This document details the acceptable use and ethics policies covering the proper utilization of the computers, networks, and related services at Oakwood University. These policies have been developed to ensure a quality computing environment at Oakwood University that furthers the academic, research, and service mission of the University. This environment requires equitable resource distribution, computer and network availability, personal privacy, and data integrity. Achieving these goals requires that everyone in the University community cooperate and adhere to these policies.

Computing resources are valuable, and their abuse can have a far-reaching negative impact. Computer abuse affects everyone who uses computing facilities. The same moral and ethical behavior that applies in the non-computing environment applies in the computing environment.

In providing computing resources to its users (faculty, staff and students), Oakwood University has outlined the following policies regarding usage. In addition to these policies, many departments and computer labs have their own policies regarding access, eligibility for using computing resources, and other matters.

Computer users are expected to familiarize themselves with all policies regarding computer usage.
COPYRIGHT AND COMPLIANCE POLICIES

These policies apply to all Oakwood University faculty, staff, and student users of commercial software and documentation which is available through Oakwood University. This includes all computer software, regardless of how the software licenses are acquired (lease, purchase, etc.).

1. The software in use by Oakwood University contains proprietary and confidential information. Proprietary information includes, but is not limited to trade secrets, programs, technical know-how, formulas, specifications, methods and procedures of operation and licensed documentation.

2. Users shall not copy, modify, trade, unlock, reverse, compile, redistribute, or remove any software, in whole or in part, available at Oakwood University which has a copyright protection clause associated with the licensed software, except to the extent permitted by the terms of the license agreement.

3. According to the United States Copyright Law, illegal reproduction of software can be subject to civil damages of $100,000 and criminal penalties, including fines and imprisonment. Unauthorized copying is by law theft. Therefore, Oakwood University does not condone the unauthorized copying of software, including programs, applications, and databases.

4. Computer software available at Oakwood University may not be used, copied, or adapted in any way for the purpose of personal gain or for use in any illegal activities. The willful damage, alteration, redistribution, or removal of any software licensed by Oakwood University shall be treated as an act of theft.

5. Failure to observe the above copyright policies and/or license agreements may result in loss of computer privileges and/or possible legal action by the software owner.
INDIVIDUAL RIGHTS

Freedom of expression is a constitutional right afforded to all members of the community, and existing University policies apply equally to computerized expression, subject to the policy "Authorized User" in this section of the Administrative Policy Manual. While Oakwood University has taken steps to halt potentially offensive material or material which is considered unacceptable by University standards, computer and network users should realize that there are services available on the Internet which may be considered offensive to some. With this in mind, users take responsibility for their own navigation of the network.

SAFETY AND FREEDOM FROM HARASSMENT

While Oakwood University cannot control harassment or unsolicited contact on the network, those who believe they have been harassed should follow standard University procedures and bring such violations to the attention of the University departmental heads or vice presidents.
Users of Oakwood University computer equipment are expected to understand these policies and abide by them. These policies are widely distributed and easily accessible, so lack of knowledge is not an excuse for failure to observe. Questions regarding these policies can be directed to the info@oakwood.edu link on the University’s Web site. Disregard for these policies may result in disciplinary actions as set forth in the policy "Sanctions" in this section of the Policy Manual.

**Morals and Ethics**

Users are expected to respect the right to privacy of other individuals on the network. Users should not go browsing around in someone’s files even if security permissions permit. This is analogous to condoning someone rifling around in another’s house simply because the person forgot to lock the door. It is expected that explicit permission from the owner of the files is obtained before they are accessed. Users are expected to respect the right of freedom of expression of other individuals on the network.

**Expected Behaviors**

This section details some guidelines relating to computer-based activities. Oakwood University computer users are expected to read sign-on messages and system news for specific information such as system changes, policies, and scheduled downtime. Additionally, valuable information is available in the Oakwood University’s Website. System and network administrators may find it necessary to contact users regarding policy issues. If repeated attempts to contact an individual are unsuccessful, the system or network administrator may be forced to temporarily deactivate the account simply to compel the owner to make return contact.

**Unauthorized Monitoring**

Users are not permitted to use computers and networks to monitor or attempt to monitor electronic transmissions.

**Disruption of Service**

Deliberate attempts to disrupt the operation or degrade the performance of computers or networks are prohibited.

**Distribution of Resources**

Users should not circumvent or attempt to circumvent any policies or procedures that have been established to ensure equitable resource distribution in the University’s shared computing environment. For example, users must not deliberately circumvent the modem inactivity timer.

