Title of Policy:	**ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES POLICY**
Approval Date:	**June 30, 2017**
Supersedes Policy:	**Computer and Information Technology Use Policy (2000) and Computer & IT Use Procedures & Guidelines (2001)**

I. Purpose

The purpose of this policy is to outline the acceptable use of information technology (IT) resources including but not limited to computer systems, computer labs, applications, networks, software, and files (hereinafter referred to as "Resources") at Morgan State University (hereinafter referred to as "University"). These rules are in place to protect the University. Inappropriate use exposes the University to risks that prevent it from achieving its mission, vision, goals, and objectives. Appropriate use of Resources should always be legal, ethical, reflect academic honesty, and show restraint exercised in the consumption of shared Resources. At all times, users must apply standards of normal academic and professional ethics and abide by University codes of conduct and policies, and all applicable laws and regulations.

II. Definitions

A. **Authorized Students** – Morgan State University students who are authorized to use the information technology resources, including but not limited to computer systems, computer labs, applications, networks, software, and files.

B. **Chain Email** - An email that is sent to a number of people that requests each recipient to send copies with the same request to other individuals.

C. **Confidential Information** – Data that is protected by federal, state, or local law, or contractual obligation, or that is specifically designated as confidential by the University. Information also is considered confidential if its loss, misuse, unauthorized disclosure, or alteration might cause substantial injury to the University, its constituents and/or affiliates in terms of financial loss, reputational damage, operational capability, and/or significant embarrassment. Examples of Confidential Information include, but are not limited to:

- Student education records (e.g., grades, biographical information, class rosters)
- Social Security Numbers and related data

- Medical Records
- Payroll Records
- Personnel (employment) records
- Bank account, credit/debit card or other financial information

The highest levels of security must be applied to restrict access to Confidential Information to authorized individuals, and to protect against its unauthorized use, disclosure, or modification.

D. **Internal Use Only Information** – The University's default classification for information, and refers to all institutional data that is not classified as either "Confidential Information" or "Public Information". Information is considered Internal Use if its loss, misuse, unauthorized disclosure, or alteration might cause moderate injury to the University, its constituents and/or affiliates. Examples include, but are not limited to:

- Internal directories
- Non-public meeting minutes or memoranda
- Drafts of official documents

A reasonable level of security must be applied to limit access to Internal Use Only Information, and to prevent its unauthorized use, disclosure, or modification.

E. **Policy** – Acceptable Use Of Information Technology Resources Policy

F. **Public Information** – As defined in the Maryland Public Information Act, Title 4, General Provisions Article of the Annotated Code of Maryland, the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; 34 CFR Part 99, and any other applicable laws.

A reasonable level of security must be applied to protect Public Information against unauthorized modification.

G. **Resources** - Any Morgan State University owned, leased, managed, controlled, or contracted information technology resource including, computing devices, data networks, software, databases, services and facilities used for data, including on-premises, third party, external, or hosted resources (Cloud solutions). Examples of Resources include, shared computer drives, network file shares, networkable copiers, University-provided wireless networks (WiFi), and University provided programs such as Microsoft Word, Outlook, etc.

H. **University** - Morgan State University

I. **Users –** Authorized Students, faculty and staff who have access to Resources.

III. Scope

The University employs its Resources to support the University's mission of instruction, research, and service. The University provides access to Resources for its Users to advance the mission and strategic goals of the University, consistent with institutional priorities and financial capabilities. In limited circumstances, the University may authorize access to its Resources to visitors, vendors, and contractors; such authorization must be in writing. In addition to applicable laws and University policies and standards, this Policy applies to all Users, including in limited circumstances, any visitors, vendors, and contractors who are authorized by the University to use its Resources, regarding the proper use of Resources, whether utilizing those Resources on campus or remotely, and the resulting information and data generated using these Resources, whether directly or indirectly. The University reserves the right to limit, deny, or extend resource privileges and access as deemed necessary. Users are solely responsible for their actions using the Resources, including the use of assigned unique identifiers, such as email accounts provided by the University to conduct activities in support of the University's mission. The University reserves the right to take appropriate action in response to violations of this Policy.

The Resources and all information and data generated using these Resources, whether directly or indirectly, or generated on behalf of the University, are the property of the University and the State of Maryland.

IV. Personal Responsibility

The University cherishes the diversity of perspectives represented on this campus and, accordingly, does not condone censorship, or the casual inspection of electronic information. Users are responsible for safeguarding their own credentials, including user IDs and passwords, and for using them for their intended purposes only. Users are solely responsible for all transactions made under the authorization of their credentials, and for activity involving Resources which originate from computing devices owned by or assigned to them. Users may not represent or imply that any personal electronic publications (e.g., web pages) or any personal communications reflect the views or policies of the University. Users are obligated to use computing resources responsibly, ethically, and in a manner which accords both with the law and the rights of others. The University depends first upon a spirit of mutual respect and cooperation to create and maintain an open community of responsible Users.

V. Users' Personal Use of Resources

A. Authorized Students' Use for Personal Purposes

Authorized Students may use Resources for personal purposes, with some limitations, provided that such use does not:

- Directly or indirectly interfere with the University's operation of computing facilities;
- Burden the University with noticeable incremental cost;
- Interfere with the student's employment with the University or other obligations to the University; and/or
- Violate other University policies, or applicable laws or regulations.

