REGENT UNIVERSITY	*ACCEPTABLE USE POLICY*
Effective Date 8/6/2024	Version 1.1

CONTENTS

PURPOSE

Regent University's technology infrastructure exists to support the institution and administrative activities needed to fulfill the institution's mission. Access to these resources is a privilege that should be exercised responsibly, ethically, and lawfully.

The purpose of this Acceptable Use Policy is to clearly establish each member of the institution's role in protecting its information assets and communicate minimum expectations for meeting these requirements. Fulfilling these objectives supports Regent University's ability to implement a comprehensive system-wide Information Security Program.

SCOPE

This policy applies to all users of computing resources owned, managed, or otherwise provided by the institution. Individuals covered by this policy include staff/faculty, students, and third parties with access to the institution's computing resources and/or facilities (collectively "Users"). Computing resources include all Regent University owned, licensed, or managed hardware and software, and related services and any use of the institution's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network. This Acceptable Use Policy is in addition to any policies in the Student Handbook, Employee Handbook, Faculty and Academic Policy Handbook, and other University policies.

PRIVACY

Users do not acquire a right of privacy for communications transmitted or stored on the institution's resources. Additionally, in response to a judicial order or any other action required by law or permitted by official Regent University policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the institution, the Chief Executive Officer/President/Chancellor or Senior Vice President and General Counsel may authorize a Regent University official or an authorized agent, to access, review, monitor and/or disclose computer files associated with an individual's account. Examples of situations where the exercise of this authority would be warranted include, but are not limited to, the investigation of violations of law or the institution's rules, regulations, or policy, or when access is considered necessary to conduct Regent University business due to the unexpected absence of a User or to respond to health or safety emergencies. Regent University, or its designated authority, reserves

the right to intercept, monitor, or record all information stored on its information systems and inspect activity to diagnose problems or identify security threats and/or violations.

POLICY

Activities related to Regent University's mission take precedence over computing pursuits of a more personal or recreational nature. Any use that disrupts the institution's mission is prohibited.

Following the same standards of common sense, courtesy, and civility that govern the use of other shared facilities, acceptable use of information technology resources is subject to the right of individuals to be free from intimidation and harassment. All users of Regent University's computing resources must adhere to the requirements enumerated below.

FRAUDULENT AND ILLEGAL USE

Regent University explicitly prohibits the use of any computing resource for fraudulent and/or illegal purposes. While using any of the institution's computing resources, a user must not engage in any activity that is illegal under local, state, federal, and/or international law. As a part of this policy, Users must not:

- Violate the rights of any individual or institution involving information 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 Regent University.
- Use copyrighted material including photographs, books, or other copyrighted sources, copyrighted music, and any copyrighted software in violation of law.
- Export software, technical information, encryption algorithms, or technology in violation of international or regional export control laws.

Any user that suspects or is aware of the occurrence of any activity described in this section, or any other activity they believe may be fraudulent or illegal, must notify his/her manager immediately.

CONFIDENTIAL INFORMATION

Regent University has ethical and legal responsibility for protecting confidential information in accordance with its Information Classification Policy. To that end, there are some general positions that the institution has taken:

