Vanderbilt University Information Technology Resources Acceptable Use Policy

I. Introduction

The mission of Vanderbilt University is to be a center of scholarly research, informed and creative teaching, and service to the community and society at large. The university upholds the highest standards and is a leader in the quest for new knowledge through scholarship, dissemination of knowledge through teaching and outreach, and creative experimentation of ideas and concepts. In pursuit of these goals, Vanderbilt values most highly intellectual freedom that supports open inquiry, and equality, compassion, and excellence in all endeavors.

To achieve its mission, the university applies substantial financial and personnel assets toward operating a reliable, available, and secure network-computing infrastructure. The mass adoption of digital technologies in the everyday lives of members of our community requires that Vanderbilt establish clear policies that guide how community members may use the university's information technology resources. This Acceptable Use Policy (AUP) communicates the respective policies associated with our role in the Vanderbilt community as students, faculty, staff or other authorized users.

The guiding purpose of the AUP is to ensure that the university's information technology resources are used to promote the core mission of Vanderbilt in education, research and scholarship, patient care, and service, either directly or through the various administrative entities and services that enable Vanderbilt's core mission. To that end, the policy has the following goals:

A. First and foremost, that information technology resources are used for their intended purposes;

B. That the use of information technology resources is consistent with the principles and values that govern use of other university facilities and services; and

C. That the integrity, reliability, availability and performance of information technology resources are protected

II. Scope

This policy applies to all Vanderbilt University students, faculty and staff and to all others granted use of Vanderbilt's information technology (IT) resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and communication facilities owned, leased, operated, or contracted for by Vanderbilt University. Information technology resources include but are not limited to Vanderbilt's Internet 1, Internet 2, private networks, telephone, fax, voice mail, electronic mail, instant messaging, electronic collaboration, content management, or other applications that attach, utilize, or otherwise interface with

Vanderbilt's data and voice network computing infrastructure. Electronic communications include but are not limited to any information–data, text, graphics, audio, video, or other artifact–that can be sent or received via an electronic system or manipulated or transferred via the network computing infrastructure or an attached device or peripheral.

III. Policies

A. PRIVACY, INTEGRITY AND OPERATIONAL SECURITY

The privacy of all users and the integrity and operational security of Vanderbilt's information technology system must be respected by all. Vanderbilt's IT resources must not be used by anyone to gain or attempt to gain unauthorized access to private information, even if that information is not securely protected or is otherwise available. The fact that an individual account and its data may be unprotected does not confer either an ethical or legal right to access it.

1. Investigations of misuse, unauthorized use, or illegal activity, compliance with federal, state or local laws or regulations, as well as routine or emergency maintenance of the IT system, may require observation of electronic information by appropriate and authorized university officials, employees, or their authorized agents. Such activities are not in violation of this principle so long as these activities are conducted by authorized individuals on behalf of Vanderbilt University and are governed by professional IT forensic protocols. Vanderbilt uses automated systems to monitor data transmissions entering and leaving the Vanderbilt networks to detect the presence of viruses, malicious software, or privileged information.

2. Unauthorized access to private information constitutes a violation of this policy, and may result in disciplinary actions under the Faculty Manual, Student Handbook, HR policies, or other applicable policy statements. Violation of this principle may also constitute a violation of state or federal law.

B. USE

Use of Vanderbilt's network computing and electronic communications infrastructure comes with certain responsibilities and obligations.

1. Unlawful Use

Tennessee and federal laws provide for civil and criminal penalties for violations of the law of systems use. Examples of unlawful actions include, but are not limited to, defamatory remarks, destruction of Vanderbilt University data or equipment, unauthorized copying of copyrighted material and the transportation of obscene materials across state lines. Any use of Vanderbilt network computing assets by anyone in the organization that violates state, federal, or local laws is prohibited.

2. Violation of Institutional Policies

Vanderbilt University's academic departments, clinical operations, and administrative areas maintain policies that govern and inform our day-to-day lives in the conduct of our Vanderbilt experience. Any use of Vanderbilt network computing assets that violates applicable institutional policies is prohibited.