B. Faculty and Staff Use for Personal Purposes

Incidental personal use of the Resources by faculty and staff is allowed as time permits; however, personal use of the Resources should be limited. Use may be limited, provided that such use of Resources:

- Does not interfere with University operations;
- Is not of a nature that could cause harm or embarrassment to the University;
- Is on faculty or staff's own time and does not interfere with timely performance of job responsibilities; and/or
- Reflects a similar understanding of the limit on personal use while at home or elsewhere off-campus.

VI. Privacy

To the extent possible in the electronic environment and in a public setting, a User's privacy will be preserved. Nevertheless, that privacy is subject to applicable federal and state law, and the information and data accessed, created, modified, transmitted, or receved using the Resources may be Public Information subject to disclosure under the Maryland Public Information Act, Title 4, General Provisions Article of the Annotated Code of Maryland and/or any other applicable State or federal law. Only authorized Office of Information Technology (OIT), University officials or their designees may monitor and access systems, network traffic and technology Resources for maintenance, operation, security, quality of service, business-related purposes (such as audits), policy or legal compliance, and investigations of alleged violations of this Policy or other regulatory requirements.

Users of Resources must respect the privacy of others, and must protect the security, confidentiality, integrity, and availablitity of information entrusted to them by the University. Users must not inspect, disclose, access, modify, render inaccessible, or delete University data unless specifically authorized to do so.

Users of Resources may be assigned one or more accounts with appropriate access restrictions. Users are not authorized to access accounts other than those to which they have been granted specific access by appropriate University officials or their designees. Users may not seek to change the permission associated with otherwise authorized accounts.

VII. Unacceptable Use

Access to Resources is a privilege, not a right. Access is granted to Users for the purpose of conducting University business, pursuing an education, furthering the mission of the University, and for personal use solely within any terms and conditions set forth by the University. This access is granted only to those Resources needed to perform these duties. Prohibited activities include, but are not limited to, the following:

A. Altering system software or hardware configurations without authorization, disrupting or interfering with the delivery or administration of Resources;
B. Adding, removing, modifying, or destroying University owned, leased, or administered equipment, data, documents, or branding without authorization;
C. Connecting or installing independent or unauthorized technology Resources, network devices, or ancillary equipment without the University's authorization;
D. Installing devices, applications, or services that interfere or conflict with University supplied Resources and services, or violates others' privacy;
E. Registering external domain names (i.e., any domain outside of morgan.edu) that reference systems on the Morgan network without the University's authorization;
F. Unauthorized exposure, disclosure, or dissemination of Confidential Information, Internal Use Only Information or any electronic information that iis not Public Information that the User does not have authority to disclose;
G. Intentionally or unintentionally introducing or transmitting destructive or malicious programs, such as viruses, on any Resources. (An example of unintentional use would be developing code or developing a device that cracks home automation systems and not putting the proper security protections in place or connecting it to the network);
H. Initiating or forwarding Chain Emails;
I. Knowingly using Resources for illegal activities. Criminal or illegal use may include, but is not limited to, obscenity, child pornography, fraud, threats, harassment, copyright infringement, trademark infringement, defamation, theft, identity theft, and unauthorized access;
J. Attempting to access or accessing another's accounts, private files, email messages, or intercepting network communication without the owner's permission except as appropriate to the User's job duties and in accordance with a legitimate University purpose;
K. Conducting, participating in or facilitating unauthorized access to Resources;
L. Misrepresenting one's identity, status, role or that of another person;
M. Using Resources for personal, commercial, religious, political (including activities supporting the nomination of any person for political office or attempting to influence the vote in any election or referendum), solicitation, or profit-making purposes, or to represent the interest of groups unaffiliated with the University or unassociated with the normal professional activities of faculty, staff, or students without written authorization from the University or

appropriate University official (e.g., an Authorized Student's class project or assignment);

N. Storing confidential data within unauthorized storage platforms, including those commonly referred to as "Cloud" services, such as Dropbox, OneDrive, GoogleDrive, and Amazon Cloud, except where such storage platforms have been provided by the University for use of University data or information. (Using storage within the free or pay-per-space cloud services transfers the ownership of the University's data to the cloud provider);

O. Installing, copying, distributing, or using digital content (including software, music, text, images, and video) in violation of copyright and/or applicable federal and State laws;

P. Downloading, accessing, using, or distributing any communications, data, information, or media which violate State or federal laws, such as copyright protected movies, music, software, or art;

Q. Using the University's name, logos, trademarks, or seal in any way that implies University endorsement of another organization's products, services, or beliefs without prior and proper authorization; and/or

R. Unauthorized use of the University's name, logo, trademarks, or seal.

VIII. Enforcement

Questions regarding the application of this Policy should be directed to the Office of Information Technology (OIT). A violation of this Policy constitutes unacceptable use of Resources and may violate other executive orders, federal, State and local laws and regulations, and/or University policies, standards, procedures and guidelines. Known or suspected violations of this Policy, or any other executive orders, federal, State, and local laws and regulations, and/or University policies, standards, procedures and guidelines related to this Policy should be reported to the OIT. If possible, reports should include a copy of any non-sensitive information relevant to the alleged violation.Violators of this Policy are subject to, but not limited to, restriction or revocation of access to Resources in accordance with any applicable University policies or procedures, and any applicable laws and/or regulations.

The University shall develop and adopt procedures to implement this Policy consistent with the provisions set forth herein.

IX. Contact

To report violations or request further information, please contact the Office of Information Technology Security.