IF YOU HAVE ANY QUESTIONS ABOUT THIS POLICY, PLEASE ASK ADMINISTRATION FOR ASSISTANCE.

FLORIDA NATIONAL UNIVERSITY
Acceptable Use Policy Regarding Information Technology

Effective Date: August 10, 2020

ARTICLE 1
PURPOSE & POLICY STATEMENT

This *Acceptable Use Policy Regarding Information Technology* (the "Policy") is intended to support the mission of Florida National University (the "University") and the needs of its students, faculty, and staff, by facilitating the use of information technology. This Policy outlines the standards of acceptable use with respect to the IT Resources that are provided by the University, and governs access to and use of such resources. Inappropriate use of information technology can place the University and others at risk. The current version of this Policy can always be obtained from administration.

ARTICLE 2
COMPLIANCE STATEMENT

The University complies with all applicable federal, state, and local laws, and nothing contained herein is intended to be a violation of those laws. The terms of this Policy shall yield to applicable law where required. Without limitation, this Policy is not intended to prevent employees from engaging in legally protected activities, and is not intended to restrict communications or actions protected by applicable law. Nothing herein is designed or intended to curtail activities under Section 7 of the National Labor Relations Act, as amended.

The University requires that all Users act responsibly in using the IT Resources, and do so in compliance with all applicable laws, administrative rules and regulations, all University policies, and all contractual and license agreements. Users are responsible for the appropriate, ethical, and lawful use of the IT Resources, and for taking reasonable precautions to secure all IT Resources used by them. Users are responsible for reporting to the Administrator or a direct supervisor (in the case of employees) malfunctioning equipment or applications, inappropriate uses of the IT Resources, unauthorized activity, and any suspected or actual breaches of security, and are responsible for assisting in the resolution of 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 IT Resources. The duties and obligations imposed by this Policy shall be in addition to and not a limitation of any duties or obligations otherwise imposed by applicable law or rule.

ARTICLE 3
AGREEMENT TO THE POLICY

By using any of the University's IT Resources, Users 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. If you do not agree to this Policy, you must not use any of the IT Resources. The use of the IT Resources by an employee of the University shall signify that employee's agreement to the terms and conditions of this Policy as a condition of such employment.

ARTICLE 4
DEFINITIONS

The following definitions shall apply in connection with this Policy:

(a) "Administrator" shall mean the University's Vice President of Operations. Where this Policy requires communications to the Administrator, such communications shall be sent to aup@fnu.edu.

(b) "Data" shall refer to any and all information residing on or transmitted through the IT Resources.

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

(d) "IT Resources" shall refer to any and all University facilities, devices, peripherals, computers, applications, services, networks, communications systems, accounts, and resources used for or in connection with the processing, transfer, storage, access, and/or dissemination of information, and even if such resources are accessed using a personally-owned device.

(e) "User" or "Users" shall refer to those individuals authorized by the University to use the IT Resources, and shall expressly include all of the University's students, faculty, staff, employees, visitors, and guests.

ARTICLE 5
PROVISION OF THE IT RESOURCES TO NON-EMPLOYEES

With respect to students, visitors, and guests, the IT Resources are provided as a courtesy and convenience, on an as-is basis, and may be discontinued or modified by the University at any time without prior notice.

ARTICLE 6
WIRELESS NETWORK USE

The University provides wireless internet access at its campuses solely as a courtesy and for the convenience of Users. Users connecting to such wireless internet access points acknowledge that such access may not be secure or private, and is subject to eavesdropping. Furthermore, such access may pose a threat to personally-owned devices that are connected to such wireless internet access points, and the data that is transmitted thereon. The University provides no warranty with respect to its provision of wireless internet access. Access to and use of the University's wireless internet is at the User's sole risk. **TO THE FULLEST EXTENT PERMITTED BY LAW, EACH USER AGREES TO HOLD THE UNIVERSITY AND ITS OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, REPRESENTATIVES, AFFILIATES AND SERVICE PROVIDERS HARMLESS FROM ANY CLAIMS IN CONNECTION WITH HIS/HER/THEIR USE OF WIRELESS INTERNET PROVIDED BY THE UNIVERSITY.**

ARTICLE 7
IT RESOURCE AND DATA OWNERSHIP; USE OF THE IT RESOURCES

All IT Resources are the property of the University. All forms of Data produced by the University and its employees, including that produced on or with the IT Resources, that relate to University operations, are the property of the University, and are considered confidential and proprietary. Users are entitled to use the IT Resources only for purposes related to their employment or studies at the University. Notwithstanding the foregoing, Users may access the internet for personal use (web browsing, checking personal email), provided that (a) employees may not use the IT Resources for any such purposes during working hours, and (b) the IT Resources may not be used for commercial purposes unrelated to the operation of the University at any time. All IT Resources used while employed by the University must be returned to the University upon termination of employment, or earlier as may be determined by administration, along with any credentials necessary for the University to continue using the respective IT Resource without interruption. Deleting and/or the inappropriate altering or sharing of Data, whether during or after employment by the University, is strictly prohibited. Data produced by students shall be the property of the respective student, unless another University policy states that such data shall be the property of the University.

