a special system from IT.

**1.5.** Guidelines

1.5.1. A request for a Special System can be processed if any of the following conditions are true:

1.5.1.1. The duties of the position cannot be performed on a Windows-based PC

1.5.1.2. The productivity of the department is hindered without the special computer system

1.5.1.3. The courseware or computer application required to meet business or academic outcomes does not function in a Windows environment (i.e., Marketing Department Art, Graphic Design, Media, and certain areas of Science and Education

**1.6.** Standard Operating Procedures (SOP)

1.6.1. PC requests for new employees (new and existing)

1.6.1.1. Human Resources personnel set up a new employee account in the Kronos system. This includes creating the employee ID and marking the employee as active.

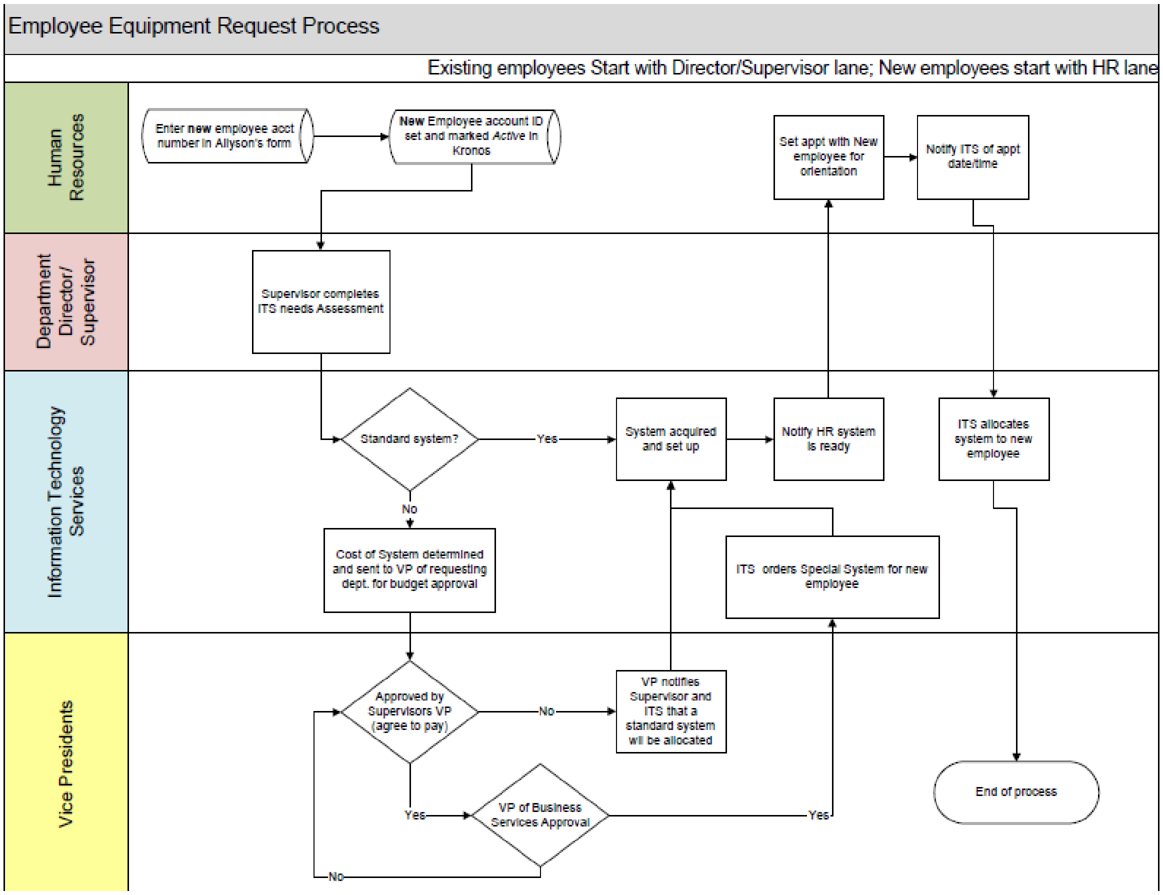
1.6.1.2. Supervisors requesting new personnel or changes in equipment for existing personnel complete an online form that includes a description of the business needs of the description (types of access). This will automatically send an electronic notice to IT.

1.6.1.3. IT personnel identify the appropriate system (standard or special) depending on business needs of the position.

1.6.1.3.1. If a standard system is allocated, IT will notify employee when the unit is available for pickup.

1.6.1.3.2. If a special system is needed, IT personnel will inform the Vice President in charge of the hiring department of the total costs of the special system. Copies will also be sent to the Vice President of Business Services. If approved by BOTH Vice Presidents, IT personnel will order and configure the special system and notify the employee when the unit is available for pickup. Total charges of the special system will be covered by the requesting department budget

1.6.1.3.3. Process map:


Employee Equipment Request Process
Existing employees Start with Director/Supervisor lane; New employees start with HR lane
Human Resources
Department Director/ Supervisor
Information Technology Services
Vice Presidents
Enter new employee acct number in Allyson's form
New Employee account ID set and marked Active in Kronos
Set appt with New employee for orientation
Notify ITS of appt date/time
Supervisor completes ITS needs Assessment
Standard system?
Yes
No
System acquired and set up
Notify HR system is ready
ITS allocates system to new employee
Cost of System determined and sent to VP of requesting dept. for budget approval
ITS orders Special System for new employee
Approved by Supervisors VP (agree to pay)
No
VP notifies Supervisor and ITS that a standard system will be allocated
Yes
VP of Business Services Approval
Yes
No
End of process

## 2. ACCOUNT & DATA RETENTION POLICY

### 2.1. Introduction

As a result of an assessment performed on the BVU network physical and logical architecture, BVU aligned with best practices of higher education institutions and activates the follow policies to ensure data integrity and relevance. It is the policy of Buena Vista University to manage its network accounts, and Records and Reference Documents in a uniform manner that will support institutional needs, provide efficient access to information, reduce storage needs, meet the University's legal and regulatory obligations, and protect the University during litigation. This Records Retention Policy (the "Policy") and their corresponding Records Retention Schedule provide guidance for managing the University's information from creation to retention to destruction. This policy was approved by President's Council on October 8, 2013.

### 2.2. Purpose

The purpose of the Account Policy is to efficiently standardize the creation, maintenance and deletion of accounts and data in the systems and applications of the BVU network.

### 2.3. Audience

The Policy governs all information created or received by the University in the course of business. It applies to all employees, temporary employees, consultants, students, and anyone else who has access to, or use of, the University's information. Anyone who creates, receives, uses, or manages the University's information is to comply with the Policy.

### 2.4. Definitions

2.4.1. ITS resources-Any and all technology-based systems owned by BVU capable of creating, printing, storing, and displaying information and used to perform BVU work. This includes computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to servers, personal computers, notebook computers, hand-held computers, smart phones, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology, telecommunication resources, network environments, telephones, fax machines, printers, wireless antennae, smart classroom and instructional devices such as projectors, document cameras, and DVD players). Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

2.4.2. Owner-The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

2.4.3. Custodian or Guardian or caretaker-The holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For Administrative applications (POISE and Jenzabar), ITS is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

2.4.4. An account is an identity on the BVU network that provides access to ITS resources. BVU data stored as part of a BVU provided account is considered the property of BVU.

2.4.5.The University's information is categorized as 1) an Institutional Record, 2) a Supporting Document, or 3) a Reference Document. The definitions for each category follow. Employees should first determine if the document with which they are working is an Institutional Record. If it is not, then they should determine if it is a Supporting Document or a Reference Documents.

2.4.5.1. Institutional Records ("Records") contain information that is created, received, or maintained as part of the University's business activities, contractual agreements, and/or legal requirements. A Record is the official, final, recorded position of the University. Records include, but are not limited to, the following:

- Charters, bylaws, board meeting minutes
- Legal opinions
- Real estate documents and blue prints
- Personnel records
- Company and department policies, procedures, training manuals
- Finance and tax documents, financial reports
- Audit reports
- Signed contracts
- Students' Academic Files

2.4.5.2. Supporting Documents support the creation, receipt, or maintenance of a Record. A Supporting Document contains information that is audited when the Record it supports is audited. Supporting Documents must be listed on the Records Retention Schedule with the Record it supports. In order for a department to list a Supporting Document on its Records Retention Schedule, the department must own the Record.

