ACCEPTABLE USE POLICY

THE ACCEPTABLE USE POLICY DEFINES REQUIREMENTS FOR THE USE OF COMPUTER AND NETWORK RESOURCES OWNED AND/OR OPERATED BY CU*ANSWERS.

POLICY 03	
	VERSION: 3.0
	EFFECTIVE DATE: JANUARY 1, 2016
	BOARD RATIFICATION DATE: NOVEMBER 8, 2016
	POLICY OWNER: ORD TEAM

WARNING

Failure to adhere to policies may result in discipline up to and including termination.

CONTENTS

POLICY PURPOSE AND OVERVIEW

CU*Answers relies on its computer network to conduct its business. To ensure that its computer resources are used properly by its employees, independent contractors, agents and other computer users, CU*Answers has created this Acceptable Use Policy. The rules and obligations described in this Policy apply to all users of CU*Answers' computer network, wherever they may be located.

Computer Resources that are the property of CU*Answers may only be used for legitimate business purposes. Users are permitted access to the Computer Resources to assist them in the performance of their jobs.

It is every employee's duty to use CU*Answers' Computer Resources responsibly, professionally, ethically, and lawfully. In the use of Computer Resources, Users must observe and comply with all other policies and guidelines of the company.

DEFINITIONS

COMPUTER RESOURCES

The term "Computer Resources" refers to CU*Answers' entire computer network and any device owned and/or operated by CU*Answers, its affiliates, or its clients; any account used to access information on CU*Answers Computer Resources; and telephones and related voice technology.

USERS

The term Users refers to all employees, independent contractors, consultants, temporary workers, and all other persons or entities that use the Computer Resources of CU*Answers.

PROHIBITED USES

UNLAWFUL OR INAPPROPRIATE MATERIAL

Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by email or other form of electronic communications or displayed on or stored in CU*Answers' computers. Users encountering or receiving this kind of material should immediately report the incident to their supervisor(s).

Employees are prohibited from using CU*Answers Internet access or a CU*Answers provided device to view sites considered to be sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate to view.

OTHER PROHIBITED USES

Without prior written permission from a Corporate Officer, CU*Answers' Computer Resources may not be used for dissemination or storage of commercial or personal advertisements, solicitations, promotions, viruses or malware, political material, chain emails, or any other unauthorized use.

MISUSE OF SOFTWARE

Without either prior authorization or as part of a job function, Users may not do any of the following with software provided by CU*Answers: copy software for use on their home computers; provide copies of software to any independent contractors or clients of CU*Answers or any third person; install software on any of CU*Answers' workstations; modify, revise, transform, recast, or adapt any software; or reverse-engineer, disassemble, or de-compile any software. In their use of Computer Resources, Users must comply with all software licenses; copyrights; and all other state, federal and international laws governing intellectual property and online activities.

Users who become aware of any misuse of software or violation of copyright law should immediately report the incident to their supervisors.

UNSUPPORTED TECHNOLOGY

CU*Answers must strike a balance between innovation, effectiveness, and security when Users wish to install unsupported software or hardware which is not issued by CU*Answers. Unregulated installation of software and hardware may result in confidential data leakage, weak security, unavailability in a disruption, access control, and lack of "liquidity" of tools, where the vendor cannot be changed easily if the vendor fails to perform. However, in the interest of innovation and effectiveness, there is a process where tools can be approved for use by the organization.

APPROVAL FORM

Any request to use an unsupported application, regardless of origin (web, cloud, etc.) must be approved by the Network Services team (and possibly a Web Services representative in the case of web applications) before use is allowed. The requestor must complete form in detail and submit to team for review. The requestor's manager must approve the request before being submitted for approval.

NO EXPECTATION OF PRIVACY

NO EXPECTATION OF PRIVACY

The Computer Resources provided to Users by CU*Answers are to assist Users in performance of their jobs. Users should not have an expectation of privacy in anything they create, store, send, or receive on the computer system, or with respect to calls and voice recordings made via the telephones and related voice technology owned and operated by CU*Answers. The Computer Resources are owned by CU*Answers and may be used only for business purposes.

WAIVER OF PRIVACY RIGHTS

Users expressly waive any right of privacy regarding anything they create, store, send, or receive on the computer of through the Internet or any other computer network. Users consent to allowing personnel of the company to access and review all materials Users create, store, send, or receive on the computer or through the Internet or any other computer network. Users understand that CU*Answers may use human or automated means to monitor use of its Computer Resources. Telephone calls may be monitored for quality assurance.