**Mass Electronic Mailings**

Mass electronic mailings are not permitted from the campus. All campus-wide announcements must be sent to the Public Relations Dept. or the Technology Department for approval, after which the announcement(s) will be sent out. Due to high demands on the e-mail resources, use of the University’s e-mail system for mass mailing is discouraged.
**Game Playing**

The policy regarding game playing on Oakwood University computers and networks is established by the department responsible for the computers and networks in question. However, no department should permit game playing to interfere with normal University business.

**Business use**

There is to be no use of Oakwood University computers or networks for non-Oakwood University business purposes or non-Oakwood University related employment.

**Individual Rights**

Most of the labs, computer workstations, and software are available for use on a first-come, first-served basis unless reserved for a class or workshop.

**Computer hardware and software**

Users should not tamper with, alter the settings, move, or reconfigure the hardware (computers, printers, terminals, etc.) or software of any equipment, whether connected to the network or stand-alone. Users should not attempt to perform any procedure that may crash the system(s).
Violators of this policy may be subject to one or more of the following sanctions which can be imposed by the department responsible for the computers and networks on which the violation occurred:

- Admonition
- Temporary or permanent suspension of computer privileges
- Temporary or permanent suspension of lab privileges

Additional sanctions, such as University suspension and employee action, may also apply as outlined in the Student Handbook and the Staff Handbook.

**Legal Restraints**

Users of Oakwood University computing facilities are expected to abide by state and federal laws that apply to the usage of computers. These laws exist to "establish certain acts involving computer fraud or abuse as crimes punishable by defined fines or imprisonment or both".

**Appeals**

Appeals to sanctions should be handled through the existing University grievance and appeals policy for both employees and students.
APPROPRIATE COMPUTER ACCOUNT USAGE

Accounts General

Accounts are provided for academic research and instruction, electronic mail, Internet access, and for activities related to the mission of Oakwood University. Each account represents an allocation of a scarce computing resource and as such is monitored by Oakwood University administrators for appropriate use. Each account is assigned for the sole use of a single user. Sharing of accounts is prohibited. The user for whom the account was created is responsible for the security of the account and all actions associated with the use of the account. Accounts may be revoked if the account is found to have been used for activities that violate any portion of this policy, the owner of the account has been found violating any portion of this policy, or the owner of the account is no longer enrolled or employed by Oakwood University. Activation of an account on an Oakwood University Host computer constitutes an agreement stating that the user understands and will abide by all policies regarding the use of the Oakwood University network.

Inactive Accounts

Active accounts are changed to the inactive state prior to deletion. The inactive state is an intermediate step between an active account and a deleted account. In the inactive state, all host access is denied and electronic mail addressed to the account is returned to the sender. Some files may be archived and deleted. An account may be reactivated from the inactive state up until the time that it is actually deleted. When an account is deleted, the username is considered unused and all files in the user's home directory are deleted. Electronic mail sent to the user is rejected.

Restricted Accounts

On occasion an account may be temporarily restricted. There are many reasons why this may occur ranging from misuse of network resources, to important information that needs to be given to the user before they attempt to login again. Upon attempting to log in, the user sees a short message to the effect of "Please see the System Administrator" and the user is immediately logged out. In most cases, once a meeting with the System Administrator is completed, the account is reinstated.

Sharing Accounts

Any abusive activities initiated from an account are traced back to the account owner and the account owner is held accountable. The behavior of someone with whom you have shared your account becomes your responsibility. If the abuse is such that network privileges are terminated, it is the account owner (you) who suffers. Therefore, it is the policy of Oakwood University that User Names are not to be shared. Each Oakwood University User Name has only one Oakwood University authorized user. If users
wish to share information or otherwise collaborate in a group, then the users shall use appropriate file permissions combined with appropriate group membership to share data.

## SELECTING A PASSWORD

Perhaps the most vulnerable part of any computer system is the account password. Any computer system, no matter how secure it is from network or dial-up attack, Trojan horse programs, and so on, can be fully exploited by intruders who can gain access via a poorly chosen password. It is important to select a password that is not easily guessed and to not share the password with ANYONE.

## ABUSE OF COMPUTING RESOURCES

### Theft and Vandalism

Oakwood University computing resources are shared by all network users on a fair and equitable basis. It is the responsibility of Oakwood University not only to provide these computing resources but also to insure that the rights of users are not infringed upon by the abuse of another. Therefore, Oakwood University utilizes every means available to detect, restrict and/or prosecute individuals responsible for the abuse of computing resources. This section serves to provide specific examples of the types of abuse not tolerated. This list is by no means complete and is subject to change without notice as new ways of abusing resources are discovered. Penalties for abuse of network resources include but are not limited to temporary restriction of network privileges, permanent restriction of network privileges, and criminal prosecution.