If the department does not own the Record, then anything it possesses relating to the record is considered a Reference Document. Examples of Supporting Documents include, but are not limited to, the following:

- "Versions" of a policy that are superseded by new version, but may be relied upon for the development of future version
- Memoranda supporting the development of a policy, procedure, or process
- Financial data supporting final financial reports

2.4.5.3. Reference Documents contain information created or received solely for reference or convenience. Reference Documents are not Records. They do not set policy, establish guidelines or procedures. As such, Reference Documents are subject to this Policy, but are not included on the Records Retention Schedule. Examples of Reference Documents include, but are not limited to, the following:

- Personal communications, including notes, e-mail, phone messages
- Handwritten notes
- Drafts (e.g., "marked-up" documents)
- Versions of a document that have been superceded by a final record
- Working copies or duplicate copies
- Unsigned letters or contracts
- Documents used for short-term reference purposes
- Publications, magazines, etc., from external sources
- Other material that is in preliminary stages or that has not been approved or authorized

### 2.5. New Account Policy

2.5.1. The following account retention policies apply specifically to employee (faculty and staff) and student accounts.

| Account Type | Access Disabled | Data Removed |
|---|---|---|
| Employees (Faculty/Staff) | Date of separation of employee as notified by HR | As per supervising Vice President; forward is also subject to approval. |
| Adjunct Faculty | Access maintained until account removed (warning of impending deletion sent 30 days prior to removal) | 1 year from end of last term taught |

| Account Type | Access Disabled | Data Removed |
|---|---|---|
| Students (non-graduating, full-time or GPS program) | Access disabled 30 days after end of last enrolled term (unless ITS is notified of pending return) | 30 days following graduation |
| Students (graduating) | Access maintained until account removed (warning of impending deletion sent 30 days prior to removal) | 1 year from end of last enrolled term |

2.5.2. ITS staff shall implement automated procedures to purge accounts as needed based on these retention windows

2.5.3. Exceptions require approval of the President or advice of Legal Counsel within defined retention window

### 2.6. Account & Data Retention Policy

2.6.1. Accounts are provided to active students, employees, and vendors and/or contractors under contract

2.6.1.1. Courtesy accounts previously provided to employee spouses and/or family members will not be provided. Existing accounts are grandfathered in.

2.6.1.1.1. An effort shall be made to contact retirees who still hold accounts and close those which are no longer needed or suggest the setup and use of alternatives or a forwarding address to those who are willing. Any remaining retirees who still wish to retain their account will be grandfathered under this policy.

2.6.2. A three month notice of cancellation will be provided for accounts identified for closure under this policy

2.6.3. The following retention policies are specific to archived tape or disk backups:

2.6.3.1. Three months for operating system or personal account data backups

2.6.3.2. Three years of POISE or subsequent ERP database backups (unless otherwise legally mandated)

2.6.4. All effort shall be made to purge unnecessary data on prospective students as soon as possible. Prospective student data that does not result in enrollment should be purged from system(s) within the time frame established in the data retention schedule..

2.6.5. Modification of existing POISE system RAMdisk snapshot backups from 60 to 30 minutes.

2.6.6.All Records (data) are the property of the University unless otherwise provided by contract.  At no time should Institutional Records be stored on a personal computer not issued by the University.

2.6.7. All Records are subject to a Records Retention Schedule (see Guidelines and SOPs below)

2.6.7.1. Each department must adhere to the Records Retention Schedule and must administer the retention and destruction of records in the normal course of business.

2.6.7.1.1. <u>Employees</u>: Every individual who generates, receives, or stores information of any type at any location are responsible for the following:

2.6.7.1.1.1. Creating all information in accordance with the University's Policies and Procedures.

2.6.7.1.1.2. Maintaining the confidentiality of proprietary and sensitive information

2.6.7.1.1.3. Retaining Records and Supporting Documents according to the Schedule;

2.6.7.1.1.4. Annually reviewing all Reference Documents to confirm destruction as appropriate.

2.6.7.1.2. <u>Record Owners</u>: Departments identified on the Schedule as "owners" are responsible for the following:

2.6.7.1.2.1. Annually reviewing the Schedule and identifying any Records with expired retention periods;

2.6.7.1.2.2. Destroying Records and Supporting Documents owned that are subject to destruction;

2.6.7.1.2.3. Providing any update to the Administration about a Record's title, owner, or retention period (such as changes in regulation).

2.6.8. Legal/Litigation Hold or Operational Hold ("Hold"): In the event of an anticipated or ongoing lawsuit or government investigation, the Administration may issue a legal hold over some or all the University's information.  Similarly, in the event of an audit, internal investigation, incident investigation or other operational activity, the relevant manager may issue an operational hold over some or all the University's information.  Information subject to a hold may include Institutional Records, Supporting Documents, and Reference Documents.  No information subject to a hold may be destroyed while the hold is in effect, nor may any individual violate the integrity of any information subject to the hold.

2.6.8.1. When a hold is imposed, the Administration or legal counsel will communicate with necessary individuals about information that is subject to the hold and about the duration of the hold.

2.6.9. E-mail communications: E-mail messages that constitute a Record or a Supporting Document will be retained according to the Records Retention Schedule based on the content of the e-mail. E-mail messages that are Reference Documents can be deleted at any time, but must never be saved longer than the Record to which the e-mail pertains. For more information about email retention, please reference BVU's Email Archiving and Retention Policy.

2.6.10. Computer systems transferred through sales or other arrangement shall only be provided with OEM software and licensing and stripped of all institutional data.

2.6.11. The Information Technology Council (IT Council) serves as the IT Services governing group that meets regularly to review proposals for policy changes.

2.6.12. Any employee in violation of these policies be subject to disciplinary action including but not limited to termination from the University.

2.6.12.1. Any employee who becomes aware of a violation of this Policy or any other University policy should promptly report any such violations to Administration or Human Resources.

**2.7. Guidelines and Standard Operating Procedures (SOP)**

2.7.1. Saved or archived email in employee accounts

2.7.1.1. Staff are advised that email correspondence should not be kept longer than 3 years

2.7.1.2. No email expiration policy will be implemented as of (June 2013) to automatically purge old messages in support of this policy, but the option to do so will be considered in the future

2.7.2. Institutional records may be stored in any format/medium; however, some storage methods are preferred over others. The following methods are preferred for storage of Institutional Records: (a) Electronic or Imaged Form on a Network Drive, (b) Paper, (c) Microfilm or microfiche and (d) Video or audio tape. The following are also valid storage formats or mediums but they are not preferred due to the lack of accessibility by other users of the information and their vulnerability to damage or loss: (a) E-mail and/or (b) hard drive, disk, jump-drive, or other electronic storage device

2.7.3. RECORDS RETENTION SCHEDULES**.** The Records Retention Schedule ("Schedule") indicates the Record owner, retention format, location, and retention period for each Record, as defined below. All Records and any Supporting Documents relating to a Record must be retained pursuant to the Schedule. Reference Documents are not included on the Schedule.

2.7.3.1. Owner: The department responsible for the Record throughout its lifecycle.

2.7.3.2. Format: Unless applicable law, regulation, or contractual arrangements state to the contrary, Records maintained exclusively in an electronic format (e.g., imaged documents) will have the same binding legal effect as Records maintained in an original paper format, as long as the electronic Records are reliable, trustworthy, and accurate versions of its original paper version.

2.7.3.3. Location: The Schedule indicates the storage location for Records. Records must be stored efficiently by limiting their storage locations. As an illustration, do not save notes regarding a meeting in the F: drive folder, and print a copy of the notes for storage in a file folder, and keep an e-mail copy.

2.7.3.4. Retention Periods: The retention periods provided in the Schedule are intended to be as short as possible to minimize the volume of Records while still complying with Institutional needs and legal or historical needs. Records should neither be kept longer than the period stated in the Schedule, nor should they be destroyed or discarded before the stated retention period expires. If a record is subject to two or more retention periods, the longer of the retention periods applies.

2.7.3.5. Every department must periodically review its Schedule to ensure its accuracy.

2.7.4. LIFECYCLE OF A RECORD

2.7.4.1. <u>Creation</u>: The University expects all individuals to act responsibly, lawfully, and professionally when creating Records, Supporting Documents, and Reference Documents. Employees are to use the utmost discretion when creating any Records or Documents, including transitory messages such as e-mail. All Records and Documents should be created with the specific purpose of communicating or documenting business matters. All Records and Documents (including e-mail) are the property of the University.

2.7.4.2. <u>Retention/Storage</u>: Each Record and any Supporting Documents must be retained according to the Schedule.

2.7.4.3. <u>Destruction</u>: When the retention period for a Record has expired, it is subject to destruction, unless the record is subject to a hold. The University will conduct an annual “Clean-Up Day” when all Records, Supporting Documents and Reference Documents will be reviewed as the follows:

2.7.4.3.1. Records will be destroyed if their retention period is expired, but only if there is no hold over the Records;

2.7.4.3.2. Supporting Documents must be retained as long as the Record it supports, but no longer;

2.7.4.3.3. Reference Documents must be reviewed to determine their use as a reference. They should be discarded annually, unless a business need dictates a longer retention, or unless subject to a hold.

2.7.4.3.4. When a Record is destroyed, all related Supporting Documents and Reference Documents in existence must be destroyed as well, unless subject to a hold.

