Document ID	Title **Acceptable Use Policy**	Print Date 7/17/19
Revision 1.0	**Prepared By** Stephanie Scere, Cyber Security & Compliance Manager	**Date Prepared** 5/1/19
Effective Date 7/17/19	**Reviewed By** Glenn Keller, IT Director & Michael Leland, HR Director	**Date Reviewed** 7/17/19

Revision History

Revision #	Date	Description of Changes	Requested By

Overview

Our intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to CountryMark's established culture of openness, trust and integrity. Rather, we are committed to protecting CountryMark's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, and FTP, are the property of CountryMark. These systems are to be used for business purposes in

serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every CountryMark 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 CountryMark. These rules are in place to protect the employee and CountryMark. Inappropriate use exposes CountryMark to risks including virus attacks, compromise of 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 CountryMark business or interact with internal networks and business systems, whether owned or leased by CountryMark, the employee, or a third party. All employees, contractors, consultants and other workers at CountryMark are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with CountryMark policies and standards, and local laws and regulation.

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

Policy

1.1 General Use and Ownership

1.1.1 CountryMark proprietary information stored on electronic and computing devices whether owned or leased by CountryMark, the employee or a third party, remains the sole property of CountryMark.

1.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of CountryMark proprietary information.

1.1.3 You may access, use or share CountryMark proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

1.1.4 For security and network maintenance purposes, authorized individuals within CountryMark may monitor equipment, systems and network traffic at any time.

1.1.5 CountryMark 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 System level and user level passwords must comply with the *Password Construction Guidelines*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

1.2.2 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 20 minutes or less. You must lock the screen or log off when the device is unattended.

1.2.3 Postings by employees from a CountryMark email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of CountryMark, unless posting is in the course of business duties.

1.2.4 Employees 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 an employee of CountryMark authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing CountryMark-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 CountryMark.
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 CountryMark 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 CountryMark business, even if you have 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 server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a CountryMark 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 CountryMark 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 employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties 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 IT is made.

12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.

14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

15. 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.

16. Providing information about, or lists of, CountryMark employees to parties outside CountryMark.

1.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

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 other 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 CountryMark's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by CountryMark or connected via CountryMark's network.
7. Posting the same or similar non-business-related messages to large numbers of newsgroups (spamming).

1.3.3 Social Media Policy

CountryMark respects the right of any employee to maintain a blog or webpage or to participate in a social networking, Twitter or similar site, including but not limited to Facebook and LinkedIn. However, to protect Company interests and ensure employees focus on their job duties, employees must adhere to the following rules:

1. All rules regarding confidentiality and proprietary business information apply in full to blogs, webpages, and social networking platforms, such as Twitter, Facebook, LinkedIn

or similar sites. Any information that cannot be disclosed through a conversations, a note or an email also cannot be disclosed in a blog, webpage or social networking site.

2. Whether an employee is posting something on his or her own blog, webpage, social networking Twitter or similar site or someone else's, if the employee mentions the Company and also expresses either a political opinion or an opinion regarding the Company's actions that could pose an actual or potential conflict of interest with the Company, the poster must include a disclaimer. The poster should specifically state the opinion expressed is his/her personal opinion and not CountryMark's position. This is necessary to preserve CountryMark's good will and reputation.

3. Any conduct that is impermissible under the law if expressed in any other form or forum is impermissible if expressed through a blog, webpage, social networking, Twitter or similar site. For example, posted material that is discriminatory, obscene, defamatory, libelous or violent is forbidden. Company policies apply equally to employee social media usage.

CountryMark encourages all employees to keep in mind the speed and manner in which information posted on a blog, webpage and/or social networking site is received and often misunderstood by readers. Employees must use their best judgment. Employees with any questions should review the guidelines above and/or consult with their manager. Failure to follow these guidelines many result in discipline, up to and including discharge.

Policy Compliance

1.4 Compliance Measurement

The 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.

1.5 Exceptions

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

1.6 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.