Universidad Ana G. Méndez
Florida Branch Campuses
Acceptable Use of Technology Resources

Introduction
Computers and other information technology resources are essential tools in accomplishing AGMU's mission. Information technology resources are valuable assets to be used and managed responsibly to ensure their integrity, confidentiality, and availability for appropriate research, education, outreach, and administrative objectives of the AGMU. This policy will standardize the use of technology resources provided by AGMU.

Purpose
The purpose of this policy is to collect and detail the institutional rules governing the proper use and access to technology resources by AGMU employees and students, as well as their responsibilities and duties.

Scope
To ensure AGMU systems and critical information are protected and free from security risks, this policy presents the acceptable usage of computers and workstations, telecommunications networks, Internet access, systems linked to the cloud, the use of social networks and other technological devices belonging to AGMU, and the information handled by all these systems.

Procedure
As specified in the Human Resources Manual, the technology resources used in the institution, and the information handled by it, are property of AGMU and can only be used for authorized purposes related to the institutional operations (Internet Access Section). Such use must follow established standards detailed within this manual. However, the organization reserves the right to change it at any time, adapting to changes and technological developments, as necessary. AGMU also reserves the right to approve any other regulation or additional policy related to the operation of technology resources.

Since technology resources and information are the property of AGMU, they may be subject to inspection and/or monitoring by any agent or authorized representative of the institution at any time, with or without previous notice. Therefore, users have no expectation of privacy in relation to the use of technology resources, or in relation to the information accessed or obtained through these resources or in carrying out their duties.

AGMU will establish a program of regular audits. With or without prior notice, the information systems will be monitored by the institution for any lawful purpose, including the following: Ensure that resources mentioned above are being used for exclusive purposes of work, to prevent misuse of the system, repair or correct any problems that the systems may have, whether it is hardware or software based, and comply with the laws and regulations of conduct and / or procedures established by AGMU that may affect the institution, its representatives, students and employees.

Failure to comply with the rules and provisions contained in this policy may result in disciplinary action, including termination of employment. Some violations could also lead to legal action against the user.

Use of Accounts and Passwords

Computers, workstations, laptops, and another computer equipment must be accessed using the user account and password previously and individually assigned to each user. The username and password must be handled as confidential information, as it is used to obtain access to privileged and / or sensitive information. Therefore, the user agrees to:

1. Use the individual username and password assigned in a responsible way.
2. Do not share the username and password at any time.
3. Do not leave visible the username and password.
4. Do not write the password down on paper, notebook, or any place where it could become compromised.
5. Change the password if it is believed that it has been exposed or compromised.
6. Change the password in the period established by the system.
7. If there is a suspicion of any compromising situation with your username and password, the user must follow procedures for responding to incidents documented in this Manual.
8. Register on the platform provided by Information Security for self-service password change if forgotten or locked account.
9. Always use a strong/complex password taking into consideration the following complexity requirements:
    a. The password must contain at least 10 characters.
    b. The password must contain letters and numbers.
    c. The password must contain at least one uppercase letter.
    d. It must also include at least one special character, such as #, $, @.
10. If you are responsible of managing a special account (visitor account), you must:
    a. Change the password during the period established by the system.
    b. Do not leave visible the username and password.

Acceptable User of Technology Resources

The use of AGMU technology resources should be in a legal and ethical manner, in support of the functions that users are assigned. Such use should be appropriate, and resources must be used in an efficient way. The following provisions, among others, define the Acceptable Use of Technology Resources:

1. AGMU users must use the institutional technology resources to manage and exchange information and content in accordance with their employment profile.
2. All portable resources that may contain sensitive information from partners, faculty and / or students must be encrypted with the Information Security selected tool. This encryption process must be certified by the AGMU IT Security Specialist.
3. Every computer or laptop must be guarded safely when utilized outside of AGMU facilities. It is your responsibility to prevent any loss or theft. In case of loss or theft of equipment you should submit a report to the police and notify the IT Department immediately, in accordance with the procedures documented for incident response in this manual.
4. All AGMU technological equipment should have an antivirus installed by the IT Department. AGMU equipment that does not require systemic antivirus will have to be preauthorized and

must remain in an isolated environment. Any personal computer connected to the wireless network must have an antivirus installed.
5. All AGMU technological equipment that will be donated, given away, or sold must be properly erased so that their information cannot be retrieved or reconstructed.
6. All technological equipment such as computers, mobile phones and tablets may be connected to the wireless networks provided but must be used in accordance with the rules governing such networks.