2.7.5. A program to document and periodically test existing emergency and critical personal safety phones should be implemented (include existing call boxes, elevator phones, and other public areas (student and staff, including classrooms). ITS, Facilities, and Campus Security departments shall work closely together to establish, implement and maintain these procedures.

2.7.6. An off-campus Disaster Recovery (DR) site has been established to house sufficient computer system hardware necessary to provide business continuity of critical University services in the event the primary on-campus facility is unavailable for any extended period of time. As of July 2013, the needed permanent cooling system is under investigation.

2.7.7. These policies shall be reviewed annually and amended as appropriate.

2.7.8. Data Handling Guidelines for Existing Employees (Human Resources)

2.7.8.1. See attending documents below

# Data Handling Guidelines for Exiting Employees

Procedures for the HR and IT Departments

Last reviewed: 01/09/2013 by ITS and HR

## Overview

The intention of this document is to help ensure exiting employee's data and hardware is handled in a manner consistent with policy and best practice. It may also serve as documentation for audit purposes.

## Procedures

The following form shall be used for managing hardware and data for exiting employees. Both ITS and HR representatives must sign at the bottom to affirm that these procedures were followed by their respective departments. A copy of the signed document shall be kept in the Human Resources shared drive.

## Retention

After 30 days any data copied to the shared drive during the recovery process will be deleted, except of course, for any signed exit procedure form(s). HR may request the user data be kept for a defined length of time with permission from the President or Legal Counsel or the Chief Information Officer. Holding data for indefinite periods of time is discouraged.

## Data Access

Requests from exited employees or approved employees for data or email access shall be handled by HR. Note that data and email is kept for 30 days after termination date. HR is given access rights to exited employees email and copied data as a part of the procedures below.

## Common Scenarios

*Exited employee wants access to their Dropbox account or wants to change the email account associated with it.*

Recommended solution: If they know their password, then they can log in to Dropbox and change the email account on their own. If they have forgotten their password, then it is at HR and VP's discretion (and the availability of the email account) as to whether or not they will assist in resetting the password – in most cases an email will be sent to their BVU email account- HR can forward that to them to help them continue with the reset process. Once they reset their password and login, they can change the email address associated with it Instructions can be found on-line on the DropBox website.

## Exiting Employees Data Handling Form

______________________________________________________________________________

Name of Exiting Employee (Print)                                    Date

Please initial and date as completed:

1) HR recovers hardware from exiting employee (e.g., laptop, iPad, etc.)
Listing of recovered hardware:

______________________________________________________________________________

______________________________________________________________________________

______________________________

HR Initials        Date

2) HR delivers hardware listed above to IT. If any hardware listed above is not returned, please explain why. List also any special handling instructions.

______________________________________________________________________________

______________________________________________________________________________

__________________________________________________________

HR Initials        IT Initials            Date

3) Unless otherwise instructed, IT copies exiting employee's user profile (and DropBox folder) from laptop/computer to shared network drive and grants HR (Beth and Melissa) permissions to access it. IT provides HR with specific network location.

______________________________

IT Initials        Date

4) Unless otherwise instructed, IT grants HR (Beth and Melissa) full access rights to exited employee's email account. IT provides HR with instructions for access.

______________________________

IT Initials        Date

5) IT follows internal recovery procedures to return hardware to service (includes removing all personal data from computer storage).

______________________________

IT Initials        Date

______________________________________    ____________________________________________

IT Representative                           HR Representative

# 3. MOBILE DEVICE SECURITY POLICY

## **3.1.** Introduction

BVU is “subject to the information security requirements established by the Federal Trade Commission (FTC) for financial institutions” (U.S. Department of Education, 2012, p. 2-136) that holds higher education institutions responsible for safeguarding customer information, establishing and maintaining an information security program.

Every member of the University community who utilizes a laptop computer or mobile electronic data device (e.g. Laptop, Blackberry, Flash Drive, Smart Phone, Hand Held PC, iPad, MacBook, etc.) is responsible for the University data stored, processed and/or transmitted via that computer or device, and for following the security requirements set forth in this policy and in the Information Security Policy. This Policy applies to the device regardless if it is institution or individually owned.

## **3.2.** Purpose

The purpose of the Mobile Device Security Policy is to assure data integrity and confidentiality of employee and student information, as well as to control access and to educate users regarding limitations and liabilities pertaining to data access. Information is a vital University asset and requires protection from unauthorized access, modification, disclosure or destruction.

Further, through this policy, BVU will comply with federal regulations governing privacy and security of information, and to protect Confidential Data in the event of laptop computer or mobile electronic data device theft.

## **3.3.** Audience

This policy is for all BVU employees (Faculty and staff) and students.

## **3.4.** Definitions

## **3.5.** Policy Statements

### 3.5.1.Protection of Confidential Data

3.5.1.1. Every user of laptop computers or other electronic data mobile devices must use reasonable care, as outlined in the University’s Information Security Policy, to protect University Confidential Data as defined in the Data Classification Security Policy.

3.5.1.1.1. Protection of Confidential Data against physical theft or loss, electronic invasion, or unintentional exposure is provided through a variety of means, which include user care and a combination of technical protections such as authentication, encryption, and remote sanitization capability that work together to secure mobile devices against unauthorized access. **Prior to** use or display of Confidential Data via laptop computer or other electronic data mobile device, the following security measures must be in place.

3.5.1.1.1.1. A laptop or other electronic data mobile device must authenticate the user before access to services on or by the device shall be permitted.

Mobile devices must be configured to timeout after 15 minutes of inactivity and require re-authentication before access to services on or by the device will be permitted. The authentication mechanism(s) must not be disabled. This can also include the use of security features on mobile devices (i.e. - automatic lock). Furthermore, if institutional data is being placed on a personal device, approval would need to be obtained (i.e. - University e-mail on personal phone). Implicit approval can be assumed upon issuing a University owned device. Temporary access of University devices can be obtained with proper approval (i.e. – vendors).

3.5.1.1.1.2. The ITS approved encryption option must be enabled on laptop computers that transmit or store University confidential information.

3.5.1.1.1.3. Laptops shall be protected with antivirus software and updated daily if supported by the device. NOTE: BVU email is protected with centralized anti-virus and anti-spam software. This protection may not apply to email systems outside of BVU.

3.5.1.1.1.4. The use of University owned laptops off-campus is determined through employee status. Exempt employees are permitted to take and/or use their laptop outside of the work premises. Non-exempt employees are not permitted to work from home or any other location off-campus using a University owned or personal device.

3.5.1.1.2. The use of unprotected mobile devices to access or store Confidential Data is prohibited regardless of whether the equipment is owned or managed by the University.

3.5.1.1.2.1. Reporting Loss/Theft of Equipment or Data

3.5.1.1.2.2. University employees who possess University owned laptop computers and other portable electronic devices are expected to secure them whenever they are left unattended. Accordingly, the University will not reimburse or cover the cost for the loss of a laptop computer or other portable electronic device unless it is burglarized (i.e. taken from a locked desk, cabinet, closet, or office, the item was secured by using a locking cable, and there are signs of forced entry thereto)…or

3.5.1.1.2.3. For University equipment, all faculty and staff are required to maintain the physical care of the device as well as the content within. All laptops are covered under ADP (Accidental Damage Protection). Apple products, to include all versions of MacBooks and iPads, are not covered under ADP. Therefore, the staff and faculty will be responsible for the cost of replacement for a broken MacBook. Furthermore, the staff and faculty will also be responsible for the cost of a broken iPad, after the first offense.

3.5.1.1.2.4. In the event a University-owned or controlled laptop computer or other device is lost or stolen, the theft or loss must be reported immediately to Campus Security.

3.5.1.1.2.5. In the event University Confidential Data is contained on any personally-owned computer or device that is lost or stolen, ITS must be contacted immediately.

3.5.1.1.2.6. The ITS department has the right to wipe the device in the case of it being lost or stolen.

3.5.2. **Requirements When Traveling Overseas**

3.5.2.1. BVU personnel and students carrying University-issued laptops or other electronic data mobile devices while traveling abroad, whether on business or for pleasure, must comply with U.S. trade control laws. U.S. Export Control laws may prohibit or restrict such activities absent special U.S. government licenses. Before traveling abroad with a laptop or other electronic data mobile device, BVU faculty, staff, and students must understand the restrictions and are responsible for investigating and complying with the laws of both the U.S. and countries visited.

**3.5.3. Care of University Equipment**

3.5.3.1. For University equipment, all faculty and staff are required to maintain the physical care of the device as well as the content within. All laptops are typically covered under ADP (Accidental Damage Protection). Apple products, to include all versions of MacBooks and iPads, are not covered under ADP. Therefore, the staff and faculty will be responsible for the cost of replacement for a broken MacBook. Furthermore, the staff and faculty will also be responsible for the cost of a broken iPad.

