FLORIDA NATIONAL UNIVERSITY
COMPUTER USE POLICY (the "Policy")

I. Purpose

To support the mission of Florida National University and the needs of the Students, Faculty, and Staff, by facilitating the use of information systems.

II. Agreement to the Policy

By using any of the Computing Resources (defined below) of Florida National University, Users (defined below) expressly agree to strictly abide by the terms and conditions contained within this Policy, in its current form and as amended from time to time.

III. Definitions

1. The "University" or "FNU" shall refer to Florida National University.

2. "Computing Resources" shall refer to any and all University facilities, hardware, software, computing services, networks, websites, social media, and computer accounts used by the University, its agents, vendors, other authorized users, employees, faculty, and/or students. The term "Computing Resources" shall expressly include, but in no way be limited to, all computers (desktop computers, laptop computers, and server computers), networks, software-as-a-service (SaaS) services, cloud-based services, disk drives, disks/discs (including but not limited to floppy disks, CD's, and DVD's), flash memory drives, tape drives, removable media, removable storage, portable storage devices, and storage media.

3. "Electronic Communication" shall refer to (but shall not be limited to) electronic mail, instant messaging, electronic messaging, social media communications, or any other form of communication transmitted through a computer network, the internet, or a similar medium.

4. "Data" shall refer to any and all information residing on or transmitted through the University's Computing Resources.

5. "Users" shall refer to those individuals authorized by the University's administration to use the University's Computing Resources. The term "Users" shall expressly include all of the University's students, faculty, staff, employees, visitors, and guests.

IV. Policy Statement

The Computing Resources of the University are the property of the University. The use of the Computing Resources is a privilege granted by the University to Users. The university requires that all Users act responsibly in using the Computing Resources, and do so in compliance with all local,

state, and federal laws, all applicable administrative regulations and policies, all contractual and license agreements, and all policies of the University.

Users are entitled to use the Computing Resources only for purposes related to their studies, their instruction, the discharge of their duties as employees, their official business with the University, and other activities as may be approved by the University's administration.

Users are responsible for the appropriate use of the Computing Resources, and for taking reasonable precautions to secure all Computing Resources and Data used by them. Users are responsible for reporting inappropriate use of the Computing Resources and Data, and any suspected or actual breaches of computer security, and are responsible for assisting in resolving such matters. Users are responsible for promptly reporting to the University in writing any suspicion or occurrence of any unauthorized activity (as outlined herein) as it may pertain to the Computing Resources. Users are responsible for adhering to the University's policies and practices as described herein, and in other policy manuals of the University, to ensure that the Computing Resources and Data are used in accordance with the University's policy guidelines, and reasonable measures are taken to prevent loss or damage of Computing Resources and Data. Users must report all malfunctioning equipment immediately including copiers, computers, computer accessories, printers, network equipment, projectors, etc. to support@mm.fnc.edu, or call 305-821-3333 ext. 1031.

V. Proprietary Information

All forms of Data are considered confidential. All forms of Data produced by the University employees on or with the University computers and network resources are the property of the University. All forms of Data either stored or transmitted are considered property of the University.

Deleting, altering, or sharing Data, and/or any confidential, proprietary, or any other computer information while employed by the University, upon and/or after termination, and/or at any other time whatsoever, is strictly prohibited.

Any Computing Resources used while employed by the University must be returned, along with the User's password, identification code, and any other appropriate information necessary for the University to continue using the respective Computing Resources and information, uninterrupted.

VI. Password Selection and Protection

Select difficult passwords. Change them regularly, and protect them from snoopers. Serious damage can be done if someone gets your password.

Do not share your password with anyone. Do not write your password down where someone can find it, and do not send it over the Internet, Intranet, e-mail, dial-up modem, or any other communication line.

1. Use 8 or more characters, and at least one numeric character. Your password should not include your login ID, your name, your spouse's name, your partner's name, your children's name, your pet's name, or any other names commonly known to others.

2. Your password should not be a word pertaining to the University, your work, or an activity that you participate in or follow that is commonly known.

3. Your password should not include anything derogatory, offensive, or defamatory. If you have a question about password selection or safekeeping, please see the System Administrator.

DO NOT LEAVE YOUR COMPUTER LOGGED ON AND UNATTENDED. WHEN STEPPING AWAY FROM YOUR COMPUTER AT ANY TIME (EVEN IF FOR JUST A SHORT PERIOD OF TIME), MAKE SURE YOUR SCREEN IS LOCKED AND PASSWORD-PROTECTED. IF YOU HAVE ANY QUESTIONS ABOUT THIS PROCEDURE, PLEASE ASK FOR ASSISTANCE.

Do not log on to your system if someone can see you keying in your password. Make sure your computer is set to deny access after three unsuccessful attempts. Report any irregularities flagged by your computer. Turn off your computer at the end of your scheduled workday. If you use a remote access program, and you need to leave your computer on, be sure the computer is locked and it is in a locked room.

USERS MUST IMMEDIATELY REPORT TO THE UNIVERSITY ANY KNOWN USE BY ANOTHER OF THEIR ACCOUNT, LOGON ID, PASSWORD, PIN, TOKENS, ETC.