The following are considered unacceptable use of technology resources:

1. The transmission of information or any actions that go against the rules, policies, mission and vision of AGMU, as well as any state and federal regulations.
2. Sending or receiving obscene language, pornography, or material including sexual or discriminatory content.
3. Any conduct that equates to harassing, stalking, discriminating against anyone.
4. Obtaining, transmitting, or distributing materials electronically in violation of intellectual property rights.
5. Performing actions that cause congestion of telecommunication networks or violate institutional operations.
6. The use of equipment or programs for the purpose of violating the implanted systemic controls.
7. The installation and / or use of unauthorized or unlicensed programs.
8. Any vandalism against institutional technology resources.
9. Accessing or attempting to access systems, devices, programs, or sections of programs for which the user is not authorized.
10. The use of personal social media to publish AGMU related events in violation of the social media for Employees Policy (P93-003-21, current version).

Acceptable Use of Other Peripheral Equipment and Electronic Devices

In addition to the technology resources, the institution may require the use of other peripheral equipment and electronic devices as part of the institutional operation. Such use shall be governed by the same rules mentioned above, and includes the following standards:

1. The use of external storage devices is permitted only if owned by AGMU and approved by the corresponding department. The copy of data to personal devices is prohibited, as is safeguarding personal information in AGMU equipment.
2. All peripheral equipment belonging to AGMU must be safely guarded inside and outside AGMU installations. It is your responsibility to prevent any loss or theft.

Misuse of AGMU devices or violation of the protocols established above can lead to disciplinary actions, as stated in AGMU manuals, policies, rules, and regulations.

Acceptable Use of Information

The use of information through technology resources is essential for all work performed by all employees. Access to information should be in accordance with the employment position and responsibilities. It is the responsibility of AGMU and the entire community to keep their data safe and protected from unauthorized access. That is why the following rules applies to the proper use of the information:

1. All members of staff are responsible for the information handled daily with their functions. You must always ensure that sensitive or confidential information is being handled with the highest standards of security (encryption or access through password).
2. All members of staff must ensure and certify in advanced that the person they are providing the information to is in fact the person for which the information is intended.
3. All staff who cease functions with AGMU will be required to return all information related to their duties immediately.
4. Data and files containing information in any form related to the operation of AGMU will be saved only in institutional technology resources.
5. The disclosure of information related to students, employees and / or faculty or any other sensitive and confidential information is prohibited without the written consent from AGMU or an authorized representative.
6. Retention, removal, or dissemination of information related to the operation of AGMU without proper explicit authorization is prohibited.
7. The extraction of sensitive information by using external devices unencrypted or through printed material is prohibited. The data extraction shall have the sole purpose of performing job related operations previously authorized by AGMU.
8. All printed material with sensitive information must be shredded once its purpose is fulfilled.
9. The sharing of sensitive information (encrypted) to third parties will only be allowed if one or more of the following scenarios are present:
    a. State or federal court order
    b. Confidentiality Agreement
    c. Official authorization
10. Using personal tools for document storage is prohibited.
11. All users must ensure that the permissions of their documents residing in the cloud (OneDrive) are correct and are not public.

Use of Office 365 or Web Administrative Tools

The Institution provides all staff with user accounts for Office 365 and all its tools and software. This cloud system is the only resource authorized by AGMU for performing administrative and academic functions. Furthermore, it continues to increase the access to web tools for an easy way to connect remotely to corporate systems. The use of these tools is governed by the following rules:

1. The user must use their reasonable judgment in using these tools, taking into consideration the purpose and content of it.
2. Communication through the Office tools must comply with institutional rules.
3. Sending or transferring sensitive, confidential, or proprietary information requires the user to use the encryption tool defined by the IT Department.

4. The institutional e-mail system does not constitute in any way a method of file storage. Any information that needs to be saved must be stored through an authorized tool that act as electronic repository of official documentation. e.g., OneDrive or SharePoint.
5. Each user is responsible for maintaining acceptable levels of utilization and consumption within the storage systems provided by the institution, including cleaning and maintenance.
6. The association of the user account or institutional email to personal social networking profiles such as Twitter, Facebook, Instagram, etc. is not allowed.
7. In general, the use of Office Suite resources for personal commercial purposes is prohibited.
8. Access or attempt to access other user's Office account is prohibited unless it is intended for legitimate research purposes and / or audit. This intervention must have the appropriate authorizations in advance.
9. The practice of sharing accounts and passwords for access to systems is prohibited.
10. Sending mass emails to groups or distribution lists should follow the rules established for such cases. 11. All mobile devices, whether property of AGMU or personal, that are used to connect to Office or any other web tools must have set a password security ('PIN') and this device must not be unlocked (jailbreak). In the case of loss or theft (of an AGMU mobile device), you must immediately notify the IT Specialist of your institution for proper cleaning (wipeout) of the device.
11. If you would like to place a profile photo on this platform, it must be a picture of the face and one that is professional (e.g., the official photo ID provided by Human Resources).