**3.5.4. Acceptable Uses**

3.5.4.1. The use of University owned laptops off-campus is determined through employee status. Exempt (salaried) employees are permitted to take and/or use their laptop outside of the work premises. Non-exempt employees (hourly) are not permitted to work from home or any other location off-campus using a University owned or personal device.

## 3.1. Guidelines and Standard Operating Procedures (SOP)

3.1.1.The ITS can be contacted to determine if appropriate protections are already in place or assist with enabling the security measures for laptops or other electronic data mobile devices.

## 3.2. References

3.2.1.Family Educational Rights and Privacy Act of 1974 (**FERPA**)

3.2.2.Health Insurance Information Portability and Accountability Act (**HIPAA**)

| | | | |
|---|---|---|---|
| Section 4 | **ITS Policies** | mm/dd/yy | -Effective |
| | | 06/12/13 | -Revised |
| Section | **Data Access and Information Security** | IT Services | -Author |

## 4. DATA ACCESS AND INFORMATION SECURITY

### **4.1.** Introduction

The BVU ITS network serves as the primarily repository of institutional, academic, employee and student data. It is the responsibility of both the ITS personnel and users of the system to protect and security all data stored on the network, on PC’s and on electronic storage media. Maintaining the security, confidentiality, integrity, and availability of information stored in the University’s computer networks and data communications infrastructure (“University systems”) is a responsibility shared by all users of those systems. All users of University systems are responsible for protecting those resources and the information processed, stored or transmitted thereby as set forth in this policy.

### **4.2.** Purpose

The purpose of the Data Access and Information Security Policy is to assure data integrity and confidentiality of employee and student information, as well as control access and to educate users regarding limitations and liabilities pertaining to data access. Information is a vital University asset and requires protection from unauthorized access, modification, disclosure or destruction.

Further, BVU is “subject to the information security requirements established by the Federal Trade Commission (FTC) for financial institutions” (U.S. Department of Education, 2012, p. 2-136) that holds higher education institutions responsible for safeguarding customer information, establishing and maintaining an information security program.

### **4.3.** Audience

This policy is for all BVU employees (Faculty and staff) and students.

### **4.4.** Definitions

4.4.1.**Electronic data** includes any data stored in personnel or student records, institutional data used for institutional research, academic program information and any data deemed sensitive by BVU supervisors, managers, or executive level leaders.

4.4.2. **Electronic storage media** includes external hard drives, USB drives, CD’s, DVD’s or other peripheral devices or technologies as they become available for storing electronic data.

4.4.3. **Administrative information** is any data related to the business of the College including, but not limited to, financial, personnel, student, alumni, and physical resources. It includes data maintained at the departmental and office level as well as centrally, regardless of the media on which they reside, wherever it resides. Administrative information does not include library holdings or instructional notes unless they contain information that relates to a business function.

4.4.4. **Confidential information** requires a high level of protection due to the risk and magnitude of loss or harm that could result from disclosure, alteration or destruction of the data. This includes information whose improper use or disclosure could adversely affect the ability of the College to accomplish its mission as well as records about individuals requiring protection under the Family Educational Rights and Privacy Act of 1974 (FERPA). Confidential information includes, for example, student financial aid information, salary and benefits information, alumni gifts and student grades.

4.4.5. **Sensitive information** requires some level of protection because its unauthorized disclosure, alteration, or destruction might cause damage to the College. It is assumed that all administrative output from the administrative database is classified as sensitive unless otherwise indicated. Sensitive information includes, for example, class lists, contract data, and vendor data information.

4.4.6. **Public Information** (public data) can be made generally available both within and beyond the College. It should be understood that any information that is widely disseminated within the campus community is potentially available to the public at large. Public information includes, for example, telephone directory information.

4.4.7. **Student "Directory Information", as defined by FERPA -** Certain information, classified as "directory information", is available for public consumption unless the student specifically directs that it be withheld. Students, including former students may direct the Office of the Dean of Students not to disclose such information. Public directory information as defined by the Act includes: student’s name, address, telephone number, date and place of birth, major field of study, participation in officially organized activities, dates of attendance, degree and awards received, and the most recent previous educational institution attended.

**4.5.** Ownership of Electronic Files

4.5.1. Electronic files created, sent, received, or stored on the BVU ITS resources are the property of BVU with ownership responsibilities designated by the CIO as Vice Presidents of functional offices, appointed by the President. “Owners” or designees of electronic information will work with the CIO to assure strategies exist to meet required responsibilities and to ensure compliance. This includes:

1. Business functional information in the following categories:
    - 1.1.1.1. Social Security Numbers
    - 1.1.1.2. Credit Card Information
    - 1.1.1.3. Other personal financial information
    - 1.1.1.4. Student records, and
    - 1.1.1.5. Health information.
2. Restricted personal information – includes SSN and other data protected under state or federal law (e.g., financial, medical, or student data).
3. Mission Critical Information – includes information that is essential to BVU operations
4. Non-critical Information – includes information that is generally available to the public or has minimum impact on BVU customers.

**4.6.** Policies

4.6.1. Users of University systems are responsible for protecting the information processed, stored or transmitted over or on those systems, and for incorporating the practices in the Standard Operating Procedures (below) into their daily activities.

4.6.2. Access to data is determined by the supervisor, manager or executive level leader of each division or department. Access to administrative systems is granted based on the employee’s need to use specific data, as defined by job duties, and subject to appropriate approval. As such, this access cannot be shared, transferred or delegated.

4.6.3. BVU recognizes administrative information as an institutional resource requiring proper management in order to permit effective planning and decision-making and to conduct business in a timely and effective manner. Employees are charged with safeguarding the integrity, accuracy, and confidentiality of this information as part of the condition of employment.

4.6.4. Requests for release of administrative information are referred to the office responsible for maintaining those data. BVU retains ownership of all administrative information created or modified by its employees as part of their job functions.

4.6.5. Access to data will be controlled by both network account and passwords.

4.6.6. Users are to use data only for the designed purpose.

4.6.7. ITS personnel and users must not share BVU data with external entities without supervisor or manager approval.

4.6.8.ITS personnel must sign, retain a copy, and submit the Access to Privileged Data form to the CIO, who will provide copies for Human Resources.

4.6.9. Users will assure data integrity by contacting both supervisors and appropriate ITS personnel immediately if data is suspected of corruption or inappropriate changes.

4.6.10. Users will protect data by password protecting screen savers, logging off the network at the end of the workday, and securing printed documents.

4.6.11. ITS personnel and users may not disclose data to others, except as required by their job responsibilities.

4.6.12. ITS personnel and users may not use BVU data for their own personal gain, nor for the gain or profit of others.

4.6.13. ITS personnel and users may not access data to satisfy their personal curiosity.

4.6.14. All aspects of personnel records are confidential. Directory information for faculty and staff as published in the BVU Telephone Directory is public. Directory information may include some or all of the following: name, home telephone, spouse/partner name, department, position title, campus address, campus phone and email address. All data maintained in the published Telephone Directory is also available on-line from off campus locations. Faculty and staff may request that this data be classified as confidential. All other employee related data, especially that which is available to users outside Human Resources such as social security number and birth date, must be vigilantly safeguarded and treated as confidential.

4.6.15.

**4.7.** Guidelines and Standard Operating Procedures (SOP)

4.7.1. New Employees to the department/division –

1. Department security manager explains the Security Policy to the new employee and provides a written copy.
2. Department security manager emails request to ITS System Administrator attaching the Security Request Form.
3. ITS System Administrator creates the login and assigns Security Classes as instructed by the “owner” of the data.
4. ITS System Administrator replies to Department Security manager’s original email indicating the security has been established and schedules an appointment with new user.

5. Department security manager prints and signs Security Request Form.
6. Employee carries signed Security Request Form and last page of the Security Policy signed by the user to ITS System Administrator to acquire a password.
7. ITS System Administrator files signed Security Request Form.

4.7.2. Modification and Termination

1. ITS should be notified immediately as soon as an employee is terminated. The ITS System Administrator will disable all account access for that employee.
2. On a daily basis, ITS System Administrators will review reports identifying failed login attempts, including unsuccessful attempts by individuals to access portions of the system to which they are not authorized. After 15 consecutive failed login attempts, accounts are automatically deactivated. ITS will immediately notify the Department security manager and other appropriate College officials if it appears security has been breached.
3. Ideally, at the end of each payroll period, Human Resources will report to the ITS System Administrators new hires, transfers and terminations.

4.7.3. Passwords

Administrative information is protected through the vigilant use of user-defined passwords. Passwords must be:

*Changed by the user on-line every 180 days

*Changed by the user no more frequently than every five days

*Consist of both letters and numbers

*Eight characters in length, minimum

*Significantly different from prior passwords

Individuals are expected to protect passwords from disclosure. Every individual must have a unique user login.