The appropriate Oakwood University authorities handle theft and vandalism of Oakwood University Computing resources. Oakwood University pursues and supports criminal prosecution of individuals suspected of theft and/or vandalism.

### Worms and Viruses

Anyone attempting to write ftp or knowingly proliferate worms or viruses of any size, shape, or form will be remanded for criminal prosecution (and will lose their computing privileges).

### Use of .rhosts Files

Through the use of .rhosts files users can allow others access to their account without the knowledge of a password. This is not only a breach of security but violates the policy on account sharing as well. Use of .rhosts files is prohibited. When found, they will be deleted. Repeat offenders will lose their computing privileges.

### Transferring Files

Using ftp to transfer files to or from remote sites, which violate the policies of the remote site, is prohibited. In particular, transferring files which are large, contain material offensive to either site, contain information to be used for the financial gain of any party, or contain monetary or sexual solicitations is prohibited. Restrictions pertaining to the duplication of copyrighted materials also apply.

### Games Network Games Policy

A computer network like Oakwood University’s is a powerful tool, for both recreational and non-recreational applications. For the purposes of this document, all recreational uses of the network,
including but not limited to network strategy games, action games, and chat programs, are described as "games".

In general, most games are permitted on the Oakwood University network. Games played on the network must comply with the same rules as all other network applications and must pose no risk of interference with other network operations. They must also comply with all other Oakwood University policies, including ethics policies. Non-game network traffic has priority at all times. Games that interfere with non-game traffic, even if run within network bandwidth limitations, are prohibited from the Oakwood University network.

Some games are banned from the Oakwood University network because they have already been found to interfere with network operations.

In the event of a conflict between this policy and the policies of individual offices, labs, and computing facilities on campus, the most restrictive takes precedence. For example, if a lab says, "no games", no games are allowed in that lab.
GENERAL

Social networking Web sites or on-line communities, such as My Space, Facebook, and Flickr are being used increasingly by students to communicate with each other, and by universities to post events and profiles to reach students.

As part of the Oakwood University commitment to building a community in which all persons can work together in an atmosphere free of all forms of harassment, exploitation, or intimidation, when using University electronic resources to access on-line social networks, University community members (faculty, staff, students and others) are expected to act with honesty, integrity, and respect for the rights, privileges, privacy, sensibilities, and property of others. By doing so, individuals will be abiding by applicable laws, including copyright law, University policy, and the University’s Statement of Ethical Values.

POSTING

University Business Use

Only University employees authorized by their departments may use social networking Web sites to conduct University business. If authorized and in keeping with University policy, an employee may post on a social network profile: the University’s name, a University email address or University telephone number for contact purposes, or post official department information, resources, calendars, and events. For example a faculty or staff is charged with student outreach and education within their job description. The department may authorize these employees to use an on-line social network site to communicate with students and post University resources.

Personal Use

Consistent with the Oakwood University policy on Electronic Communications, personal use of University electronic resources to access social networking sites is to be limited to incidental use. Incidental use must not interfere with an individual’s performance of his/her assigned job responsibilities or someone else’s job performance or compromise the functionality of the department or campus network.

Individuals or groups within the University community are not permitted to present personal opinions in ways that imply endorsement by the University. If posted material may reasonably be construed as implying the support, endorsement, or opposition of the University with regard to any personal statements, including opinions or views on any issue, the material shall be accompanied by a disclaimer: an explicit statement that the individual is speaking for himself or herself and not as a representative of the University or any of its offices or units. An example of a disclaimer is as follows:
• **The contents, including all opinions and views expressed, in my profile [or on my page] are entirely personal and do not necessarily represent the opinions or views of anyone else, including other employees in my department or at the Oakwood University. My department and the Oakwood University have not approved and are not responsible for the material contained in this profile [or on this page].**

The University’s name, University telephone numbers, University email addresses, and University images are not to be posted on social network profiles for academic and staff employees for personal purposes. However, a faculty or staff employee, or student government officer, or registered campus organization may use their University title for identification purposes. If the use of the title might imply endorsement, support or opposition of the University with regard to any personal statements, including opinions or views on any issue, an explicit disclaimer must appear proximate to the material. See disclaimer above.