- Access to user data is granted to Regent University employees as a privilege for working for the University. Access is granted based on an employee's role and job function. Reference the Access Management procedure for more information on user data access.
- End-user traditional messaging technologies (for example, e-mail, instant messaging, SMS, chat, Peer-to-Peer, etc.) are subject to compromise. Transmission of confidential information by these messaging technologies is discouraged.
- Creating and storing confidential information on unauthorized mobile devices (phones, tablets, USB drives) and removable media is prohibited, unless through university approved external hard drives provided by the University IT (Information Technology) Help Desk. Mobile devices that access confidential information will be physically secured when not in use and stored to minimize the risk of unauthorized access.
- All staff/faculty and third parties will use approved workstations or devices to access the institution's data, systems, or networks. Non-institution owned workstations that store, process, transmit, or access confidential information are prohibited unless covered by the Bring Your Own Device (BYOD) policy. Remote workers can connect to the Regent University network using approved university provided VPN and Remote access software. Processing and storing confidential information on devices not owned by the university is prohibited.
- All institution portable workstations will be securely maintained while in the possession of staff/faculty. Such workstations will be handled as carry-on (hand) baggage on public transport. They will be concealed and/or locked when in private transport (e.g., locked in the trunk of an automobile) when not in use.
- Photographic, video, audio, or other recording equipment will not be utilized in secure areas where confidential information is stored, processed, transmitted, or viewed.
- All confidential information stored on workstations and mobile devices must be encrypted.
- All Users who use institution-owned workstations will take all reasonable precautions to protect the confidentiality, integrity, and availability of information contained on the workstation.
- Institution Users and third parties who move electronic media or information systems containing confidential information are responsible for the subsequent use of such items and will take all appropriate and reasonable actions to protect them against damage, theft, and unauthorized use.
- Institution Users will lock their workstation whenever they leave their workstation unattended or will log off or lock their workstation when their shift is complete.

PASSWORDS

Password Security is an integral aspect of information security. As passwords are the first layer of protection for user accounts, a poorly chosen (weak) password may result in the compromise of personal information and confidential Regent University information. As such, all Regent University faculty, staff, and students (including visitors, contractors, and vendors with access to Regent University systems) are responsible for taking appropriate measures, as outlined below, to select and secure passwords.

Password Selection Guidelines

All users of Regent University managed assets should understand how to select strong passwords.

A strong password has the following characteristics:

- Contains no less than eighteen (18) characters
- Contains at least one upper case alpha character (A-Z)
- Contains at least one lower case alpha character (a-z)
- Contains at least one numeric character (0-9)
- Contains at least one allowed non-alphanumeric character !#*,-._+=:?[\]^~
- Is not based on personal information, names of family, etc.
- Best practice is to use a “pass phrase” of something that you can remember, such as a song lyric with mixed case and non-alphanumeric characters and numbers separating the words in the phrase
- Password length, character for character, is more important than password complexity

A poor, weak password has the following characteristics:

- Contains less than 12 characters
- Is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software
    - The words "RegentUniversity", "vabeach", "cbn" or any derivation
    - Birthdays and other personal information such as addresses and phone numbers
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Password Secrecy Guidelines

The following suggestions provide a guideline for protecting password secrecy.

- Never share passwords with anyone, including instructors, assistants, technology service staff, or supervisors, either verbally, via email, fax, photocopy, or any other means of communication, unless it is a University branded asset as described in the *Social Media* section.
- Do not use similar passwords utilized on external accounts (AOL, Yahoo, MSN, etc.)
- Do not write down passwords on paper
- Use a trusted password management application such as Bitwarden or 1Password
- Change passwords immediately if compromise is suspected
- Use two-factor authentication when available

Password Aging and Expiration

All users must change any Regent University managed password in their control, at a minimum, every 365 days. Passwords exceeding this limitation are subject to enforcement as defined in the 'Password Policy Enforcement' paragraph of this policy.

SOCIAL MEDIA

To limit the institution's risk exposure related to the use of social media sites/software:

- Employees shall not claim to represent Regent University in social media postings or messages unless specifically authorized to do so by the Marketing Department.
- Personal use of any chat or streaming media service as a representative of Regent University shall not be permitted without explicit approval from Marketing.
- Hosting or publishing any websites claiming association with or sponsorship by Regent University without explicit approval by Marketing is prohibited. See the *Web Presence* section of the *Information Systems Policy*.

Access to social media sites must comply with the following:

a. Account credentials used to access Social Media sites for university business must be configured with unique pass phrases, must be @regent.edu accounts, and provided to Marketing and Information Technology.
b. Accounts used to access Social Media sites, where possible, must be configured to use multi-factor authentication.
    - Employees must not, under any circumstances, defame or otherwise discredit the products or services of Regent University, their partners, affiliates, students, vendors, or other institutions.
    - Postings shall not use Regent University's logo, trademark, proprietary graphics or photographs of the institution's premises or personnel without explicit approval

from Marketing.

