BRANDMAN
University
CHAPMAN UNIVERSITY SYSTEM

# Brandman University

## Information Technology

## Acceptable Use and Copyright Infringement Policy

Version 1.0 March 29th, 2017

Table of Contents

## 1. Executive Summary

Brandman University (BU) is committed to becoming the recognized leader in the evolution of adult learning. BU supports the educational, instructive, research, and administrative activities of its University community.

To be effective, information security policies must be a team effort involving the participation and support of every user using University information systems.

All users of Brandman University technology agree to abide by this policy. Use of Brandman University technology resources constitutes acceptance of the terms and conditions specified by these policies. The policy describes acceptable use of Brandman University technology, whether accessed through computers and devices owned by Brandman University, or through personally owned computers and devices connected to the Brandman network, or remotely through outside equipment. For the purposes of this policy, Brandman University technology resources is defined to include all Brandman University owned computer equipment, the operating systems and application software that reside on this equipment, and the networking hardware and software which connects this equipment. By extension, this policy applies to all Internet traffic that flows through Brandman University infrastructure.

Brandman University provides various information technology resources to authorized employees and students to assist them in performing their job/study duties for the University. Each employee and student has a responsibility to use the university's information technology resources in a manner that increases productivity and/or improves study capabilities, enhances the University's public image, and is respectful of other employees and students. Failure to follow the University's policies regarding its technology resources may lead to disciplinary measures, up to and including termination or revocation of student privileges.

"Information technology resources" consist of all electronic devices, software, and means of electronic communication, including but not limited to, the following, whether provided or supported by the University: personal computers and workstations; laptop computers; servers; computer hardware, such as wireless devices and network components; peripheral equipment, such as printers, scanners, fax machines, and copiers; computer software applications and associated files and data, including software that grants access to external services, such as the Internet; electronic mail; telecommunications systems such as telephones; cellular phones; smart phones; pagers; personal digital assistant devices, voicemail and text mail systems, TVs and appliances.

Although Brandman University implements due diligence and takes all the reasonable steps to preserve the individual's privacy, files, messages and electronic data could potentially need to be reviewed for subpoenas to respond to court order or law enforcement requirements.

## 1.1 Purpose

The goal of this policy is to define the user's behavior and clarifies the responsibilities of University users and the steps they must take to help protect University information and information systems.

## 1.2 Scope

This policy applies, to all Brandman University users such as: employees, vendors, contractors, visitors and students.

## 1.3 Overview

This document is organized into 4 sections and 1 Appendix.

This Executive Summary is Section 1 and provides the intent of this policy.

Section 2 defines this policy.

Section 3 defines this policy's enforcement.

Section 4 identifies related standards, policies and processes.

Appendix A contains References and Revision history.

## 1.4 Terminology

The following terms are used throughout this policy and are defined here to avoid ambiguity and misunderstanding.

**Port Scanner**[1] - is an application designed to probe a server or host for open ports. This is often used by systems/network administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities.

**Honeypot**[2] - is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site, but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, which are then blocked.

# 2. Policy

## Introduction

The University's Information technology resources are meant to be used only for the purpose of conducting University business.

Brandman users may access, use or share University's information technology resources only to the extent it is authorized and necessary to fulfill their assigned job duties or study activities.

The University strongly discourages users from storing any personal data on any of the University's Information technology resources.

As a condition for receiving a Brandman University account, users agree to observe the following:

1. It is appropriate to use Brandman University technology resources for classroom and instructional activities, research related activities, correspondence and support and administrative functions. Misuse includes but is not limited to violation of federal or state law, violation of University policies, unauthorized use of the technology for commercial purposes, displaying sexually graphic images or text, abusive language, harassing behavior, and excessive use for non-official or frivolous purposes.