### **4.8.** Disciplinary Actions

Violation may result in a denial of access to College computer resources, and those disciplinary actions provided or authorized by the Rules and Regulations of Buena Vista University through the Office of Human Resources or Student Services.

### **4.9.** References

Federal Trade Commission (FTC)

Family Educational Rights and Privacy Act (FERPA)

Gramm-Leach-Bliley Act, 15 U.S.C., Subchapter I, §§6801-09, Disclosure of Nonpublic Personal Information. Retrieved from http://www.ftc.gov/privacy/glbact/glbsub1.htm

U.S. Department of Education. (2012). School Eligibility and Operations 2012-2012. (FSA HB Jul 2012). Washington, DC: U.S. Government Printing Office.

### **4.10.** Other Information

Privileged Access Agreement

# Buena Vista University
# Information Technology Services
# Privileged Access Agreement

## INTRODUCTION

Privileged access enables an individual to take actions which may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically granted to system administrators, network administrators, staff performing computing account administration, or other such employees whose job duties require special privileges over a computing system or network.

Individuals with privileged access must respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with any relevant laws or regulations. Individuals also have an obligation to inform themselves regarding any procedures, business practices, and operational guidelines pertaining to the activities of their local department.

Individuals with privileged access may have the inherent ability to peruse confidential and proprietary information in the course of an assigned duty. While pursuing appropriate actions required to provide high-quality, timely, and reliable computing services, the Information Technology Services (ITS) employees must comply with applicable policies, laws, and regulations pertaining to confidential and sensitive information. The ITS policies are defined in the ITS Policies document and it is the responsibility of the ITS employee to be cognizant of changes and/or updates to said and other institutional policies. Changes will be communicated to BVU by the Information Technology Council (ITC).

## GENERAL PROVISIONS

1. Privileged access is granted only to authorized individuals. Privileged access shall be granted to individuals only after they have read and signed this Agreement.
2. Privileged access may be used only to perform assigned job duties.
3. Privileged access may be used to perform standard system-related duties. Examples may include:
   - installing system software;
   - relocating other individuals' files from critically overloaded locations;
   - performing repairs required to return a system to normal function, such as fixing files or file processes, or killing runaway processes;
   - running security or data checking programs.

4. Privileged access may be used to grant, change, or deny resources, access, or privilege to another individual only for authorized account management activities or under exceptional circumstances. Such actions must follow any existing organizational guidelines and procedures. Examples may include:

   - Disabling an account apparently responsible for serious activities such as: attacking the network or using a hosting to send harassing or threatening email, or using software to mount attacks on other hosts, or engaging in activities designed to disrupt the functioning of the host itself;
   - Disconnecting a host or subnet from the network when a security compromise is suspected;
   - Accessing files for law enforcement authorities with a valid subpoena.

   In the absence of compelling circumstances, the investigation of information in, or suspension of, an account suspected to be compromised may be delayed until normal business hours to allow appropriate authorization and/or notification procedures. With the exception of emergencies, suspension of a network account or access to data requires approval of the account holder's supervisor.

5. In all cases, access to electronic information that belongs to other employees shall be limited to the least perusal of contents and the least action necessary to resolve a situation.
6. Individuals with privileged access shall take necessary precautions to protect the confidentiality of information encountered in the performance of their duties.
7. If, during the performance of their duties, individuals with privileged access inadvertently see information possibly indicating inappropriate use, they are advised to consult with their supervisor. If the situation is an emergency, intervening action may be appropriate.
8. If, in the course of performing their duties, an employee makes discovery of a student or employee violating the terms of the Acceptable Use Policy, ITS or institutional policies, the CIO must be notified, as well as the Vice President of Business Services and the Director of Human Resources, or the Supervisor of the violator, whichever is appropriate.

**Authorization**

Under most circumstances, the consent of the account owner should be obtained if possible, before accessing their files or interfering with their processes before performance routine maintenance. However, if good faith efforts to obtain consent are not successful, or would unduly interfere with performance of assigned duties; obtain permission from the individual's direct supervisor, the CIO, the Vice President of Business Services and/or the Director of Human Resources, before taking such actions without consent.

**Notification**

If inspection of data or files is imminent, the ITS employee's supervisor, the affected individual's supervisor, or other authority shall, at the earliest possible opportunity, attempt to notify the affected individual of the action(s) taken and the reasons for the action(s) taken. This notification must occur before action is taken.

Attempts to notify the affected individual are not required if the individual is suspect of institutional, division, or department policy violations.

**AGREEMENT**

- I have read this *Privileged Access Agreement* and the ITS Policies.
- I agree to comply with the provisions of this *Privileged Access Agreement* and the ITS Policies of Buena Vista University.

**Employee**

Signature ______________________________ Date ___________________

Print Name _____________________________

Title___________________________________

**Supervisor**

Signature of Receipt ______________________ Date: ____________________

Print Name _____________________________

Title __________________________________

## 5. CHANGE MANAGEMENT

### **5.1.** Introduction

The Information Technology Services (ITS) infrastructure at Buena Vista University (BVU) is expanding and continuously becoming more complex. There are more constituencies dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between ITS and the BVU community grows, the need for a strong change management process is essential.

From time to time each ITS element requires an outage for planned upgrades, maintenance or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance or fine-tuning.

Managing these changes is a critical part of providing a robust and valuable ITS resource infrastructure.

### **5.2.** Purpose

The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that BVU employees can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of ITS resources.

### **5.3.** Audience

The Change Management Policy applies to all individuals that install, operate or maintain ITS resources.

### **5.4.** Definitions

5.4.1. ITS resources-Any and all technology-based systems owned by Buena Vista University capable of creating, printing, storing, and displaying information and used to perform AC work. This includes computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology, telecommunication resources, network environments, telephones, fax machines, printers, wireless antennae, smart classroom and instructional devices such as projectors, document cameras, and DVD players). Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

5.4.2. Owner-The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

5.4.3. Custodian or Guardian or caretaker-The holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For Administrative applications (POISE, CS and/or JX) ITS is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

5.4.4. Change Management-The process of controlling modifications to hardware, software, firmware, and documentation to ensure that ITS resources are protected against improper modification before, during, and after system implementation and to ensure minimum disruption of the business processes of the institution.

5.4.5. General Maintenance-General maintenance is not covered by the change management policy and includes minor modification to existing systems or applications such as software updates within a version, reimaging computers, basic maintenance of computers and/or AV systems.

5.4.6. Change-Modifications to hardware or software that have the potential to interrupt service, alter functionality or provide new technology capability.

5.4.7. Scheduled Change-Formal notification received, reviewed, and approved by the review process in advance of the change being made. These are performed within an announced, regularly occurring maintenance window.

5.4.8. Unscheduled Change-Absence of notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable if based on maintaining system integrity and security in a timely manner to prevent an emergency situation.

5.4.9. Emergency Change-When an immediate response to imminent critical system failure is needed to prevent widespread service disruption, such as a system failure, security breach, or data corruption.

**5.5.** Change Management Policy

5.5.1. Every change to a ITS resource such as: operating systems, computing hardware, networks, and applications is subject to the Change Management Policy and must follow the Change Management Procedures.

5.5.2. The Information Technology Council (IT Council) will serve as a Change Management Committee and will review change requests that impact business operations and to ensure that communications are being satisfactorily performed.

5.5.3. All changes or modifications to ITS systems, networks, programs or data must be approved by the owner department that is responsible for their integrity.

5.5.4.The IT Council may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate backout plans, the timing of the change will negatively impact a key business process such as yearend accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.

5.5.5. Owner and custodian notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures below.

5.5.6. A Change Management Log must be maintained for all changes. The log must contain, but is not limited to (a) Date of submission and date of change, (b) Owner and custodian contact information, (c) Nature of the change, and (d) Indication of success or failure.

5.5.7. All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with IT Directors, the CIO and the Vice President of Business Services.

**5.6.** Guidelines and Standard Operating Procedures (SOP)

5.6.1. A formal request for ITS related changes must be

**5.7.** Disciplinary Actions

Violation of this policy may result in disciplinary action which may include a verbal or formal documentation of a reprimand filed in an employee’s personnel file.

ACCEPTABLE USE POLICY

This policy applies

### **5.8.** Introduction

Information Technology resources at BVU are owned by Buena Vista University and administered by the Information Technology Services (ITS) division. BVU ITS provides access to appropriate campus IT resources to all members of the BVU community. Users are responsible for managing their use of IT resources and are accountable for their actions relating to the information technology and data security. This policy delineates user responsibilities. Information technology resources are strategic assets of Buena Vista University that must be managed as valuable resources.

### **5.9.** Purpose

The purpose of the Acceptable Use Policy describes specific user responsibilities related to both access and use of electronic information resources that assures system and data security, system availability and speed, and the prevention of illegal or inappropriate activity conducted on BVU computer equipment. This policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information technology resources.
- To establish prudent and acceptable practices regarding the use of information resources.
- To educate individuals who may use information resources with respect to their responsibilities associated with such use.

