Marist College Technology Acceptable Usage Policy

1.1 Purpose:

The standards defined in this Acceptable Usage Policy (AUP) are the guidelines for usage of the college's technology resources by its users as are set in the IT Security Policy. The use of the campus technical resources is a privilege and access can be revoked at any time for improper usage. This policy applies to all faculty, staff, students, and guests using the technical resources of the campus. By using or accessing Marist College's technical resources all individuals agree to comply with this policy and the campus code of conduct along with all federal, state, and local laws. Use of the campus technical resources without authorization is prohibited. The purpose of the college's technical resources is to support education, research projects and administrative services of the campus. All other uses of the college's technical resources are secondary. Any type of activity that will prevent the technical resources of the campus from meeting their primary purpose may be terminated without notice.

1.2 Policies:

1.2.1 Copyright and License:

1. Software may not be copied without the owner's permission, unless permitted by copyright.

2. Individuals will respect the privacy of information stored on campus computer systems regardless of whom it belongs to. Individuals agree not to acquire or modify information belonging to another person without permission of the original owner. Information that has been acquired or modified from someone else is still the property of the original owner and may not be distributed or modified without the permission of the original owner.

3. Individuals that acquire a copy of someone else's work in any from with or without the owner's permission and have the intent to present it as their own work is an act of plagiarism, which is forbidden. Individuals who also provide their own work to others knowing they intend to present it as original work is strictly prohibited.

4. The number of simultaneous users for a piece of software will not exceed those stated in the copyright, purchase, or license agreement for that software.

5. The use of Marist's resources will not be used to violate copyright or patent laws.

6. Individuals who use their personal machines will not use the campus networking resources to acquire or distribute copyrighted works.

7. Individuals will not modify software or data without the consent of the creator of the software or data.

8. This college complies with the DMCA act of 1998 and will take the appropriate disciplinary action for individuals who use the campus resources to violate copyright.

1.2.2 Security and Protection of Information:

1. All individuals are responsible for the security of the accounts and equipment assigned to them. Any policy or security violation traced back to a certain account or technical resource will be held against the person assigned to that resource accountable for the violation, regardless if the owner personally committed the violation.

2. Access to Marist College technical assets by unauthorized individuals or for unauthorized purposes is forbidden.

3. Operating systems and software that use the campus network will be required to have the latest security patches installed.

4. All computers that access Marist technical resources, either on or off campus, will be required to run an anti-virus scanner specified by Marist with current virus detections files.

5. Individuals will not install software or hardware that monitors keyboard, Internet access, or other user monitoring activities on Marist's technical resources. These include traffic sniffers, key loggers, or other data logging applications that are configured to violate an individual's privacy.

6. Individuals who must store sensitive or personal information on their computers are accountable for that data. The individual must make sure the appropriate security is in place to protect that data.

7. Individuals will not access or transmit sensitive or personal data over un-secure mediums such as Wireless or the Internet without the appropriate security. The use of a VPN or types of encryption must be used in these cases.

8. All individuals with a Marist account will be required to change their password every 365 days on those accounts.

1.2.3 Usage:

1. The technical resources of the campus are shared resources, and all individuals are expected to keep their use of these resources to a reasonable level. An individual's access will be denied to these resources if they are discovered taking unfair advantage of these shared offerings.

2. Students using campus resources for educational activities have priority over anyone using the campus resources for recreational activity. Students who need certain resources may ask the recreational user of those resources to stop if there are insufficient resources for their educational activity.

3. The use of switches, routers, or access points to allow multiple systems on the network via one port are forbidden without the consent of the Department of Information Technology.

4. The use of personal computers is allowed on the campus network, however owners are responsible for the maintenance and support of those systems.

5. Use of Internet communication is voluntary with the understanding that individuals may encounter material that may be offensive. Marist College assumes no responsibility for the material viewed.

6. Individuals will only use accounts assigned to them. Accessing someone else's account or providing someone else with access to your account is prohibited.