ARTICLE 8
NO EXPECTATION OF PRIVACY

Users shall not have any expectation of privacy in connection with their use of the IT Resources. The University expressly reserves the right to audit and monitor all Data, Electronic Communications, and the use of all IT Resources. All employee Electronic Communications and Data transmitted through the IT Resources that relate to University operations are the property of the University. No employee Electronic Communications or Data transmitted through the IT Resources, even if personal in nature, are private or confidential to the employee transmitting or receiving such communications, and may be disclosed and produced to third-parties in connection with any information disclosure that encompasses or includes (inadvertently or otherwise) such transmissions. The University has the right to monitor and review all Electronic Communications transmitted through the IT Resources at all times. Users are responsible for the content of their Electronic Communications. All employee Electronic Communications transmitted through the IT Resources that relate to University operations are considered the University's business records, and may be discoverable in the event of litigation. Notwithstanding anything contained in this Paragraph, the University reserves all of its respective rights with respect to its confidential, private, non-public, and/or

proprietary information. The University reserves the right to monitor, log, and review a record of all websites and internet addresses visited through the IT Resources by any User, along with all content pertaining thereto.

ARTICLE 9
LOGIN CREDENTIALS AND ACCESS CONTROL

Login credentials must meet certain minimum guidelines. Serious damage can be done to the University and the IT Resources if someone obtains a User's login credentials. The following shall apply to all login credentials and access controls:

(a) Users must choose a strong password that is complex and random (e.g., a password must never include a User's login ID, name, family member's name, pet's name, or any other names commonly known to others, and it must never be a word pertaining to the University or a User's work, studies, or activities).

(b) Passwords must be kept strictly confidential and must immediately be changed whenever a User thinks or knows that it has become known to someone else. Passwords must not be shared with anyone. Users are prohibited from allowing anyone else to access their accounts, and Users are prohibited from accessing anyone else's account.

(c) Passwords must not be kept or written down where someone else can find it, and must never be sent over email, text message, or any other communication.

(d) No User may enter their login credentials if someone else can see them typing in their password.

(e) Users will be prompted to change their passwords from time to time.

(f) Users are responsible for all actions taken with their passwords. Users must immediately report to the Administrator any known or suspected use by another of their account or login credentials.

(g) Employees must leave their computers on at night, but reboot them each morning. Employees using a remote access program must keep their computers locked and in a locked room.

(h) **USERS SHALL NOT LEAVE ANY COMPUTER UNLOCKED WHEN UNATTENDED. WHEN STEPPING AWAY FROM A COMPUTER AT ANY TIME (EVEN IF FOR JUST A SHORT PERIOD OF TIME), USERS MUST MAKE SURE THAT THE SCREEN IS LOCKED AND PASSWORD-PROTECTED. USERS SHALL NOT RELY ON A SCREENSAVER TO AUTOMATICALLY LOCK A COMPUTER AFTER A CERTAIN AMOUNT OF TIME.**

(i) **USERS SHALL IMMEDIATELY REPORT TO THE ADMINISTRATOR ANY IRREGULARITIES, ALERTS, OR ERRORS FLAGGED BY A COMPUTER. NO UNIVERSITY EMPLOYEE OR SERVICE PROVIDER WILL EVER ASK A USER FOR THEIR PASSWORD. USERS SHOULD CONTACT THE ADMINISTRATOR IF THEY HAVE ANY QUESTIONS ABOUT THESE PROCEDURES.**

ARTICLE 10
PROHIBITED ACTIVITIES

The IT Resources may only be used for lawful and appropriate purposes, and in accordance with this Policy. The below activities are strictly prohibited in connection with the IT Resources, and the University additionally may deem any other activity prohibited from time to time, as determined in the University's sole discretion.

(a) Accessing or attempting to access IT Resources:

  a. without the University's authorization; or

  b. that are beyond a User's access rights, or are the private files of another.