3. Violation of Student Honor and Conduct Codes

Vanderbilt University maintains high standards for its students and various codes and policies govern and inform a student's day-to-day life in the conduct of his or her Vanderbilt experience. Students are prohibited from using the Vanderbilt network computing assets for activities that violate the conduct code, the honor code, or other policies and regulations delineated by The Student Handbook.

C. FIDUCIARY RESPONSIBILITIES

1. Vanderbilt Community Members

Members of the Vanderbilt community possess a great personal responsibility to themselves and to other community members to utilize technology while maintaining their fiduciary responsibilities. These responsibilities include, but are not limited to:

a. Being responsible for the security of one's personal information

b. Protecting personal and private information of others

c. Taking care to minimize risks of various undesirable events, such as disclosure of sensitive personal information, identify theft, and even threats to personal safety when using Vanderbilt information technology assets.

2. Information Technology Professionals

Vanderbilt IT personnel are granted elevated or privileged access to Vanderbilt University's information and information systems. This privileged access places the Vanderbilt IT professional in a higher level of trust. To maintain this level of trust, Vanderbilt IT professionals must develop, maintain, and continually enhance their skills and abilities on behalf of those they serve. IT professionals employed by Vanderbilt University must strive to be trusted and highly skilled custodians through:

a. Preserving confidentiality

b. Protecting data and information integrity

c. Establishing and maintaining availability of information systems

d. Educating those around them about IT and social risks related to information systems

e. Enhancing and maintaining technical skills

f. Demonstrating an understanding of the areas they serve

D. INTELLECTUAL PROPERTY

At the heart of any academic or research endeavor resides the concept of intellectual property. All copyrighted information (text, images, icons, programs, video, audio, etc.) retrieved from computer or network resources must be used in compliance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of digital information is subject to the same sanctions as apply to plagiarism in any other media. Acquiring or sharing copyrighted materials without obtaining the appropriate licenses or permissions may be unlawful.

E. PUBLICATION OR DISTRIBUTION OF UNAUTHORIZED RECORDINGS, PHOTOS, IMAGES, TEXT OR VIDEO

With the availability of low cost cameras, smart phones, and consumer electronics, it is possible for someone to acquire voice, video images, still images, multimedia, or text in non-public situations without the knowledge or consent of all parties. Vanderbilt network computing assets must not be used by anyone in the organization to publish or distribute this type of material without the expressed consent of all involved parties.

F. RIGHT TO COPY AND INSPECT FOR LEGAL AND UNIVERSITY PROCESS

Vanderbilt University is committed to protecting the privacy of faculty, students, staff, patients, and other users of its IT resources, and their electronic communications. However, because Vanderbilt operates subject to compliance with various federal and state laws and regulations and must be able to enforce its own policies, Vanderbilt must occasionally inspect, preserve and produce records to fulfill legal obligations and to carry out internal investigations. Vanderbilt University reserves the right to obtain copy and convey to outside persons any records or electronic transactions completed using Vanderbilt University information systems in the event it is required by law or institutional policy to do so. Vanderbilt University may also in its reasonable discretion, when circumstances require, obtain and review any records relevant to an internal investigation concerning compliance with Vanderbilt University rules or policies applicable to students, faculty, staff, or to all others granted use of Vanderbilt's information technology resources. Users therefore should not expect that records created, stored or communicated with Vanderbilt information technology or in the conduct of Vanderbilt's business will necessarily be private. Vanderbilt University reserves its right to any work product generated in the conduct of its business.

G. LOCALLY SPECIFIC POLICIES

Individual units within the University may create additional policies for information resources under their control. These policies may include additional detail, guidelines and further restrictions but must be consistent with principles stated in this policy document. Individual units adopting more specific policies are responsible for establishing, publicizing and enforcing such

policies, as well as any rules governing the authorized and appropriate use of equipment for which those units are responsible.

IV. Disclosures

A. All members of the Vanderbilt University community are given notice of this policy by virtue of its publication and are subject to it on the same basis. Ignorance of this policy does not relieve any user of his or her responsibilities under the policy. All users are expected to familiarize themselves with the contents of this policy and act in conformance with these principles regarding any use of the University's IT resources.

B. Due to the rapid nature of change in both information technologies and their applications, the University may amend this policy whenever deemed necessary or appropriate. Users are encouraged to periodically review this policy in order to understand their rights and responsibilities under it.