7. The use of the college's technical resources to attack other resources, individuals, execute Denial of Service attacks against other networks, or to hack other networks is forbidden. Individuals will not use campus resources to spread spam, chain emails, or hoaxes to other individuals. Performing these activities will be grounds to have all access terminated.

8. All individuals using Marist's technical resources will not attempt to gain unauthorized access to system both on and off campus.

9. The use of the college's technical resources for commercial purposes or for personal financial gain is forbidden.

10. The campus reserves the right to require the removal of any technical resources that has been deemed a security or network risk.

11. Users waive any right to compensation for lost work or time due to issues with the campus technical resources.

12. Only IP addresses assigned by the Information Technology Department may be used on the campus network.

13. All devices that access the campus network must be registered with the Information Technology Department.

14. All users of the campus technical assets agree not to take any actions, which would be considered inappropriate. Such actions may include, but are not limited to, the following; foul language, harassment, consumption of food or drink in the computer labs, or any behavior that causes distractions.

1.2.4 Theft/Damage:

1. Theft, rearrangement, or damage to college technical assets is forbidden.

2. Anyone using the technical assets of the campus agrees to use these resources in a careful and responsible manner for the assets made available to them.

3. Individuals are financially responsible for the loss, damage, or destruction of equipment caused by negligence, misuse, abuse, or carelessness.

4. Any equipment that is stolen, whether personal or Marist owned should be reported to the Office of Safety and Security.

1.2.5 Vendor Responsibilities:

1. Vendors will not disclose to anyone outside of Marist College, induce the disclosure of, or use in other than Marist College business any confidential information or material relating to Marist College business, either during or after the relationship with Marist College, without the express written permission of Marist College. Information received in confidence from the IBM Corporation, from Marist College customers, or from any other third party, is included within the meaning of this paragraph.

2. Vendors will not disclose to anyone within Marist College, or induce the disclosure of, any confidential information or material relating to Marist College business, either during or after the relationship with Marist College, without the express written authorization of that party's need to know. This applies to information flow between distinct departmental areas of Marist College, as well as among members of any one departmental area.

3. Vendors will not disclose to Marist College, or induce Marist College to use in any way, any confidential information or material belonging to others.

1.2.6 System Administrator Responsibilities:

1. The system administrators of the college will monitor technical resources for their availability.

2. Campus administrators will develop policies and implement technologies to prevent theft or damage to the campus's technical resources.

3. System administrators are responsible for securing central technical resources used by any member of the campus community.

4. System administrators will follow and enforce agreements used by software or hardware packages that they maintain.

5. System administrators will cooperate with administrators or legal entities from off campus locations to deal with problems caused by Marist's technical resources.

6. System administrators will enforce the policies created by Marist College that govern the running of the campus and its assets.

7. System administrators will not access or view a computer without the consent of the account holder. The only exceptions will be in cases where an account or computer is affecting services for the rest of the campus, or to investigate policy or legal violations.

8. System administrators will not take any efforts to monitor electronic communications. The only exceptions will be in cases where an account or computer is affecting services for the rest of the campus, or to investigate policy or legal violations.

1.3 Violation:

By accepting this usage policy, you understand that violation of this agreement may result in punitive damages. Such action may include, but is not limited to, suspension of technology privileges, revocation of technology privileges, charges and/or fines for damages occurred, suspension from College

or employment by the College, expulsion from College or termination of employment from the College, and referral to local, state, or federal law enforcement agencies. Any decision in regard to violation of the agreement can be appealed through the proper channels.

1.4 About this AUP:

This Acceptable Usage Policy will remain in effect as long as the individual makes use of Marist College technical assets. The Office of Information Technology may add rules, regulations, or guidelines related to Acceptable Usage of the campus technical resources. A current copy of this policy can be found online at Marist College's Information Security website located at http://security.marist.edu .

1.5 Contact:

If a violation of this policy or other campus technology policies occurs, individuals should report them to the Department of Information Technology. Failure to report a violation of this policy will be treated as a violation. For questions or clarification regarding these policies, please contact the Cybersecurity office via email at informationsecurity@marist.edu . The Department of Information Technology reserves the right to update this Acceptable Use Policy when it is deemed necessary.