2. University owned equipment and Brandman University technology resources and services may not be used for illegal purposes. Users must abide by all software licenses, copyright and intellectual property policies and applicable federal and state laws. Plagiarism of electronic works is prohibited. The unauthorized use and downloading of copyrighted material is prohibited. This includes but is not limited to:
   a. Reproduction of copyrighted materials, trademarks, or other protected material in any electronic form without express written permission from the material's owner.
   b. Use, distribution or duplication of copyrighted software without appropriate licensing agreements, or use of software in a manner inconsistent with its license;
   c. Use, distribution or reproduction, in any digital form, of copyrighted music, video, or other multimedia content without the express written permission of the material's rightful owner;
   d. Copyright violations as they apply to all information available electronically including unauthorized peer-to-peer software.

Violations may result in civil and criminal penalties, including fines and imprisonment. For more information on copyright law, please visit the U.S.

Copyright Office at www.copyright.gov[3]. Aside from civil or criminal penalties, such actions are deemed a violation of the Student Conduct Code, and may result in adjudication and possible sanctions as called for by the same. The Student Conduct Code may be found here[5].

### 2.1 Improper Uses

Brandman users cannot use the University's Information technology resources to transmit, receive, or store any information that is discriminatory, harassing, or defamatory in any way (e.g., sexually -explicit or racial messages, jokes or cartoons), or to violate the University's policy against harassment.

Brandman users must not use the University's information technology resources to copy, retrieve, forward, send, or trade secret, patent or other intellectual property, including, but not limited to, the installation or distribution of "pirated", including unauthorized peer-to-peer file sharing or other software products that are not appropriately licensed for use by University or copyrighted[3] materials unless the user has the author's permission. Violations may result in civil and criminal penalties, including fines and imprisonment.

Brandman users may not use any of the University's technology resources for any illegal purpose, violation of any University policy, in a manner contrary to the best interests of the University, in any way that discloses confidential or proprietary information of the University or third parties, or for personal or pecuniary gain.

The following activities are strictly prohibited, with no exceptions:

1. Violating the rights of any person or company protected by copyright, unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which University or the end user does not have an active license.

2. Accessing data, a server or an account for any purpose other than conducting University business, even if the user have an authorized access.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.

4. Introducing of malicious programs into the network or server (e.g., viruses, worms, trojan horses, e-mail bombs, ransomware, phishing or spear-phishing emails, etc.).

5. Revealing an assigned account password to others or allowing use of an account by others different than the authorized owner, either deliberately or

through failure to secure its access. System level and user level passwords must comply with the Information Technology Password Policy. This includes family and other household members when work/study is being done at home.

6. Using a University computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. Making fraudulent offers of products, items, or services originating from any University account.

8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless is part of the user duties and prior notification.

11. Executing any form of network monitoring which will intercept data not intended for the user’s host, unless this activity is a part of the user’s normal job/study duty.

12. Circumventing user’s authentication or security of any host, network or account.

13. Introducing honeypots, honeynets, or similar technology on the University network.

14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

16. Providing information about, or lists of, University employees to parties outside University, unless it has been authorized by department head.

17. Using, except as authorized in writing or by e-mail, by the University, Brandman University resources for compensated outside work, or profiting organizations not related to the University (except in connection with scholarly, creative or community service activities), or commercial or personal advertising.

18. Directing political campaigning and fundraising of any kind is considered an inappropriate use of Brandman University's technology resources.

19. Transferring or extending the privilege of using Brandman University technology resources provided by the University, to people or groups outside of the University.

20. Using another person's account, or giving his or her own password to another person for the purpose of gaining access to Brandman University technology resources. Users are responsible for the use or misuse of their own accounts. Users are responsible for safeguarding their account passwords. Account holders are responsible for all actions performed with their accounts.

21. Being able to read, alter or copy a file does not imply permission to read, alter, or copy that file.

22. Trying to bypass standard procedures, including attempting to discover another person's password, or to use an account for purposes for which it was not intended. Attempts to gain unauthorized access to machines via the network, to decrypt encrypted material, or to obtain privileges to which the user is not entitled are prohibited by public law. Attempts to circumvent data protection schemes, to discover security loopholes, or possession of software for such purposes by users are prohibited. Network vulnerability scanning to discover open services on computers inside or outside the Brandman network is prohibited except for use by the Information Technology personnel.