- Postings, whether business-related or personal, must not contain information that Regent University considers derogatory or damaging to the institution's reputation and goodwill. Any such posts, even those made anonymously, are subject to investigation and appropriate remedial action.

ARTIFICIAL INTELLIGENCE (AI)

Regent University is continuously working to identify areas of Artificial Intelligence (AI) usage related to confidentiality, integrity, availability, processing, storing, and transmitting confidential data. Therefore, there may be instances where the AI component is temporarily disabled while Regent verifies its security to prevent any data exfiltration.

Purpose of AI Systems: AI systems must be used for lawful, ethical, and responsible purposes only. Users should clearly define the intended purpose of AI systems and ensure that their use aligns with legal and ethical standards.

- Clearly define the objectives and use cases for the AI system.
- Regularly review and update the system's purpose to ensure it remains lawful and ethical.
- Obtain legal advice or consult relevant guidelines to verify compliance with regulations and ethical considerations.

Acceptable Use: Users must use AI systems in compliance with all applicable laws, regulations, guidelines, and University policies.

Privacy and Data Protection: Users must respect the privacy and confidentiality of individual and institutional data and adhere to applicable data protection laws and regulations.

Bias and Fairness: Users must strive to ensure fairness and prevent bias in the development, deployment, and usage of AI systems.

Transparency and Interoperability: Where feasible and appropriate, AI systems must be transparent, and their operations and decision-making processes must be explainable.

Safety and Security: Users must prioritize the safety and security of AI systems and take necessary precautions to protect them from unauthorized access, tampering, or misuse.

Accountability: Users must be accountable for the actions and outcomes resulting from the use of AI systems.

Ethical Considerations: Users must consider the ethical implications of AI systems, including potential societal impact.

Intellectual Property: Users must respect intellectual property rights when using AI systems.

Compliance and Reporting: Users must report any suspected violations or any concerns regarding the use of AI systems to the Information Technology Help Desk.

HARASSMENT

Regent University is committed to providing a safe and productive environment, free from harassment, for all Users. For this reason, users must not:

- Use institution information systems to harass any other person
- Actively procure or transmit material that is in violation of sexual harassment or hostile workplace laws.

If a user feels he/she is being harassed using the institution's information systems, the user must report it as outlined in the Employee Handbook.

INCIDENT REPORTING

Regent University is committed to responding to security incidents involving personnel, institution-owned information, or institution-owned information assets. As part of this policy:

- The loss, theft, or inappropriate use of institutional access credentials (e.g., passwords, key cards, or security tokens), assets (e.g., laptop, cell phones), or other information shall be reported to the IT (Information Technology) Help Desk.
- The loss of data due to viruses, worms, Trojan horse programs, or other harmful components present on any Regent University computer system shall be reported to the IT Help Desk immediately upon detection.
- No employee of the university shall prevent any other employee or student from reporting a security incident.

MALICIOUS ACTIVITY

Regent University prohibits the use of information systems for malicious or illegal activity against other users, the institution's information systems themselves, or the information assets of other parties.

- Abuse or misuse of the information systems, including without limitation e-mail and the Internet, in any way, which would result in the detriment to the information systems, or which would in any way reveal or disclose nonpublic information, data, or materials of Regent University without express authorization, is prohibited.

DENIAL OF SERVICE

Users must not:

- Perpetrate, cause, or in any way enable disruption of Regent University's information systems or network communications by *denial-of-service* methods
- Knowingly introduce malicious programs, such as viruses, worms, ransomware, and Trojan horses, to any information system
- Intentionally develop or use programs to infiltrate a computer, computing system, or network and/or damage or alter the software components of a computer, computing system or network

CONFIDENTIALITY

Users must not:

- Perpetrate, cause, or in any way enable security breaches, including, but not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access
- Attempt to gain access to files and resources to which they have not been granted permission, whether such access is technically possible or not, including attempting to obtain, obtaining, and/or using another user's password
- Make copies of another user's files without that user's knowledge and consent
- All encryption keys created by users must be provided to Information Technology upon request.