### **5.10.** Audience

This policy applies to all users including faculty, staff, students, and guests granted  user access to Buena Vista University computer networks, equipment, or connecting resources.

### **5.11.** Privacy

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of BVU are not private and may be accessed by BVU ITS employees at any time without knowledge of the ITS resource user or owner Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in supporting BVU policy documents. Further, BVU has the right to disclose the contents of electronic files, as required by legal, audit, or legitimate state, local, federal and/or institutional purposes.

### **5.12.** Policy

5.12.1. Users must report any weaknesses in BVU ITS computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.

5.12.2. Users must not attempt to access any data or programs contained on systems for which they do not have authorization or explicit consent.

5.12.3. Users must not share their BVU account(s), passwords, or similar information or devices used for identification and authorization purposes.

5.12.4. Users must not make unauthorized copies of copyrighted software. Employees will adhere to the terms of software licenses and other contracts. Persons loading software on any College computer must adhere to all licensing requirements for the software. Except where allowed by BVU site licenses, copying software licensed for BVU use for personal use is a violation of this policy.

5.12.5. Users must not use non-standard shareware or freeware software without BVU ITS management approval unless it is on the BVU standard software list.

5.12.6. Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of ITS resources; deprive an authorized BVU user access to a BVU resource; obtain extra resources beyond those allocated without communicating with ITS; circumvent BVU computer security measures.

5.12.7. Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, BVU users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on BVU ITS resources.

5.12.8. BVU ITS resources must not be used for personal benefit or profit.

5.12.9. Users must not intentionally access, create, store or transmit material which BVU may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the BVU official processes for dealing with academic ethical issues).

5.12.10. Access to the Internet from a BVU owned, home based, computer must adhere to all the same policies that apply to use from within BVU facilities. Employees must not allow family members or other non-employees to access BVU computer systems.

5.12.11. Users must not otherwise engage in acts against the aims and purposes of BVU as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

5.12.12. Users are to respect other people and the College's intellectual environment. Use of the network may not violate federal, state, or local law, including the laws of defamation, forgery, copyright/trademark infringement, and harassment. The copying or serving of copyrighted material such as music, movies, and other multimedia is strictly forbidden.

5.12.13. Incidental Use: As a convenience to the BVU user community, incidental use of BVU ITS resources is permitted with the following restrictions:

5.12.13.1. Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to BVU approved users; it does not extend to family members or other acquaintances.

5.12.13.2. Incidental use must not result in direct costs to BVU.

5.12.13.3. Incidental use must not interfere with the normal performance of an employee's work duties.

5.12.13.4. No files documents may be sent or received that may cause legal action against or embarrassment to BVU.

5.12.13.5. Storage of personal email messages, voice messages, files and documents within BVU Information Resources must be nominal.

5.12.13.6. All messages, files and documents – including personal messages, files and documents – located on BVU Information Resources are owned by BVU may be subject to open records requests, and may be accessed in accordance with this policy.

### **5.13.** College Inspection of Personal Electronic Information

5.13.1. Electronic information on BVU networks or equipment, including, but not limited to, electronic mail and personal information, is subject to examination by BVU staff where (a) it is necessary to maintain or improve the functioning of computing resources (b) where there is a suspicion of misconduct under BVU policies, or suspicion of violation of Federal or State laws; or (c) It is necessary to comply with or verify compliance with Federal or State law.

### **5.14.** Disciplinary Actions

Violation of the Acceptable Use Policy may result in a denial of access to College computer resources, and those disciplinary actions provided or authorized by the Rules and Regulations of Buena Vista University through the Office of Human Resources or Student Services.

## 6. NETWORK ACCESS AND SECURITY

### **6.1.** Introduction

The ITS network infrastructure is provided as a central utility for all users of Buena Vista University. It is important that the infrastructure, which includes cabling and the associated ‘active equipment’, continues to develop with sufficient flexibility to meet BVU’s demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

### **6.2.** Purpose

The purpose of the ITS Network Access and Security Policy is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of BVU information.

### **6.3.** Audience

The ITS Network Access and Security Policies apply equally to all individuals with access to any BVU electronic information resource that resides on the network and devices attached to the central network, such as PC’s and external storage devices.

### **6.4.** Definitions

**Information Technology Resources:** Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

### **6.5.** Policies

6.5.1.Users are permitted to use only those network addresses (IP) issued to them by BVU ITS.

6.5.2. All remote access to ITS resources will be through approved processes such as MyBVU or web access to email.

6.5.3. Employees and students may connect to the BVU Network information resources through Internet Service Providers of their own choice.

6.5.4. Users inside the BVU firewall may connect to the BVU network using approved devices only.

6.5.5. Users must not extend or re-transmit network services in any way. This means employees and students may not install a router, switch, hub, or wireless access point to the BVU network without ITS approval. (see 6.5.10 below)

6.5.6. Users must not install network hardware or software that provides network services without ITS approval.

6.5.7. Non-BVU computer systems that require network connectivity must conform to BVU ITS Standards.

6.5.8. Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, BVU users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the BVU network infrastructure.

6.5.9. Users are not permitted to alter network hardware in any way.

6.5.10. Users must not utilize, on campus, wireless devices that operate at 2.4 GHz, this includes wireless routers, wireless printers, chrome cast, etc.

**6.6.** Guidelines and Standard Operating Procedures (SOP)

6.6.1. Users may contact to 2FIX, ITS Directors or the CIO to arrange approval for new types of network access.

**6.7.** Disciplinary Actions

6.7.1. Violation of the Acceptable Use Policy may result in a denial of access to College computer resources, and those disciplinary actions provided or authorized by the Rules and Regulations of Buena Vista University through the Office of Human Resources or Student Services.

**6.8.** Other Information

**6.9.** References

## 7. INTERNET USE

### **7.1.** Introduction

Information resources are strategic assets of BVU that must be managed as valuable institutional resources. Thus this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of the internet.
- To educate individuals who may use the internet, the intranet, or both with respect to their responsibilities associated with such use.

### **7.2.** Purpose

To fulfill Buena Vista University's mission, Buena Vista University provides access to a broad range of information resources, including those available through the Internet. We make this service available as part of our mission to offer a broadly defined program of informational, educational, recreational and cultural enrichment opportunities for the members of the College and community of Storm Lake. Buena Vista University only assumes responsibility for the information provided on the home page and the supporting web pages resident on the Buena Vista University's server network. Buena Vista University does not monitor and has no control over the information accessed through the Internet. The Internet offers access to many valuable local, national, and international sources of information. However, not all sources on the Internet provide accurate, complete, or current information. A good information consumer evaluates the validity of information found.

### **7.3.** Audience

The BVU Internet Use Policy applies equally to all individuals granted access to any BVU Information Resource with the capacity to access the internet, the intranet, or both. Policies related to instructional labs for student use are addressed in those labs. If you have any questions about the policy, please contact Information Technology Services personnel for more information.

### **7.4.** Definitions

7.4.1. **User**: An individual, automated application or process that is authorized to access the resource by the owner, in accordance with the owner's procedures and rules.

7.4.2. **Internet**: A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges.

7.4.3. **Intranet:** A private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized users within an organization. An organization's intranet is usually protected from external access by a firewall.

7.4.4. **World Wide Web**: A system of Internet hosts that supports documents formatted in HTML (HyperText Markup Language) which contains links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Microsoft Internet Explorer and Foxfire.

7.4.5.**Vendor:** someone who exchanges goods or services for money.

### **7.5.** Ownership

Electronic files created, sent, received, or stored on computers owned, leased administered or otherwise under the custody and control of BVU are the property of BVU.

### **7.6.** Privacy

Electronic files created, sent, received, or stored on BVU ITS Information Resources owned, leased, administered, or otherwise under the custody and control of BVU are not private and may be accessed by BVU employees at any time without knowledge of the user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards established in this policy manual.

### **7.7.** Policy

7.7.1. Responsibility of users - The user will engage in no activity, which abuses any resource of the Buena Vista University network, whereby the network is restricted in use or is damaged in any manner. The Information Technology Services staff constantly monitors the BVU network to insure the proper operation of the service. The ITS staff will counsel with individuals whose practices impinge on the capabilities of services and assist those individuals in eliminating any abusive practices.

7.7.2. Software for browsing the Internet is provided to authorized users for business, academic and research use only.

7.7.3. All software used to access the Internet must be part of the BVU standard software suite or approved by the ISO. This software must incorporate all vendor provided security patches.

7.7.4. All files downloaded from the Internet must be scanned for viruses using the approved ITS distributed software suite and current virus detection software.