**Malevolent**

The malicious use of online social networks, including derogatory language; demeaning statements about or threats to any third party; incriminating photos or statements depicting hazing, sexual harassment, vandalism, stalking, underage drinking, illegal drug use, or any other inappropriate behavior, will be subject to disciplinary actions.

**RISKS – SPAM, SPYWARE, AND VIRUSES**

Many social networking sites collect profile information for advertising (SPAM) targeted at individuals with particular affiliations and interests. Use of the sites may increase SPAM to your email account. In addition, from the social networking sites or links on social networking sites, your machine or network may be exposed to spyware and viruses that may damage your operating system, capture data, or otherwise compromise your privacy, your computer and the campus network, as well as affect others with whom you communicate.

**MONITORING**

Oakwood University doesn’t routinely monitor social networking sites, however, as with other electronic resources, University systems administrators may perform activities necessary to ensure the integrity, functionality and security of the University’s electronic resources. (UC Electronic Communications Policy, Section IV) However, other employers, organizations, and individuals do monitor and share information they find on social networking Web sites. Posted information is public information.

**INVESTIGATIONS**

In response to concerns or complaints or information provided by individuals, University administrators may look up profiles on social networking sites and may use the information in informal or formal proceedings. In addition, the University has no control over how other employers, organizations, or individuals may use information they find on social networking Web sites.
AUTHORIZED USERS

Individuals who have been granted and hold an active and authorized administrative account on an Oakwood University computer or network and abide by this policy are considered authorized users.

AUTHORIZED USE

Authorized use is predicated on access by an authorized user. Authorized use is that which is consistent with the academic, research, and service goals of this institution and falls within the guidelines of this policy and the policy of the Board of Trustees, which states that property owned by the institution shall be used only for institutional purposes. The following are guidelines regarding authorized use.

1. Computer accounts are for the sole use of the person to whom they are issued. The owner assumes all responsibility for the usage of the account. Sharing of accounts is prohibited.

2. It is recommended that student workers who use the computers use an account with a generic username (e.g., ADMSTUDENT for admissions student; REGSTUDENT for records student; FINSTU for financial aid student; FISSTUDENT for fiscal student, etc.).

3. Students should work only in the assigned account as stated above and not in the accounts of their supervisor or any other user.

4. Users should not attempt to access the administrative system outside of the office in which they work and should not access the system at all upon termination, resignation, or transfer to another department.

5. It is the responsibility of the user’s supervisor to notify the director of the Administrative Systems when an employee resigns or is transferred or terminated so that appropriate precautions can be taken for protection of the department’s data. The account of the user will be immediately disabled to protect against tampering and/or sabotage.

6. Users should not access or attempt to access another department’s data on the administrative system when they are no longer employed by that department without proper prior authorization from the department.

7. No institutionally owned computing resource should be used for commercial purposes or personal gain.

8. Microsoft Office Suite have been identified as the preferred software packages for support by the Administrative Systems.
PRIVACY

The computing professionals at Oakwood University are committed to preserving the privacy of each authorized user of the computer systems and exercise every effort to ensure that computers and electronic devices are not used to circumvent this. However, it is impossible to guarantee such privacy, and there are several specific issues that users must be aware of. Electronic mail messages are not secure and therefore should not be assumed to be private. Also, despite best efforts to prevent it, a determined person could gain unauthorized access to stored data and thus violate users’ privacy. Finally, in the process of performing normal systems/network management and auditing functions, it may be necessary to view user’s files or confidential information. However, system, network, and application administrators are bound by both professional ethics as well as job requirements to respect the privacy of those involved and not disclosure of information obtained in this manner.

GUIDELINES FOR PASSWORD SELECTION AND USAGE

Users should

1. Choose passwords that contain at least eight characters, with a minimum of 4 complex characters (e.g. Uu#&). Adequate length makes passwords more secure. Users should include both letters and numbers for an even more secure password.

2. Not share passwords with anyone, and not log on while someone can observe the password being entered. Users should not write or display a password where it can be seen.

3. Contact the Computer Center if they forget their password or suspect that a breach of security has occurred.

For administrative users:

1. The system will notify users of the number of tailed log-in attempts after they log on to the system. If this number seems excessive, users should report it to the Computer Center. The system allows for three unsuccessful log-in attempts within a specified amount of time. After that the username under suspicion will not be allowed to log in until a specified amount of time set by the system has expired.

2. The system will prompt administrative users to change their password every semester. The system will guide the user through the process. The system will not accept previously used passwords.

