Acceptable Use Policy

1. Overview

The intentions of Hood College in publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the College's established culture of openness, trust, and integrity. The College is committed to protecting all authorized computer users and the College from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts, electronic mail, web browsing, and data transfers, are the property of Hood College. These systems are to be used for business purposes in serving the interests of the College, and of all authorized computer users in the course of normal operations.

Effective computer security is a team effort involving the participation and support of every authorized computer user at Hood College who deals with information and/or information systems. It is the responsibility of every authorized computer user to know these guidelines, and to conduct their activities accordingly.

The College's information technology resources are provided with the understanding that the entire College community will use them in a spirit of mutual cooperation. Resources are limited and must be shared.

2. Purpose

The purpose of this policy is to outline the acceptable use of all computer equipment at Hood College. These rules are in place to protect all authorized computer users and the College. Inappropriate use exposes the College to systemic risks including, but not limited to, cyberattacks, compromised network systems, disabled technology services, and legal issues.

3. Scope

This policy applies to the use of information, computing devices, and network resources to conduct Hood College business or interact with internal networks and business systems, whether owned or leased by Hood College or by the College's authorized computer users. All authorized computer users at Hood College are responsible for exercising good judgment regarding appropriate use of information,

computing devices, and network resources in accordance with College policies and standards, local Maryland law, and regulation. Exceptions to this policy are documented in Section 5.2

4. Policy

4.1 General Use and Ownership

4.1.1 Proprietary information stored on computing devices whether owned or leased by Hood College remains the sole property of Hood College. You must ensure through legal or technical means that proprietary information is protected in accordance with all Hood College's policies and standards.

4.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Hood College proprietary information.

4.1.3 You may access, use, or share Hood College proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Authorized computer users are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, authorized computer users should be guided by departmental policies on personal use, and if there is any uncertainty, users should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within Hood College may monitor equipment, systems, and network traffic at any time.

4.1.6 Hood College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy and other legal statutes.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the College's *Acceptable Use Policy*.

4.2.2 System-level and user-level passwords must comply with the College's *Minimum Password Complexity Requirements*.

4.2.3 Providing access for another individual, either deliberately, or through failure to secure your own access, is prohibited.

4.2.4 All authorized computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 30 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.5 Postings by authorized computer users from a Hood College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Hood College, unless posting is in the course of business duties.

4.2.6 Employees must use extreme caution when opening e-mail attachments received from unknown senders as they may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Certain authorized computer users may be exempted from these restrictions during the course of their legitimate job responsibilities. For example, an IT staff member may have a need to disable the network access to a host if that host is disrupting production services or is compromised.

Under no circumstances is an authorized computer user of Hood College authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing College-owned or leased resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Hood College.

2. 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 Hood College or the end user does not have an active license is strictly prohibited.

3. Attempting to access data, computer systems and/or networks on or off campus for which there is no authorization, or all other forms of "hacking" activity.

4. Introduction of malicious programs into the College's network or server farm (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Accessing or using a protected computer account assigned to another person, or sharing a password to a protected account with another person. This includes family and other household members.

6. Using any computer network or computing resources to access or transmit material or participate in activities that include, but are not limited to, obscenity, child pornography, defamation, solicitations, and theft.

7. Using any computer network or service for a purpose other than scholarship, research, learning, legal entertainment, or limited personal communications. For example, utilizing the College's resources on behalf of any commercial, political, religious, or other non-academic organization is prohibited.

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

9. Causing or effecting security breaches or disruptions of network communication. For example, the installation and running of any server service, or device which hosts such service, without prior authorization from the College's Administration and Information Technology. Services include, but are not limited to, e-mail (SMTP), Web and secure Web (HTTP and HTTPS), FTP, DHCP, IRC, ICQ, P2P, WINS, DNS, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning unless prior notification and permission to Information Technology is made and approved.

11. Executing any form of network monitoring that will intercept data unless this activity is a part of normal job duties.

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

13. Introducing honeypots, honeynets, or similar technology on the Hood College network or server farm.

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

15. Providing information about, or lists of, Hood College employees to parties outside of Hood College.

16. Misusing, using excessively, or abusing computer equipment, software, peripherals, or supplies.

4.3.2 Email and Communication Activities

The following activities are strictly prohibited, with no exceptions:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging of email header information. For example, forging messages or otherwise altering electronic communications for the purpose of trying to hide the identity of the user or to impersonate another person.
4. Solicitation of email for any other email address, other than that of the sender's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type, offensive or obscene language communications.
6. Use of unsolicited email originating from within Hood College's networks to other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Hood College or connected via Hood College's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 Blogging and Social Media

The following activities are strictly prohibited, with no exceptions:

1. Blogging by authorized computer users, whether using Hood College's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of Hood College's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Hood College's policy, is not detrimental to Hood College's best interests, and does not interfere with regular work duties. Blogging from Hood College's systems is also subject to monitoring.

2. With respect to confidential information, Hood College's human resource policies also apply to blogging. As such, authorized computer users are prohibited from revealing any confidential or proprietary information, trade secrets, or any other material covered by these policies when engaged in blogging.

3. Authorized computer users shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Hood College and/or any of its authorized computer users. Authorized computer users are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging or otherwise engaging in any conduct prohibited by Hood College's human resource policies.

4. Authorized computer users may also not attribute personal statements, opinions, or beliefs to Hood College when engaged in blogging. If an authorized computer user is expressing his or her beliefs and/or opinions in blogs, the authorized computer user may not, expressly or implicitly, represent themselves as a user or representative of Hood College. Authorized computer users assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Hood College's trademarks, logos and any other Hood College intellectual property may also not be used in connection with any blogging activity.

5. Policy Compliance

5.1 Copyright Infringement Notice

No one is authorized to perform, exhibit, reproduce, transmit or otherwise distribute copies of copyrighted motion pictures, sound files or other copyrighted materials. Doing so constitutes copyright infringement under the Copyright Act,

Title 17, United States Code Section 106(3). This conduct may also violate the laws of other countries, international law and/or treaty obligations.

5.2 Exceptions

Any exception to Hood College's acceptable use policy must be approved by Information Technology in advance of any request.

5.3 Non-Compliance

Individuals who violate this policy will be subject to disciplinary action or referral to law enforcement authorities. Information Technology personnel are authorized to monitor suspected violations and to examine items stored on any College storage medium by individuals suspected of violating this policy.

You must accept the Hood College Acceptable Use Policy to connect to and use the College's network or any information technology resource.