VII. Use of Personal Software

Users may NOT use or install personal software or programs (whether obtained by purchase, on a trial period, free of charge, or otherwise) on the University's Computing Resources at any time or for any reason.

VIII. Acceptable Use, and Prohibited Activities

Computing Resources may only be used for legal purposes. Examples of prohibited activities ("Prohibited Activities") include, but are in no way limited to, the following (all of the following Prohibited Activities shall expressly include, but not be limited to, engaging in any such conduct through the use of internet, intranet, micro-blogging, and/or "social media" sites):

1. Accessing or attempting to access the Computing Resources without the approval of the University;

2. Attempting to alter or damage Computing Resources or Data, or any other property (whether tangible or otherwise) belonging to the University, other Users, others, or external networks;

3. Attempting or actually gaining unauthorized entry to the University's network or external networks, or accessing in any manner the private files of another, except as may be provided by appropriate authority;

4. Stealing or unauthorized copying of Data or other information without permission;

5. Posting, sending, or transmitting any sensitive, proprietary, and/or confidential information (or disclosing any information which is not otherwise public) outside of the University and/or to anyone not reasonably authorized to obtain such information;

6. Intentional propagation of computer viruses, Trojans, worms, etc., or the introduction of any self-replicating and/or malicious code (or any other code whose purpose is to damage or hinder a computer or network system) into the Computing Resources or any other system maintained by any other individual and/or entity;

7. Performing any act which may, or is reasonably likely to, degrade the performance of the Computing Resources (including but not limited to utilizing an unreasonable amount of bandwidth). Such acts may include, but are not limited to, downloading media files such as music and video files, and the playing of video games;

8. Violation of any local, state, or federal laws, or any administrative regulations or policies, or performing any act which is reasonably likely to result in violation of same, including but in no way limited to copyright and/or other intellectual property laws;

9. Performing any act which causes or is reasonably likely to cause damage to any of the University's Computing Resources, Data, or the property (whether tangible or intangible) of another;

10. Using the Computing Resources in connection with a denial-of-service attack, or a distributed denial-of-service attack;

11. Performing any act intended to, or reasonably likely to, circumvent security or access controls of the Computing Resources, or the systems of any other individual and/or entity, including but not limited to the possession or use of any software or hardware used or reasonably likely to be used for purposes such as analyzing network performance or security, circumventing or removing software copy protection, revealing or uncovering

passwords, identifying or probing security holes or vulnerabilities, decrypting files without authorization or without the proper decryption key/password, or otherwise exposing or weakening computer security methods, etc.);

12. Violating any software license agreements;

13. Software piracy;

14. Transmitting speech not protected by the First Amendment;

15. Promoting or maintaining a private business;

16. Sharing or using someone else's login information (login ID and/or password);

17. Performing any fraudulent or illegal activities, including but in no way limited to: gambling, trafficking in drugs or weapons, participating in terrorist activities, participating in any pyramid or Ponzi schemes, or attempting or gaining unauthorized entry into any computer system, whether part of the Computing Resources or otherwise;

18. Publishing information or performing any act that results in defamation, libel, disparagement, or portrayal in a false light.

19. Using the Computing Resources in any manner that could be reasonably deemed as unethical and/or unprofessional by the University.

20. Using the Computing Resources in any manner that could be reasonably deemed as bullying and/or harassment towards any other person or group of persons.

21. Sending out any unsolicited commercial email or Electronic Communication whatsoever. Any unsolicited commercial email or Electronic Communication which is otherwise permitted by applicable laws, shall only be sent with the advance express written approval of the University's administration, and then only from an account designated by the University's administration.

22. Sending out any email or Electronic Communication which contains pornographic, racist, bullying, harassing, or otherwise offensive content, or content which is reasonably likely to be deemed by anyone as containing such content;

23. Sending out, perpetuating, or re-transmitting, any chain letters via an Electronic Communication;

24. Sending out, perpetuating, or re-transmitting, any mass mailings whatsoever, whether for commercial purposes or not, via an Electronic Communication;

25. Sending out any malicious code, or code which is designed to (or actually does) damage or hinder performance of any computer system or network, via an Electronic Communication;

26. Sending out any email or Electronic Communication which contains a falsified or misleading header or header information, or an alias sender;

27. With respect to internet, intranet, micro-blogging, or "social media" sites, establishing any group, subgroup, listserv, mailing list, fan site, fan club, fan page, pseudonym, custom URL, or any other similar identity, which either purports to be or could reasonably be interpreted to be an official identity of the University, without the University's prior express written permission to do so;

28. Transmitting any Electronic Communication which either purports to be or could reasonably be interpreted to be an official communication of the University, without the University's prior express written permission to do so.

IX. Back-up

Students are responsible for safeguarding the work and information they produce and must backup their information frequently (but no less than daily) to a removable memory device of their own. If visitors and/or guests wish to save any of their data, they must do so only to a removable memory device. The University is not responsible for any data loss suffered by a student, visitor, and/or a guest. Additionally, students, visitors, and guests should retain a current secondary backup of all of their data. The University shall not be responsible for damage or data loss to any removable memory device.