7.7.5. All software used to access the Internet shall be configured to use the firewall http proxy.

7.7.6. All sites accessed must comply with the BVU Acceptable Use Policies.

7.7.7. All user activity on BVU ITS resource assets are subject to logging and review.

7.7.8. Content on all BVU Web sites must comply with the BVU Acceptable Use Policies.

7.7.9. No offensive or harassing material may be made available via BVU Web sites.

7.7.10. Non-business related purchases made over the internet are prohibited. Business related purchases are subject to BVU procurement rules.

7.7.11. No personal commercial advertising may be made available via BVU Web sites.

7.7.12. BVU internet access may not be used for personal gain or non-BVU personal solicitations.

7.7.13. No BVU data will be made available via BVU Web sites without ensuring that the material is available to only authorized individuals or groups.

7.7.14. All sensitive BVU material transmitted over external network must be encrypted.

7.7.15. Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

7.7.16. Incidental Use

7.7.16.1. Incidental personal use of Internet access is restricted to BVU approved users; it does not extend to family members or other acquaintances.

7.7.16.2. Incidental use must not result in direct costs to BVU.

7.7.16.3. Incidental use must not interfere with the normal performance of an employee’s work duties.

7.7.16.4. No files or documents may be sent or received that may cause legal liability for, or embarrassment to, BVU.

7.7.16.5. Storage of personal files and documents within BVU’s ITS resources should be nominal. All files and documents – including personal files and documents- are owned by BVU, may be subject to open records requests, and may be accessed in accordance with this policy.

**7.8.** Guidelines and Standard Operating Procedures

7.8.1. Choosing and evaluating resources - The Internet is a global entity with a highly diverse user population and information content. BVU patrons use it at their own risk. The College cannot censor access to materials or protect users from materials they may find offensive. The user alone is responsible for the information accessed through the Internet. BVU reserves the right to choose sources to link to our home page. In doing so, the College will provide links only to those sites that conform to the College's mission and goals. Beyond this, we do not monitor or control information accessible through the Internet and do not accept responsibility for its content. We are not responsible for changes in content of the sources to which we link, nor for the content of sources accessed through secondary links. As with printed information, not all sources on the Internet provide accurate, complete, or current information. Users should evaluate Internet sources just as they do printed publications, questioning the validity of the information provided. The College expressly disclaims any liability or responsibilities arising from access to or use of information obtained through its electronic information systems or any consequences thereof.

**7.9.** Disciplinary Actions

Violation may result in a denial of access to College computer resources, and those disciplinary actions provided or authorized by the Rules and Regulations of Buena Vista University through the Office of Human Resources or Student Services.

**7.10.** Other Information

**7.11.** References

Copyright Act of 1976

Foreign Corrupt Practices Act of 1977

Computer Fraud and Abuse Act of 1986

Computer Security Act of 1987

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The State of Texas Information Act

Texas Government Code, Section 441

Texas Administrative Code, Chapter 202

IRM Act, 2054.075(b)

DIR Practices for Protecting Information Resources Assets

DIR Standards Review and Recommendations Publications

## 8. E-MAIL USE POLICY

### **8.1.** Introduction

Electronic mail is available to facilitate the professional and business work of persons employed at Buena Vista University. It provides a way to communicate with individuals and with designated groups. Buena Vista University encourages appropriate use of E-mail to enhance productivity through the efficient exchange of information in furtherance of education, public service and the expression of ideas. Use of this resource must be consistent with these concepts. As a responsible member of the college community, employees are expected to act in accordance with the following general guidelines. These guidelines are not meant to be all-inclusive. Generally accepted practices of common sense, decency, civility and legality should be taken in to account when E-mail is utilized.  BVU information resources are strategic assets that must be managed as valuable resources. Thus this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of email.
- To educate individuals using email with respect to their responsibilities associated with such use.

### **8.2.** Purpose

The purpose of the BVU Email Policy is to establish the rules for the use of BVU email for the sending, receiving, or storing of electronic mail.

### **8.3.** Audience

The BVU Email Policy applies equally to all individuals granted access privileges to any BVU information resource with the capacity to send, receive, or store electronic mail.

### **8.4.** Definitions

8.4.1.**Electronic mail system**: Any computer software application that allows electronic mail to be communicated from one computing system to another.

8.4.2. **Electronic mail (email):** Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

8.4.3. "**Mass e-mailings**" are considered those sent to the entire campus, student body or a subset of students larger than a department, program, or satellite campus.

**8.5.** Policies

8.5.1. The Information Technology Service (ITS) staff is charged with maintaining the hardware, software and network for maximum efficiency of the E-mail system. Lack of adherence to these guidelines will adversely impact the capabilities of campus-wide servers. ITS staff will counsel with individuals or supervisors of individuals whose practices impinge on the capabilities of the services and assist them in reducing their drain on resources.

8.5.2. Messages sent as electronic mail should meet the same standards for distribution or display as if they were tangible documents. The user should identify him or herself clearly and accurately in all electronic communications. A user's concealing or misrepresenting identity or affiliation is inappropriate**.**

8.5.3. Alteration of the source of electronic mail or its message is unethical and illegal. Such action can get Buena Vista University blacklisted as a spammer.

8.5.4. Electronic mail is the property of the college; however, no attempt to access another's electronic mail by unauthorized individuals is permitted. ITS employees may, from time to time, have a need to access a user's E-mail for routine purposes of repair, upgrades, etc.

8.5.5. Concerning the issue of federal law governing privacy, network system administrators will not intentionally access the content of E-mail messages and if content is accidentally accessed, it will be treated as confidential.

8.5.6. The user is asked to be sensitive to the inherent limitations of shared network resources. No computer security system can absolutely prevent unauthorized access to its files. The college will be unable to guarantee absolute privacy and confidentiality of electronic documents. Password security and confidentiality are the responsibility of the user. ITS will provide guidelines for the frequency of change and the nature of passwords. In keeping with good judgment, users should create electronic documents as if they were to be made available to the public**.**

8.5.7. Abusive, threatening, or harassing E-mail is prohibited. While debate on controversial issues is inevitable and essential at an educational institution, E-mail of a debate nature should advance the cause of learning and mutual understanding.

8.5.8. The user is expected to promote efficient use of network resources consistent with the instructional, research, public service and administrative goals of the college. The user is expected to refrain from any use that would interfere with another's work or disrupt network resources. The user should avoid wasteful and disruptive practices such as allowing large amounts of E-mail to go unattended, spreading **chain letters**, or sending of other unsolicited material.

8.5.9. Restraint in the use of the **Everyone Group** feature of the E-mail software is expected of the user. Use of the **Everyone Group** feature for non-BVU related content must have supervisor approval.

8.5.10. The user is not to use the **Everyone Group** to send recipes, jokes or humor, large attachments, requests for placement of a pet, distribution of any form of spam, or any non-college related announcement.

8.5.11. E-mail and other network resources may not be used for commercial purposes or for personal financial gain. This does not preclude the user from investigating the relative advantages or disadvantages of a potential college-purchased product.

8.5.12. Standards of conduct expected of students, faculty and staff in regard to the use of telephones, libraries and other institutional resources apply to E-mail. Users will be held accountable for their actions, as they would be when using other forms of communication.

8.5.13. Individuals must not send, forward or receive confidential or sensitive BVU information through non-BVU email accounts.  Examples of non-BVU email accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).

8.5.14. Individuals must not send, forward, receive or store confidential or sensitive BVU information utilizing non-BVU accredited mobile devices.  Examples of mobile devices include, but are not limited to, Personal Data Assistants and cellular telephones.

8.5.15. Sending Mass E-Mailings to Students

8.5.15.1. The purpose of this policy is to provide guidance on the appropriate use of mass e-mailings to the student population. For the purposes of this policy, “mass e-mailings” are considered those sent to the entire student body or a subset of students larger than a department, program, or satellite campus. This policy does not limit the right of individual faculty members, departments, programs, or satellite campus directors to send e-mails to their respective constituencies nor does it limit the right of the College Relations Office to use prospective student email addresses for marketing and recruitment purposes.

8.5.15.2. All requests for student e-mail address extracts from the Student database must be initiated through the Registrar.

8.5.15.3. Mass e-mailings are an internal form of communication to be used for official academic and administrative purposes only. The sale/distribution of BVU student e-mail addresses to non-BVU entities is prohibited, except as allowed by FERPA regulations. In such cases where distribution is allowed, the request must be fulfilled by the Registrar's office.

8.5.15.4. E-mail addresses extracted for purposes of mass mailings may only be used by officially designated "Gatekeepers" - individuals assigned responsibility to approve mass e-mailings for certain student populations. They should never be provided to "end-users".

8.5.15.5. Mass e-mailing approvals will be handled by various Gatekeepers as follows:

8.5.15.5.1. Academic mass e-mailings to the entire student body or a subset greater than the Division level must have the approval of the Vice President of Academic Affairs (or designee).

8.5.15.5.2. Academic mass e-mailings to a subset of students at the Division level must have the approval of the appropriate Division Chair (or designee).