23. Intentionally interfering with the normal operation and delivery of services over the network.

No person must use or facilitate the use of any software on the University's computers that does not fall into at least one of the following categories:

a) It is in the public domain.
b) It is covered by an effective licensing agreement with the software author, authors, vendor or developer, whichever is applicable.
c) It has been donated to the University and a record of a bona-fide contribution exists.

d) It has been purchased by the University and a record of a bona-fide purchase exists.

e) It has been purchased by the user and a record of a bona-fide purchase exists and can be produced by the user upon demand.

f) It is being reviewed or demonstrated by the users, pursuant to permission given by the owner, in order to reach a decision about possible future purchase or request for contribution or licensing.

g) It has been written or developed by a Brandman University employee for the specific purpose of being used in the University's computer environment.

h) It is authorized by a University official with appropriate contractual signatory authority.

i) It has been copied in compliance with the published copyright and licensing agreements provided with the purchase of all software.

j) It is specifically authorized by the Information Technology Department. This includes the use of all Brandman University servers, including but not restricted to web servers, ftp servers, email servers, game servers and computers equipped with peer-to-peer file sharing software through which files are made available to other users.

   Authorized servers must not interfere with the performance of the network by consuming excessive amounts of resources.

### 2.2 Consequences of Misuse

The University reserves the right to restrict the use of its computing facilities and limit access to its networks when faced with evidence of violations of university policies or standards, contractual obligations, and federal, state or local laws. Violations of the law may be reported to the appropriate civic authorities.

Misuse of Brandman University technology may result in the loss of computing privileges and may require financial restitution to the University for losses incurred by the University. Misuse of Brandman University technology resources could also result in University disciplinary action and/or civil or criminal actions. Both unauthorized use of Brandman University technology resources and use of Brandman University technology resources for personal gain constitute theft under California law and will be prosecuted by the University.

Any actions which deter others from doing their work or which would be otherwise deemed malicious will result in the loss of access to the system and possible University disciplinary action and/or civil or criminal actions. Violations of this policy shall be referred to the appropriate University officials for disposition in accordance with the applicable policy governing the individual’s conduct University access to technology resources and social media.

Freedom of speech is central to the mission of higher education. Brandman University respects and encourages the exchange and debate of ideas, including electronic interchanges. However, all communications conducted on University computers or networks should be business-like, courteous and civil. The protection of confidential, sensitive, and proprietary information is of critical importance to the University; therefore it is essential that faculty, students and staff take steps to safeguard such information.

The University does not condone messages of hate, bigotry, violence or intimidation directed at any individual or group, or harassment of any kind. Acts of harassment and threats will be thoroughly investigated by University, and may be subject to review by state and federal enforcement agencies.

Postings by employees from a University email address to newsgroups, social media (Facebook, Twitter, Instagram etc.) should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of University unless posting is in the course of business duties.

### 2.3 User Passwords and Data Security

Most of the University's Technology resources can be accessed only by entering a password. Passwords are intended to prevent unauthorized access to information.

Passwords do not confer any right of privacy upon any user. Thus, even though users may maintain passwords for accessing Information technology resources, users must not expect that any information maintained on the University's technology resources, including text, electronic-mail and voicemail messages, may be maintained in private.

Regardless of available encryption methods or other security, users should understand even with the commitment to safeguard Brandman University's technology resources, it is impossible to eliminate all risk of breach; therefore, every effort should be made to secure data that is considered highly sensitive, confidential or personal.

All wireless traffic is presumed to be insecure and susceptible to unauthorized examination. Due to this lack of privacy, users should not use the wireless network to access critical and essential applications or transmit sensitive material and information, social security numbers or credit card information. Individuals assume full responsibility and accountability of wireless network communications. Brandman University will take precautions to minimize this exposure and will proactively introduce new technologies, when available, to secure and safeguard network traffic.

When connecting personally owned computers to Brandman University technology resources , the user of those computers must take steps to make sure that the computers are free from security vulnerabilities and viruses. In particular these computers must have operating systems that are supported by their manufacturers (e.g. Microsoft Windows OS and Apple OS/X) and must have antivirus software packages installed which are updated with the latest antivirus data files.