(b) Sharing login credentials, and/or using someone else's login credentials (login ID and/or password);

(c) Performing any act that does, that is intended to, or that is reasonably likely to, violate or circumvent the integrity,

security, or access controls of, gain unauthorized access to, or interfere with, damage, disrupt, disable, overburden, or impair the IT Resources, or the systems of any other individual or entity;

(d) Using any device, software, method, or routine that analyzes network performance or security, monitors or copies network traffic or resources, circumvents or removes software copy protection, reveals or uncovers passwords, identifies or probes security holes or vulnerabilities, decrypts files without authorization or without the proper decryption key/password, exposes or weakens computer security methods, interferes with or attempts to interfere with the proper working of the IT Resources;

(e) Circumventing or attempting to circumvent security, access controls, content filters, firewalls, digital rights management, or encryption;

(f) Altering, damaging, attempting to alter or damage, or performing any act which reasonably could alter or damage any of the IT Resources or the property of another (including but not limited to making changes to any computer or network settings, downloading or installing programs, or opening any device);

(g) Altering, copying, or moving any University Data without authorization from administration, except where such activity is directly connected to job-related duties (such as with copying/cutting and pasting information while working with a file);

(h) Transmitting, storing, or retrieving:

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

b. media such as music and video, if such conduct reasonably interferes with the learning experience of any student, the job performance of any employee, or the quiet enjoyment of either;

c. any Data that is defamatory, discriminatory, abusive, offensive, sexually explicit, pornographic, racist, obscene, indecent, profane, violent, hateful, harassing or bullying, or that is reasonably likely to be deemed by anyone as containing such content, or that could give rise to civil or criminal liability under applicable laws, rules, or regulations; or

d. any material that violates the rights of another, including but not limited to any intellectual property rights.

(i) Transmitting:

a. any spam, junk mail, chain letter, unsolicited commercial email, or any other similar email, except with prior express written permission from the Administrator in connection with official University operations, and in compliance with all applicable laws, rules, and regulations;

b. any communication which is deceptive, contains a falsified or misleading header or header information, or an alias sender, or which impersonates or attempts to impersonate any other person or entity; or

c. any communication that purports to be or could reasonably be interpreted to be an official communication of the University, without the prior express written permission from the Administrator, or representing a User's personal opinion as that of the University.

(j) Introducing or propagating computer viruses or malicious code into or from the IT Resources, using the IT Resources to conduct or participate in a denial-of-service attack, or using the IT Resources in a way that disrupts, degrades, restricts, inhibits, or interferes with its use by others;

(k) Playing video games;

(l) Violating any local, state, or federal laws, or any administrative regulations, rules, or policies, or performing any act which is reasonably likely to result in the violation of same;

(m) Violating any software license agreements or committing software piracy;

(n) Operating, promoting, marketing, or maintaining a private business or any commercial activity;

(o) With respect to any internet site (including but not limited to any social media site or platform), establishing any identity that purports to be or could reasonably be interpreted to be an official identity of the University, without the prior express written permission from the Administrator;

(p) Installing or downloading software of any kind, except where approved in advance by the Administrator or where installed on a personally-owned device;

(q) Accepting any End User License Agreements or the terms and conditions of any other software or service agreements on behalf of the University, including website agreements, without first obtaining the written approval of the Administrator;

(r) Removing from the University's premises any IT Resources (except for those Users assigned laptop computers or other portable devices intended for such purpose, and in such instances only for such assigned devices);

(s) Deleting or altering University Data, except where such alteration is directly connected to job-related duties (such as with the editing of a file);

(t) Interfering with, degrading, or impairing another User's permitted use and enjoyment of the IT Resources;

(u) Connecting any personally-owned device or storage medium to any of the IT Resources, except when connecting to a public University wireless internet access point solely for the purpose of obtaining internet access;

(v) Performing, conducting, promoting, soliciting, or assisting in any fraudulent or illegal activities, including but in no way limited to: (i) gambling, (ii) trafficking in humans, drugs, or weapons, (iii) exploiting or harming, or attempting to exploit or harm, any person, (iv) participating in terrorist activities, (v) participating in any pyramid or Ponzi schemes, or (vi) attempting or gaining unauthorized entry into any computer system, whether part of the IT Resources or otherwise; and

(w) Using the IT Resources in any manner that:

a. interferes with either the learning experience (as to a student) or the job performance (as to an employee) of the University; or

b. violates any other policy or procedure of the University.