8.5.15.5.3. Administrative mass e-mailings to students must have the approval of the Dean of Student and Academic Development (or designee) regardless of the student population targeted.

8.5.15.5.4. Recruitment-oriented mass e-mailings to prospective students must have the approval of the Dean of College Advancement (or designee), regardless of the size of the population targeted.

8.5.15.5.5. Mass e-mailings to all students will be restricted to those messages that are considered to be an emergency, time-sensitive, or critical to support the academic and administrative functions of the College.

8.5.15.6. Examples of appropriate mass e-mails to all students

8.5.15.6.1. Issues involving College facilities or affecting working/teaching conditions, such as power outages or building closures; essential or urgent official administrative e-mail from College departments, such as financial aid and registration information, policy and procedure dissemination, and technology updates.

8.5.15.7. Examples of inappropriate mass e-mails to students

8.5.15.7.1. Those from non-BVU entities; for personal gain; from an individual rather than a College department; optional student event announcements; chain letters; general broadcast messages or announcements (clubs, student government, intramural events, theater); for unlawful purposes; containing information of a confidential or sensitive nature; promotion of political viewpoints; surveys that do not serve sanctioned College purposes; messages containing confidential information such as course grades, financial aid award amounts, or tuition/fee payment amounts.

**8.6.** Guidelines and Standard Operating Procedures (SOP)

8.6.1. Examples of Acceptable Uses of E-mail

8.6.1.1. The distribution of minutes of various committees as well as other notices of general interest to all faculty and staff.

8.6.1.2. The use of **personal groups** is appropriate in circumstances, such as updating mailing lists, announcing committee assignments, and distributing facts about pending legislation.

8.6.2. Examples of Inappropriate Uses of E-mail

8.6.2.1. Announcement of the sale of personal property or the solicitation of support for a particular political position. However, **point-to-point** communication with governmental representatives is acceptable.

8.6.2.2. User subscription to **listservs** is an acceptable method of keeping current on many issues. The user is expected to confine subscriptions to a limited number and not **backlog** the E-mail system with large number of unattended items.

8.6.2.3. The sending of large attachments such as personal photographic images is strongly discouraged.

8.6.2.4. The user is expected to be honest, legal, and ethical and consider what he or she is sending before sending it. Abuse of computing privileges and any violations of these guidelines and policies established by the college will be treated as a serious matter. By using the college's E-mail system, the user agrees to abide by these policies. These policies are subject to change as technology advances, legal outcomes, or other unforeseen events may occur.

8.6.2.5. General Guidelines

8.6.2.5.1. Keep messages simple and direct.

8.6.2.5.2. Ensure that any non-directory information (see FERPA for definition of directory information) is sent only to the student.

8.6.2.5.3. Use plain text in messages--do not include HTML or formatted content.

8.6.2.5.4. Format messages so that lines wrap at 72 characters or less.

8.6.2.5.5. Include the name, title, and e-mail address of both the sender and the approving Gatekeeper.

8.6.2.5.6. Include the recipient e-mail addresses in the BCC (Blind Carbon Copy) field if the e-mail is sent to more than one individual at a time.

8.6.2.5.7. Include requestor's phone number/extension.

8.6.2.5.8. The e-mail cannot contain attachments (links to web pages should be used instead).

8.6.2.5.9. Content and grammar are the responsibility of the requestor.

8.6.2.5.10. When a message is to be sent to more than 1,000 students, send separate mailings in groups of no more than 1,000 email addresses.

8.6.3.Procedure

8.6.3.1. Make request to Registrar and obtain proper approval, obtain email listing, compose message and send.

8.6.3.2. Requests for mass e-mailings can be submitted by filling out the web-based request form located on the Registrar's Intranet site.

8.6.3.3. Turnaround time goals for sending mass emailings

8.6.3.3.1. As soon as possible for critical e-mailings

8.6.3.3.2. Within 3 business days for standard e-mailings

8.6.3.3.3. Within 3 business days of receiving the student population extract from the Registrar's Office for specialized populations.

**8.7.** Disciplinary Actions

Violation may result in a denial of access to College computer resources, and those disciplinary actions provided or authorized by the Rules and Regulations of Buena Vista University through the Office of Human Resources or Student Services.

**8.8.** Other Information

**8.9.** References

## AUDIOVISUAL EQUIPMENT USE POLICY

### **8.10.** Introduction

Equipment Services maintains a large inventory of multimedia equipment to support instruction. Services include equipment check-out, equipment delivery for one-time and regularly scheduled event, and maintenance and repair.

### **8.11.** Purpose

The purpose of the Audio-Visual (AV) Equipment Use Policy is to assure availability of AV equipment for instructional purposes and to protect the assets of the BVU community.

### **8.12.** Audience

This policy pertains to all employees of the BVU community.

### **8.13.** Definitions

8.13.1. Audio-Video equipment includes overhead projectors, LCD projectors (ceiling-mounted and portable), televisions, DVD players, carts, screens, audio recorders, mixers and systems, and in some cases, laptop computers.

### **8.14.** Policy

8.14.1. BVU Employees: College-owned equipment may be reserved for use, subject to availability, by any employee of Buena Vista University for use at a College-sponsored activity, provided that proper check-out procedures have been followed. Buena Vista University reserves the right to deny use of equipment if deemed not to be in the interest of the College. Equipment may be checked-out for off campus use overnight and over weekends for instructional preparation or presentation and is subject to availability.

8.14.2. Students: Students may only check-out equipment for instructional/class projects, not for personal use. A valid student I.D., written authorization from the instructor and the type of equipment requested is required. The student's instructor assumes responsibility for the use and security of the equipment. Students will follow the same procedures as Instructors/Employees for off campus equipment check-out.

8.14.3. Equipment Services do not provide equipment for non-college sponsored activities.

8.14.4. Equipment Services will maintain and regularly update lists of types of equipment available for classroom use and check-out on the ITS website.

8.14.5. Due to limited supply, LCD projectors and laptop computers cannot be checked out for the entire semester and limited to a maximum of 48 hour check-out timeframe.

8.14.6. Purchases of AV and video conferencing equipment require collaboration with ITS personnel for product specifications and pricing prior to requesting purchase approval from the Technology Replacement Task Force (TRTF).

8.14.7. Equipment services will purchase new systems on behalf of the institution based on either needs articulated by individual departments during annual reviews or obsolescence of equipment. Both scenarios require approval from the TRTF.

8.14.8. Priority availability. Equipment will be distributed for use according to the following order of priority:

a. Classroom and official college programs
b. miscellaneous administrative use
c. faculty use for instructional preparation
d. support of student activities
e. other campus use

**8.15.** Guidelines and Standard Operating Procedures (SOP)

8.15.1. General Information

8.15.1.1. Equipment will be delivered for use on a one-time or regularly scheduled basis.

8.15.1.2. Equipment that is in adequate supply can be reserved for semester use. These items will be picked-up for servicing at the end of the semester and will be returned upon request.

8.15.1.3. Items checked-out on a semester basis may be placed into hourly use by Equipment Services in the event of equipment shortage.

8.15.1.4. Equipment Services operating hours are 7:00 a.m. to 4:00 p.m. Monday through Friday.

8.15.2. Equipment Delivery/Sign-Out Procedures

8.15.2.1. On Campus Use: Equipment will be delivered to a secure location, set up before the time requested and retrieved by Equipment Services personnel. Requests must be received 24 hours in advance of the time at which the equipment is needed. If video or computer projection is required, the request must be received 48 hours in advance.

8.15.2.2. Off Campus Use: A request must be received 72 hours (not including weekends) prior to the time that the equipment is needed. Equipment Services cannot guarantee the availability of the desired equipment. The person making the request will be notified at that time if the equipment is not available. The person making the request must pick up, sign for, and return the equipment to Equipment Services Distribution, Russell Hall-121. For College-sponsored activities, Equipment Services personnel can be available for delivery, set-up, and retrieval of the requested equipment.

8.15.2.3. Equipment Deliveries for Off Campus, College Sponsored Functions: All functions must be scheduled where equipment can be delivered to a secure location and pick-up can be made during normal working hours. The request must be received and approved a minimum of 3 working days in advance of the setup.

8.15.2.4. Late Requests for Equipment: Equipment Services cannot guarantee availability and/or delivery of equipment requested less than 24 hours in advance of the need. Faculty and staff making late requests may have to pick up equipment, subject to availability, from Equipment Services in Russell Hall 121. The user must return this equipment unless prior arrangements have been made.

8.15.3. Equipment Repair

8.15.3.1. Equipment Services maintains qualified personnel and facilities to repair most types of equipment. Call either the HelpDesk or Equipment Services to request assistance with the repair of any malfunctioning equipment. In a request for repair, please specify the type of equipment, the location, when the malfunction occurred, and the nature of the problem.

**8.16.** Other Information

**8.17.** References