Users must download and install the latest operating system and application software security patches on their own personal devices. Security patches can be downloaded at no cost to the user. Brandman provides antivirus software to be used by faculty, staff and students free of charge.

Each user is ultimately responsible for his or her own backup of his or her own data using a computer if the data are not backed up on the shared folder.

**Users must not share their passwords and must not access coworker/student systems without express authorization.**

### 2.4 Data Collection by the University

The best way to guarantee the privacy of personal information is not to store or transmit it on University technology resources. To ensure that users understand the extent to which information is collected and stored, below are examples of information currently maintained by the University.

Although Brandman University does not make a practice of monitoring Brandman University e-mail, the University reserves the right to retrieve the contents of University-owned computers or Brandman University e-mail messages for legitimate reasons to comply with investigations of wrongful acts to respond to subpoenas.

Electronic mail is backed-up and archived.

The University expects that when users use the Internet or electronic mail during work/study hours, while on University premises, or remotely through the use of University computer equipment, they will do so in a responsible manner, and for work/study-related purposes only.

### 2.5 Telephone Use and Voicemail

Records are kept of all calls made from and to a given telephone extension.

### 2.6 Desktop Facsimile Use

Copies of all facsimile transmissions sent and received are maintained in the facsimile server.

### 2.7 Document Use

Each document stored on University computers has a history, which shows which users have accessed the document for any purpose.

### 2.8 Employees Personal Electronics Policy

Employees must devote their full time, energy and attention at work to their job responsibilities and duties. The University reserves the right to prohibit use of University technology resources for personal purposes, including access to internet radio services, video services and games.

### 2.9 Employees Use of University Property

Employees who misuse University property may be personally liable for replacing or fixing the item and may be subject to discipline, up to and including termination.

## 3. Policy Enforcement

### 3.1 Policy Enforcement, Auditing, Reporting

This section states what a violation is and the penalties for non-adhering to any security policies. The violation of a policy usually implies an adverse action that needs to be enforced.

#### 3.1.1 Policy Violation

A Policy violation is any act that fails to follow to existing statements contained in the policy itself. The Brandman University (BU) security policies describes behaviors methods, security configurations, controls and settings that conform to the security posture of the BU infrastructure.

Brandman University technology users should keep in mind that many people use the Brandman University network for daily work. Behaviors that inhibit or have the potential to inhibit the ability of others to utilize shared computing resources are considered policy violations. Such behaviors include but are not limited to:

1. Exceeding limits for resource usage (e.g. disk space, bandwidth, and CPU time).
2. Providing access to Brandman resources to individuals outside the university community.

#### 3.1.2 Penalties for Non-Compliance

Each violation or failure to enforce any policy by anyone, will be reported in writing by the Information Security Team as a security incident. The responsible party's supervisor, unless overridden by the Department Head or Human Resources, is responsible for determining the penalties.

### 3.2 Control and Maintenance

This section describes the conditions and process in which the policy is reviewed.

#### 3.2.1 Update

Policies are reviewed and modified as needed, or when major changes in the Brandman University Information Technology, systems and network entail different security requirements.

## 4. Related Standards, Policies and Processes

Higher Education Opportunity Act – 2008, Internet, June 25, 2010 at:
https://ed.gov/policy/highered/leg/hea08/index.html

## Appendix A – References and Revision History

1) Port Scanner, Internet, 26 January 2017, at:
https://en.wikipedia.org/wiki/Port_scanner

2) Honeypot, Internet, 28 January 2017 at:
https://en.wikipedia.org/wiki/Honeypot_(computing)

3) US Copyright Office, Internet, February 14, 2017 at:
https://www.copyright.gov/

4) SANS Acceptable Use Policy, Internet, June 2014, at:
https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy

5) Student Conduct Code, Internet, July, 06-2016, at:
https://www.brandman.edu/files/documents/enrollment-student-affairs-documents/Student-Conduct-Code-2016-17-Revised.pdf

## Revision History

| Version | Date | Author(s) | Comments |
|---|---|---|---|
| 1.0 | 03/29/2017 | Emilio Valente (ISO) | Initial Draft (by the ISO) |