ARTICLE 11
FILE STORAGE

Employees are responsible for safeguarding and saving their work and the Data that they produce, and must save all Data to the appropriate network drive and location. Employees may not retain any copies of Data on their local drive, on removable storage, or on online platforms not provided by the Administrator for such use. Unless expressly authorized to do so by the Administrator, saving, copying, moving, or backing up University Data 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. Students are responsible for safeguarding and saving their work and the Data that they produce. The University does not provide any backup or archival services for student Data.

ARTICLE 12
THIRD-PARTY PROVIDERS

The University may store any or all of its Data (and any backups thereof) internally, or on file storage that is located at remote hosting, service, and storage facilities maintained and controlled by third-party providers.

ARTICLE 13
ELECTRONIC MAIL

Employees and students are provided with email accounts by the University. These email accounts are provided through a third-party provider, and all information pertaining to these accounts (including the electronic mail messages themselves, and any attachments thereto) may be located at remote locations maintained and controlled by a third-party provider. By using an electronic mail account provided by the University, Users agree to the terms of use and privacy policies of the University's third-party providers. Users should avoid opening unsolicited messages and report any suspicious messages to the Administrator. Users should delete all spam immediately, and not reply to any such messages in any way, even if the message states that you can request to be removed from its distribution list. If you continue to receive such messages, contact the Administrator who can block any incoming messages from that address or domain. Employee electronic mail is subject to Article 8 (No Expectation of Privacy) of this Policy.

ARTICLE 14
COPYRIGHTS

Users shall respect all copyrighted works and shall not copy, disseminate, or transmit any copyrighted materials without the prior express written permission of the copyright holder. Removing or altering any copyright or other intellectual property notices shall be strictly prohibited. For additional information, please refer to the University's Policy on Unauthorized Distribution of Copyrighted Materials and the Copyright Infringement Compliance Plan in the University Catalog.

ARTICLE 15
MONITORING & ENFORCEMENT

The University shall have the sole and exclusive right to determine whether a User is in compliance with this Policy. In connection therewith, the University shall have the right to:

(a) Monitor User activity and content on, and User use of, the IT Resources, for any purpose and in any manner determined by the University;

(b) Terminate or suspend, temporarily or permanently, a User's access to any or all of the IT Resources; and/or

(c) Take any other action deemed necessary by the University if the University believes that a violation of this Policy has occurred or likely will occur, including, without limitation, referral of illegal activity to law enforcement.

The University shall have the right to fully cooperate with law enforcement authorities and court orders in connection with any investigation of User conduct in connection with the IT Resources. Such cooperation may include, but shall not be limited to, disclosing a User's identity, provided that such disclosure is made in compliance with all applicable laws. For the avoidance of doubt, any Data of a student User that meets the definition of an Education Record under the Family Educational Rights and Privacy Act ("FERPA") will only be disclosed without the student's consent if the disclosure is permitted by FERPA, which includes the disclosure of education records to comply with a judicial order or lawfully issued subpoena. FERPA protections do not extend to the records of FNU's law enforcement unit. For additional information, please refer to the University's policy on FERPA in the University Catalog. **TO THE FULLEST EXTENT PERMITTED BY LAW, EACH USER AGREES TO HOLD THE UNIVERSITY AND ITS OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, REPRESENTATIVES, AFFILIATES AND SERVICE PROVIDERS HARMLESS FROM ANY CLAIMS IN CONNECTION WITH ACTION TAKEN BY THE UNIVERSITY IN CONNECTION WITH ANY SUCH INVESTIGATION OR COOPERATION, PROVIDED THAT SUCH ACTION IS IN COMPLIANCE WITH ALL APPLICABLE LAWS.**

No portion of this Policy may be waived by any University employee. The failure of the University to enforce any of the terms of this Policy, or to exercise any right herein, shall not operate to or be construed as a waiver or relinquishment of any of the

requirements, or any of the University's rights hereunder, with respect to further conduct. A violation of any portion of this Policy shall be grounds for disciplinary action up to and including termination of employment (with respect to employees) or expulsion from the University (with respect to students), in the University's sole and absolute discretion, subject to all applicable laws, rules, and regulations.

ARTICLE 16
AMENDMENTS

This Policy may be amended at any time by the University, and in a manner determined by the University. Once revised, the revised Policy shall immediately become the official Policy of the University with respect to the IT Resources. The University will notify Users when this Policy is amended, and Users are responsible for staying up to date on the most current version, which can always be obtained from the Administrator.

[End of Document]

POLICY REVIEW STATUS

This policy was last reviewed on **August 9, 2020** by Frank Andreu, Vice President of Operations.

ADMINISTRATOR:

Frank Andreu
(305) 821-3333 Ext. 1008
fandreu@fnu.edu