IMPERSONATION

Users must not:

- Circumvent the user authentication or security of any information system;
- Add, remove, or modify any identifying network header information ("spoofing") or attempt to impersonate any person by using forged headers or other identifying information;
- Create and/or use a proxy server of any kind, other than those provided by Regent University, or otherwise redirect network traffic outside of normal routing; or
- Use any type of technology designed to mask, hide, or modify their identity or activities electronically.

NETWORK DISCOVERY

Users must not:

- Use a port scanning tool targeting either Regent University's network or any other external network, unless this activity is a part of the user's normal job functions, such as a member of the Information Technology department, conducting a vulnerability scan, and faculty utilizing tools in a controlled environment.
- Use a network monitoring tool or perform any kind of network monitoring that will intercept data not intended for the user unless this activity is a part of the user's normal job function as a member of the Information Technology department.

OBJECTIONABLE CONTENT

Regent University prohibits the use of institutional information systems for accessing or distributing content that other users may find objectionable. Users must not post, upload, download, or display messages, photos, images, sound files, text files, video files, newsletters, or related materials considered to be:

- Political
- Racist
- Sexually explicit
- Violent or promoting violence
- Contrary to Regent University's Christian mission

See the Employee Handbook for more information.

HARDWARE AND SOFTWARE

Regent University strictly prohibits the use of any hardware or software on a Regent device that is not purchased, installed, configured, tracked, and managed by the institution. Users must not:

- Install, attach, connect, or remove or disconnect, hardware of any kind, including wireless access points, storage devices, and peripherals, to any institutional information system without the knowledge and permission of Information Technology department;
- Download, install, disable, remove, or uninstall software of any kind, including patches of existing software, to any institutional information system without the knowledge and permission of the Information Technology department;
- Use personal flash drives, or other USB based storage media; or
- Take Regent University equipment off-site without authorization by the Information Technology Department.

ELECTRONIC MESSAGING

The University provides a robust communication platform for users to fulfill its mission. University email services may be used for incidental personal communication. However, such use must comply with all applicable University policies, guidelines, and the terms outlined in this Acceptable Use Policy. All messages, in any format, are the property of Regent University. Regent University does not guarantee confidentiality with respect to any information stored, sent, or received through its electronic messaging systems.

Regent University reserves the right to inspect electronic messages and/or disclose electronic messages to law enforcement or government officials or to other third parties, at its sole discretion, without notification to or permission from those creating, sending, or receiving the information. Routine automated messaging inspection is performed for virus and phishing protection, Data Loss Prevention and the security Regent-confidential information and Users personal information.

Users must not:

- Automatically forward electronic messages of any kind outside of the Regent University domain regent.edu, by using client message handling rules or any other mechanism; unless approved by the AVP of Information Technology.
- Utilize Email to transmit (send or receive) any part/s or whole copyrighted works for which the user has not received permission, or it is otherwise illegal to use.

- Email messages, in stored, forwarded, received, or sent format, should not be used in a way which may constitute intimidating, hostile or offensive material, including but not limited to such conduct based on sex, race, color, religion, national origin or disability. The University's policy against sexual or other harassment applies fully to its Email systems.
- Use Email for personal business transactions or political purposes.
- Use Email to facilitate a local, state, or federal crime.
- Utilize encryption devices to conceal illegal or prohibited activities. Users who employ encryption mechanisms to protect confidentiality agree to provide "plain text" copies of messages upon request to Regent University. Failure to abide by such requests is a violation of this policy and will be treated accordingly.
- Sign up for 3rd party services, subscriptions, mailing lists, etc. that are not related to the operation of the University.
- Use Email to send or forward chain letters, offensive jokes, messages carrying viruses or worms, and mass mailings unrelated to the operation of the University.
- Send messages, unrelated to the operation of the University, in another person's name or a fictitious name.
- Send messages that adversely affect the normal operation of the Email systems.

