P.O. Box 6082, Willemstad, Curaçao – Telephone: +1 (631) 480 2118 (USA)

Acceptable Use Policy Electronic Equipment

Document version: 01-2023

1 – Purpose

The purpose for publishing an Acceptable Use Policy for electronic equipment is not to impose restrictions that are contrary to CUN's established culture of openness, trust and integrity. CUN is committed to protecting its students, employees, providers, affiliates and other partners from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet-, Intranet- and Extranet-related systems, including but not limited to computer equipment, mobile devices, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing and FTP, are the property of CUN, its providers or its affiliates. These systems are to be used for purposes in serving the interests of CUN, its students, employees, providers, affiliates and other partners during normal operations.

Effective security is a team effort involving the participation and support of everyone involved, 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.

This policy outlines the acceptable use of computer equipment and other electronic devices at CUN's premises or at other locations, where CUN equipment is used. Inappropriate use exposes CUN's electronic devices, systems and software, as well as devices, systems and software used to access CUN's electronic systems and software to cyber-risks, including virus attacks, compromise of network systems and services, data breach and legal issues.

2 – Scope

This policy applies to the use of information, electronic and computing devices and network resources to conduct CUN's business or interact with internal networks and business-systems, whether owned or leased by CUN, its students, employees, providers, affiliates or any other user. All users are responsible for exercising good judgment regarding appropriate use of information, electronic devices and network resources in accordance with CUN's policies and standards and relevant laws and regulations. Exceptions to this policy are documented in section

This policy applies to all users of electronic equipment and to all electronic equipment, owned, leased or used by CUN.

3 – Policy

3.1 – General use and ownership

Proprietary information, stored on any electronic and computing devices, whether owned or leased by CUN or any other user, remains the sole property of the owner of the information. Proprietary information is protected in accordance with the Data Protection Standard.

Users have the responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information.

Users may access, use or share proprietary information only to the extent it is authorized and necessary to fulfill an assigned duty or study-task.

Users are responsible for exercising good judgment regarding the reasonableness of personal use. In case there is any uncertainty about the eligibility to use or access any of CUN's electronic devices, systems or software, they should consult CUN's ICT Department.

For security and network maintenance purposes, authorized CUN staff or authorized providers may monitor equipment, systems and network traffic at any time, per CUN's Audit Policy.

CUN will audit networks and systems on a periodic basis to ensure compliance with this policy.

3.2 – Security and proprietary information

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

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

All computing devices must be secured with a password-protected screen-lock, with the automatic activation feature set to ten minutes or less. Using a screen-lock or logging off when the device is unattended is mandatory.

Postings from a CUN email address to newsgroups or other online platforms, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of CUN, unless posting is duty- or study-related, to the discretion of CUN.

Users must use extreme caution when opening email attachments received from unknown senders, which may contain malware or viruses.

3.3 – Unacceptable use

The following activities are, in general, prohibited. Users may be exempted from these restrictions during the performance of legitimate duty- or study-related tasks.

Under no circumstances is a user authorized to engage in any activity that is illegal under national or international law, while utilizing CUN-owned or leased 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.

The following system and network activities are prohibited.

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 CUN.
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 CUN 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 performing duty- or study-related tasks is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. CUN's ICT Department and/or CUN's Legal Affairs Department should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.).
6. Revealing account passwords and passphrases to others or allowing use of your account by others. This includes colleagues, fellow-students, friends, relatives and household-members when work is being done at home or at a dormitory.
7. Using a CUN computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in CUN's or the user's jurisdiction.
8. Making fraudulent offers of products, items or services, originating from any CUN account, device or system.

9. Making statements about warranty, expressly or implied, unless it is a part of normal duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are 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, unless these duties are authorized. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, brute-forcing accounts and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited.
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 the user's authorized duties.
13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honeynets or similar technology on CUN's networks.
15. Interfering with or denying service to any user other than the user's host (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 CUN students, employees, affiliates or any other organization or person, related to CUN, to parties outside CUN.

The following e-mail and communication activities are prohibited.

1. When using CUN resources to access and use the Internet, users must realize they represent CUN. Whenever users state an affiliation to CUN, they must also clearly indicate that "the opinions expressed are their own and not necessarily those of CUN". Questions may be addressed to the ICT Department. In these cases preferably a private e-mail account is used.
2. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
3. Any form of harassment via e-mail, telephone, text or paging, whether through language, frequency, or size of messages.
4. Unauthorized use or forging of e-mail header information.
5. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
7. Use of unsolicited e-mail originating from within CUNs networks of other Internet/Intranet/Extranet service providers on behalf of or to advertise any service hosted by CUN or connected via CUN's network.
8. Posting the same or similar non-duty or non-study-related messages to large numbers of Usenet newsgroups (newsgroup spam).

The following blogging and social media activities are prohibited.

1. Blogging or posting to social media platforms, whether using CUN'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 CUN's systems to engage in blogging or other online posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate CUN's policy, is not detrimental to CUN's best interests and does not interfere with regular duties and tasks. Blogging or other online posting from CUN's systems is also subject to monitoring.
2. CUN's confidential information policy also applies to blogging. As such, users are prohibited from revealing any CUN confidential or proprietary information, trade secrets or any other material covered by CUN'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 CUN and/or any person or organization in any way affiliated with CUN. Users are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by CUN's policies.
4. Users may also not attribute personal statements, opinions or beliefs to CUN when engaged in blogging. If a user is expressing his/her beliefs and/or opinions in blogs, he/she may not, expressly, or implicitly, represent themselves as representing CUN. Users 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, CUN's trademarks, logos, study-materials and any other CUN intellectual property may also not be used in connection with any blogging or social media activity.

3.4 – Policy compliance

CUN's ICT Department will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits.

Any exception to the policy must be approved by CUN's ICT Department in advance.

A user found to have violated this policy may be subject to disciplinary action.

Related standards, policies and processes are the following.

1. Data Classification Policy
2. Data Protection Standard
3. Social Media Policy
4. Minimum Access Policy
5. Password Policy

3.5 – Revision History

Date of Change	Summary of Change
January 1, 2023	