Use of Internet

AGMU provides access to the Internet for academic, research and administrative use. The use of the Internet entails rules related to their use. AGMU may monitor and / or limit user access to the Internet using institutional technology resources, this to ensure safety and quality service to our university community. Given the nature of the Internet, AGMU cannot ensure the availability, accuracy, accessibility, and appropriate use of Internet resources. Any violation or misuse of Internet access will result in disciplinary action and could lead to corrective action in accordance with the provisions contained in the manuals and policies of the Ana G. Mendez University (AGMU).

The following actions, among others, are considered unacceptable:

1. Accessing pornographic material, criminal activities, offensive, defamatory, discriminatory or any illegal-in-nature material that may be considered offensive to others or affecting the image and institutional security.
2. Accessing, downloading, or distributing material through the Internet in violation of intellectual property rights or copyright.
3. Interfering with or evading security systems, controlling and monitoring the access to the Internet.
4. Transmitting sensitive or confidential information for personal purposes unrelated to the assigned functions.
5. Transmitting sensitive or confidential information that is not adequately protected (encrypted) before being transmitted.
6. Misrepresenting oneself by name, title, or authority.
7. Using social networks that directly or indirectly interfere with the functions and / or user's productivity.

   a. All social networking accounts that are identified with the name or logo of any of the institutions must be associated with an official email account. The link of official accounts to a personal email account is not permitted. This account must have more than one administrator associated with it, who will be responsible for content development, updating and monitoring. The creation of these accounts must have the corresponding approval.
8. Accessing online messaging conversation ("chat", "chat rooms", "blogs", "messenger", etc.) using institutional technology resources for personal business, and not for academic and / or administrative tasks.
9. Accessing web pages that can compromise network security.
10. Attempting any security attack within AGMU technology resources with the purpose of exposing, experimenting, testing, damaging, or affecting services inside and / or outside the organization.

AGMU can limit Internet navigation service if one of the following is suspected: misuse, infections by viruses, suspicious navigation, attacks, among others.

Security Incident Response Information

The complexity of new applications, the fact that the systems are connected to the Internet and the increase in cyber-criminal activity makes information security incidents almost inevitable. It is essential to have a management plan for these incidents so that the impact is reduced, and a reaction can be more effective with greater speed and efficiency. Effective communication at all levels of the institution is essential to limit the impact of security events reported. Therefore, it is important that our community knows how to identify security incidents and knows the process for reporting them.

<u>Identification Information Security Incidents</u>
Users must report any information security incident detected, including but not limited to the following:

1. Erratic and inexplicable behavior of computers, servers, and networks. Examples:
   a. The mouse moves by itself and / or open screens automatically.
   b. Many internet interruptions in a short period (5 to 10 minutes).
   c. Exaggerated sluggishness in the system.
2. Detection of accounts that have been blocked without any explanation.
3. Detection of unauthorized access to electronic devices of the institution. Examples:
   a. Personal computers connected to the administrative network (cable).
   b. People who are not AGMU employees using computers in the administrative area.
   c. Loss or theft of equipment.
4. Discovery of unauthorized wireless systems, such as wireless access points ("hot spot").
5. Phishing email that has been accessed.
6. Confidential or sensitive information that has been inadvertently distributed to unauthorized persons or posted online.
7. Erratic behavior on our web pages. Examples:
   a. The website contains ads or images with inappropriate content that is not representative of or authorized by our institution.
   b. If the information on the website is not readable or understandable.
   c. If the website is out of service.

   d. If you are redirected to another page that is not an AGMU or UAGM website.
8. Threats of cyber-attacks aimed at AGMU by any means of communication (email, regular mail, social networks, etc.).

AGMU is not responsible for individual actions of members of the university community who violate the provisions of the use of technological resources. If AGMU believes that it is appropriate, it can report any incident to state and / or federal agencies.

How to Report Information Security Incidents

Every user has the responsibility to immediately report information security incidents to the corresponding department.