4. All MyOakwood users must use an oakwood.edu email to receive their forgotten password.

5. All Administrative Systems support must be entered into the Track-It system.
WEBSITE POLICIES AND PROCEDURES

Purpose

The Oakwood University’s website serves three major purposes. The first is to attract prospective students to Oakwood University. The second is to give students at Oakwood access to information about courses, financial aid, schedules, the registrar, and other areas to assist students with important questions they might have during their University career at Oakwood. The third purpose is to provide information to faculty, staff, students, parents, benefactors, alumni, and friends to keep them up to date on events and information happening at the University.

Scope

The scope of this policy covers the website that can be found at http://www.oakwood.edu. This would include all sub-domains including: my.oakwood.edu, d2l.oakwood.edu, etc.

Policies

1. The information on the website will not violate any individual’s rights to privacy. The University will not place any private information about faculty, staff or students on the website.

2. Personal E-mail addresses, phone numbers, personal data, addresses, and the like should not be placed on the web site unless an individual submits a written request to have this information published and signs a waiver.

3. The Webmaster will hold waivers and request forms until the information is permanently removed from the website. At any time the individual may submit a written request to the Webmaster to have his/her information removed from the web site. All federal, state, and local laws regarding privacy will be followed.

4. The use of images, recorded sounds, recorded video, copyrighted materials, trade secrets and trade markets is subject to legal restriction.

5. No one may use photographs, video clips, sound clips, or material which may be subject to copyright, trademark or trade secret restrictions without written permission of all parties involved.

6. No faculty, staff, or students of the University may use the University seal, pictures, or any other copyright materials without permission of the University. Anyone violating copyrighting laws may be punished in accordance with federal, state, and local laws.

7. Any website that violates the University’s web site policies will be removed from the server immediately.
8. Any person violating federal, state, or local laws will be held responsible for their actions.

9. Anyone violating the University’s rules of conduct or ethics, located in the University Handbook, is subject to disciplinary action in accordance with University policy.

Procedures

1. The official method of submitting written request for all web functionality must be submitted through Track-It. (Oakwood’s Ticket/solution management system)

2. To get a site on the server, a faculty, staff, and/or student must complete and sign a request form and submit it to the Webmaster.

3. Users must also submit a sample web site that demonstrates the faculty, staff, or student’s competence in using HTML and in web design. This may be submitting on a CD, DVD, and USB drive or by indicating a website containing the faculty, staff, or student’s work.

4. If the faculty, staff or student does not know how to create their own site, a meeting will be scheduled with a web consultant from the Oakwood University web team who will provide assistance in the design the site.

5. To request a site on the Oakwood University’s web server, the faculty, staff, or student must agree to the following policies and procedures:
   - The faculty, staff, student’s web site must be created with one of the templates maintained by the Webmaster.
   - Templates will have embedded office links and graphics to maintain institutional consistency.
   - The respective faculty, staff, or student must insure that pages are updated and current.
   - The faculty, staff or students website must be University related.
   - Web sites may not contain personal material or links to personal sites on the web.
   - The web sites may not be used for personal or financial gain.
   - No CGI, Perl or plug-in will be permitted.
   - Images used on the web site are to be jpegs (use only at low compression), Gifs (used only at 72 dpi and saved at 8 bit), or PNGs (used at 8 bit or 24 bit).
   - The faculty, staff, or student must make sure that all pages work with Internet Explorer.
ELECTRONIC MAIL POLICIES

1. E-mail accounts are for the sole use of the person to whom they are issued. The owner assumes all responsibility for the usage of the account. Sharing of accounts is prohibited.

2. E-mail username and password should never be given out to anyone, not even to the email administrator.

3. Users should not fill-out forms requesting for confidential information such as username, password, social security number, etc. via the e-mail.

4. It is important that users follow the procedures outlined for selection of passwords because e-mail accounts have the potential of being accessed from anywhere in the world.

5. E-mail accounts are provided as a benefit to faculty, staff and students of Oakwood University. Therefore, accounts are canceled upon termination or resignation.

6. Users should read and delete unwanted e-mail messages on a regular basis.

7. Users should not send viruses and threatening, abusive or objectionable e-mail messages from Oakwood University’s e-mail system. Neither should users generate or send SPAM mail using the system.

8. Users should remember that e-mail is being transmitted over a medium that may not be private. Therefore, users should not send or keep any e-mail message that may be potentially embarrassing.

9. Users should keep the number of e-mail messages at a minimum, since disk quotas are strictly enforced.

10. Users should not read, alter, copy, attempt to intercept, or destroy e-mail messages which belong to another user. E-mail received in error should be returned to the sender as soon as the error is discovered.