REMOTE WORKING

Please refer to the Employee Handbook for guidance on eligibility factors and criteria used to grant permission for teleworking or telecommuting assignments. Once permission is granted and when working remote the user must:

- Safeguard and protect any institution-owned or managed computing asset (e.g., laptops and cell phones) to prevent loss or theft.
- Not store or transfer any university restricted, private, or confidential information to personally owned devices.
- Not access or process confidential information in public places or over public, insecure networks.
- Take reasonable precautions to prevent unauthorized parties from utilizing computing assets or viewing Regent University information processed, stored, or transmitted on institution-owned assets.
- Not create or store confidential or private information on personally owned computing devices.
- Only use approved methods for connecting to the institution (e.g., VPN or Citrix).

ROLES AND RESPONSIBILITIES

Regent University reserves the right to protect, repair, and maintain the institution's computing equipment and network integrity. Any information obtained by Information Technology personnel about a user through routine maintenance of the institution's computing equipment or network should remain confidential, unless the information pertains to activities that are not compliant with acceptable use of Regent University's computing resources.

ENFORCEMENT

Any Users found to have violated this procedure may be subject to disciplinary action up to activation of the Progressive Discipline Policy, please see the ***Employee Handbook***.

The institution may temporarily suspend or block access to an account, prior to the initiation or completion of disciplinary procedures, when it appears necessary to do so to protect the integrity, security, or functionality of the institution or other computing resources or to protect Regent University from liability.

All users of Regent University's information systems may report university policy or law violations to their immediate supervisor, representative faculty, or school personnel, or directly to the Information Technology Department Help Desk at 757-352-4076 or helpdesk@regent.edu.

EXCEPTIONS

Exceptions to the policy may be granted by the AVP of Information Technology, or by his or her designee. All exceptions must be reviewed annually.

REFERENCES

- The Gramm - Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- The Higher Education Opportunities Act of 2008 (HEOA) [34 CFR Section 668]
- Code of Ethics of the American Library Association
- NIST 800-171
- PCI DSS 3.1

RELATED POLICIES

- Information Security Policy
- Information Systems Policy
- Information Classification Policy

OWNERSHIP AND REVIEW

This document is owned by EVP for Finance and Administration.
This document shall be reviewed annually.
Changes to this document shall be in accordance with the ***Document and Records Control Standard.***

CONTACT INFORMATION

Executive Director of Network Engineering

DOCUMENT PROPERTIES

PROPERTIES	
Property	**Description**
Circulation	All University employees or other authorized student users
Next Scheduled Review	March 2025

DOCUMENT APPROVALS	
Title	Date
EVP for Finance and Administration	8/6/2024
AVP for Information Technology	8/6/2024

REVISION HISTORY			
Version	**Date**	**Description of Changes**	**Revised by**
0.01	2/14/2024	Initial draft version	Managed Security Services Provider
1.0	7/17/2024	Initial Version	ISO
1.1	8/6/2024	Initial Version	ISC

Information Systems
Acceptable Use Policy Acknowledgement

I have received a copy of, read and understand Regent University's Acceptable Use Policy regarding the information systems that have been provided to me by the university, for my use. I understand that Regent University reserves the right at any time to examine, inspect, and/or monitor my use of university telephones, computers, computer networks, electronic voice mail systems, e-mail systems, Internet, or World Wide Web (WWW) activity, or any other communications systems provided or owned by Regent University, at its sole discretion and without further notice to me, or permission from me.

I acknowledge and agree that any electronic files, records, and communications which I create or use on the information systems shall always remain subject to access, review or deletion by Regent University as set forth in such policy. I further agree that I will not install any electronic data or software not authorized by Regent University. I have no expectation of privacy regarding documents or communications created, received, stored on, or sent through Regent University's information systems and electronic communications systems, including without limitation e-mail and voice mail messages.

CURRENT REGENT STATUS (Please Check All that Apply):
_____ Faculty, Adjunct, Staff, Student Employee
_____ Temporary
_____ Student

_____
User Signature

_____
Date

_____
Printed Name