Faculty and staff are responsible for saving all of their University-related work on the University's servers. Saving information on any other storage medium (including, but not limited to, a desktop computer, laptop computer, a removable storage device, or online storage) is strictly prohibited. Activity on the Computing Resources is monitored for tampering, security breaches,
and compliance with this Policy. Maintenance and back-ups are performed on the servers daily.

X. No Expectation of Privacy

Users shall not have any expectation of privacy in connection with their use of the Computing Resources. The University expressly reserves the right to audit and monitor all Data and use of the Computing Resources.

XI. Hosted Service and Third-Party Control of Data

The University stores its Data (and any backups thereof) on file storage (in the form of file servers and/or other media) which is located at a remote hosting, service, and storage facility (or facilities) maintained and controlled by a third-party provider (or third-party providers). However, the University reserves the right to maintain its Data (and any backups thereof) internally, in the University's sole discretion and without further notice.

XII. Computer Resource Availability

The University's IT resources are divided between the Student Labs, the Library, the Resource Rooms, the Faculty, and the Staff.

Computer Labs are used Monday through Thursday from 8:30 A.M. to 12:30 P.M. and from 6:00 P.M. to 10:00 P.M. for teaching as per the Master Schedule. Monday through Friday, one lab at each campus will be open from 8:00 A.M. to 10:00 P.M. with a lab assistant. All labs must remain locked when not in use. The computers will be available to the students under the supervision of the Instructor or lab assistant. A Faculty or Staff member must supervise the students if a lab assistant is not present. The computers will be used to teach the approved curriculum. Instructors must refer to the Master Schedule for availability of the Computer Labs. The Computer Labs are available to Faculty and Staff when class is not in session.

Library and Resource Room Computers are available from 8:00 A.M. to 10:00 P.M., Monday through Thursday, and 8:15 A.M. to 8:00 P.M. on Fridays. These computers are available on a first come first serve basis; the users are limited to 30 minutes if there is someone waiting to use them. If no one is waiting to use the computer, users may stay on as long as needed. There is a $0.10 (ten cents) per page charge to print in black and white. There is a $0.25 (twenty five cents) per page charge to print in color. Color printing is only available at the Hialeah Campus.

Students must use the computers for work related to their field of study and must leave the computers in the same state of functionality as they found them. Users MAY NOT disable or make changes to any computer or network settings, install programs, download programs of any kind, bypass the content filter or firewall, open any computer or remove from the University's premises any component of the Computing Resources. The Library and Resource Room computers cannot be opened or altered under any circumstances. Course work calling for alteration of a computer must be done in the approved computer lab only. The student is responsible for safeguarding the work and information they produce and must backup their work and information daily to a removable memory device of their own.

Faculty office computers are accessible to the faculty only and are available to them during Campus hours of operation; these computers operate Campus Vue Software, Microsoft Office, and Windows Operating System, and are password protected. Faculty computers must be

used for the University's work only. The student records are processed and kept in Campus Vue Software. Campus Vue Software has many levels of security and has integrated modules including: Admissions, Financial Aid, Registrar, Student Accounts, and Placement. Everyone using Campus Vue has security levels appropriate to the work they will be performing. Each faculty member is responsible for saving all of their University-related work on the University's servers. Saving information on any other storage medium (including, but not limited to, a desktop computer, laptop computer, a removable storage device, or online storage) is strictly prohibited.

Staff computers are available only to staff and only during their scheduled work hours; these computers operate Campus Vue Software, Microsoft Office, and Windows Operating System, and are password protected. Staff computers must be used for university work only. The student records are processed and kept in Campus Vue Software. Campus Vue Software has many levels of security and has integrated modules including: Admissions, Financial Aid, Registrar, Student Accounts, and Accounting. Everyone using Campus Vue has security levels appropriate with the work they will be performing. Each staff member is responsible for saving all of their University-related work on the University's servers. Saving information on any other storage medium (including, but not limited to, a desktop computer, laptop computer, a removable storage device, or online storage) is strictly prohibited.

Users MAY NOT disable or make changes to any computer or network settings, install programs, download programs of any kind, bypass the content filter or firewall, open any computer, or remove from the University's premises any component of the Computing Resources.

XIII. Violation of the Policy

Any User who violates this Policy (or any portion of this Policy) shall, in the University's sole and absolute discretion, have their access to the Computing Resources suspended and/or terminated, and/or shall be subject to any other lawful administrative action by the University, up to and including termination of employment and/or expulsion, as applicable.

XIV. Waiver; Non-Waiver

No portion of this Policy (nor this Policy as a whole) may be waived by any employee or faculty member of the University. Any waiver or purported waiver of this Policy (or any portion of this Policy) by the University shall not operate as a waiver as to any future or subsequent violation(s) of this Policy (or any portion of this Policy) by any User.

XV. Changes to this Policy

This Policy may be changed at any time by the University, and in a manner determined by the University. Once changed, the revised Computer Use Policy shall immediately become the official Computer Use Policy of Florida National University.

Revision 06-2012.