Acceptable Use Policy

Overview

This policy is not intended to impact UACCM's established culture of openness, trust, and integrity. We are committed to protecting our students, employees, partners, and the college from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of UACCM. These systems are to be used for educational and business purposes in serving the interests of the students, college, and our constituents during normal operations.

Effective security is a team effort involving the participation and support of every UACCM student, employee, and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at UACCM. These rules are in place to protect the students, employees, and UACCM. Inappropriate use exposes UACCM to risks including virus attacks, compromised network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct UACCM business or interact with internal networks and business systems, whether owned or leased by UACCM, the employee, or a third party. All students, employees, contractors, consultants, temporary, and other workers at UACCM and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with UACCM policies and standards, and applicable laws and regulations.

This policy applies to students, employees, contractors, consultants, temporaries, and other workers at UACCM, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by UACCM.

1. Policy

1.1 General Use and Ownership

1.1.1 UACCM proprietary information stored on electronic and computing devices whether owned or leased by UACCM, an employee, or a third party, remains the sole property of UACCM. Users must ensure through legal or technical means that proprietary information is protected in accordance with the UACCM *Data Protection Policy.*

1.1.2 Users have a responsibility to promptly report the theft, loss, or unauthorized disclosure of UACCM proprietary information, personally identifiable information (PII), or personal health information (PHI), hereto known as sensitive information.

1.1.3 Employees may access, use, or share UACCM sensitive information only to the extent it is authorized and necessary to fulfill their assigned job duties.

1.1.4 Users are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should consult their supervisor or manager about personal use expectations.

1.1.5 For security and network maintenance purposes, authorized individuals within UACCM may monitor equipment, systems, and network traffic at any time, per UACCM's *Audit Policy*.

1.1.6 UACCM reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

1.2 Security and Proprietary Information

1.2.1 All mobile and computing devices that connect to the internal network must comply with the UACCM *Minimum Access Policy*.

1.2.2 System level and user level passwords must comply with the UACCM *Password Protection Policy*. Providing access to another individual, either deliberately or through failure to secure access, is prohibited.

1.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. Users must lock the screen or log off when the device is unattended.

1.2.4 Postings by users from a UACCM email address to newsgroups, blogs, social media sites, etc. should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of UACCM, unless posting is in the course of business duties.

1.2.5 Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

1.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is a student or employee of UACCM authorized to engage in any activity that is illegal under local, state, federal or international law while using UACCM-owned resources. The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

1.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company 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 UACCM.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which UACCM or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server, or an account for any purpose other than conducting UACCM business, even if the employee has authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing an employee's or student's account password to others or allowing use of an employee's or student's account by others. This includes family and other household members when work is being done at home.
7. Using a UACCM computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any UACCM account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the student or employee is not an intended recipient or logging into a server or account that the student or employee is not expressly authorized to access, unless these actions are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to the UACCM IT department is made.
12. Executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of an employee's normal job/duty.
13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, honeynets, or similar technology on the UACCM network.
15. Interfering with or denying service to any user (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, UACCM users to parties outside UACCM.

1.3.2 Email and Communication Activities

When using college resources to access and use the Internet, users must realize they represent the college. Whenever users state an affiliation to the college, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the college".

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any email address other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within UACCM's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by UACCM or connected via UACCM's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

1.3.3 Blogging and Social Media

1. Blogging by employees, whether using UACCM's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of UACCM's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate UACCM's policy, is not detrimental to UACCM's best interests, and does not interfere with an employee's regular work duties. Blogging from UACCM's systems is also subject to monitoring.
2. UACCM's *Confidential Information Policy* also applies to blogging. As such, Employees are prohibited from revealing any UACCM confidential or proprietary information, trade secrets or any other material covered by UACCM's *Confidential Information Policy* when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of UACCM and/or any of its constituents. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by UACCM's *Non-Discrimination and Anti-Harassment* policy.
4. Employees may also not attribute personal statements, opinions or beliefs to UACCM when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of UACCM. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, UACCM's trademarks, logos and any other UACCM intellectual property may also not be used in connection with any blogging activity

2. Policy Compliance

2.1 Compliance Measurement

The UACCM IT team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

2.2 Exceptions

Any exception to the policy must be approved by the UACCM IT team in advance.

2.3 Non-Compliance

A student or employee found to have violated this policy may be subject to disciplinary action.

3. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Blogging
- Honeypot
- Honeynet
- Proprietary Information
- Spam

Revision History

Date of Change	Responsible	Summary of Change
8/19/2019	Stephen Wallace	Initial creation of document
11/15/2019	Stephen Wallace	Added language for students
7/21/2020	Amanda Otto	Grammar check