Users expressly waive any right of privacy when using the telephone system or any voice-related technology owned or operated by CU*Answers. Users consent to allowing personnel of the company to review any recorded call. CU*Answers may use human or automated means to monitor use of its telephone system.

ACCESSING THE FILES OF ANOTHER USER

Users may not alter or copy a file belonging to another user without first obtaining permission from the owner of the file. Ability to read, alter, or copy a file belonging to another User does not imply permission to read, alter, or copy that file. Users may not use the computer system to "snoop" or pry into the affairs of other users by unnecessarily reviewing their files and email.

ACCESSING OTHER COMPUTERS AND NETWORKS

A User's ability to connect to other Computer Resources through the network does not imply a *right* to connect to those Resources or to make use of those Resources unless specifically authorized by the operators of those systems.

NO LOCAL ADMINISTRATOR RIGHTS

Users should not expect to have Local Administrator rights on their machines, unless an exception is granted by the Network Services team. Exceptions may be granted upon a showing of business need and completion of the proper form.

UNAUTHORIZED TECHNOLOGY OR SOFTWARE

Users are responsible and may be disciplined for any security breaches related to the use of unauthorized technology or software.

DUTY TO SECURE

Each User is responsible for ensuring that use of Computer Resources, as well as outside computers and networks, such as the Internet, does not compromise the security of CU*Answers. This duty includes taking reasonable precautions to prevent intruders from accessing the company's network without authorization, preventing introduction and spread of malware, and the use of other reasonable means to protect sensitive information.

Users must take reasonable steps to ensure sensitive information is maintained and transmitted securely. Users must not disclose sensitive information unless authorized by job description or by an officer of CU*Answers.

ADDITIONAL INFORMATION

Consult the Cybersecurity Policy for additional information on the requirements for protecting sensitive information.

REMOTE DESKTOP SUPPORT

FROM THIRD PARTIES

Users may require a third party to provide remote desktop support, including WebEx and Citrix GoToAssist remote support tools. The following are the rules for obtaining remote desktop support from third parties:

PERMISSION REQUIRED

Users participating in remote access sessions with third parties must first obtain permission from their manager or supervisor.

PHYSICAL ATTENDANCE REQUIRED

A User participating must remain in attendance with the PC at all times in order to observe the actions of the third party.

SOFTWARE INSTALLATION REQUIREMENTS

Installation of software in a remote access session is governed by the software installation rules of this policy.

TO CLIENTS AND OTHER THIRD PARTIES

Users may need to support clients through remote desktop support. Users must adhere to all policies and procedures of CU*Answers while engaged in remote session support of a client.

ELECTRONIC COMMUNICATIONS

Examples of electronic communications include but are not limited to: email; messaging (both text and instant); and social media. A User should never consider electronic communications to be either private or secure unless encrypted with CU*Answers approved encryption software. Note that electronic communications may be stored indefinitely on any number of computers, including that of the recipient and any individuals the recipient has forwarded the electronic communications onto.

When using electronic communications, a User must comply with the following guidelines:

ENCRYPTION OF SENSITIVE INFORMATION

Users who send or receive sensitive information via electronic communications are required to use encryption when this information is sent out beyond the CU*Answers network borders (such as external email recipients).

NO EXPECTATION OF PRIVACY ON THE INTERNET

Users who post Information Internet should not be consider the data to be private or secure, even when a User is employing a private feature of an electronic communications site. Do not rely on the privacy controls of the provider to keep communications confidential.

ATTORNEY-CLIENT COMMUNICATIONS

Email sent from or to in-house counsel or an attorney representing the company in or potential litigation should include this warning prominently displayed: "ATTORNEY-CLIENT PRIVILEGED; DO NOT FORWARD WITHOUT PERMISSION."

LOGOS AND MARKS

Do not use without authorization the CU*Answer name, names of partners, clients or their logos that would infringe on the intellectual property rights of the owner. If a User has a personal blog where advice or opinion is offered on work-related matters, add a disclaimer to the homepage that states the comments are personal opinions and do not necessarily reflect the opinion of CU*Answers or any of its partners or affiliations.

WARNING

! CU*Answers does not audit the personal electronic communications of Users with respect to non-work related matters. However, should a personal electronic communication be brought to the attention of CU*Answers which adversely affects the reputation of CU*Answers or involves the unauthorized dissemination of sensitive information, this data may be used to discipline the User or terminate employment.

MOBILE/REMOTE COMPUTING AND ACCESS

CU*Answers recognizes that some Users may require mobile or remote access to Computer Resources. This access may include but is not limited to VPN access, a CU*Answers provided laptop or tablet, or access through a personal device. In addition to the other acceptable use rules encompassed in this policy, employees are required to follow these additional policy rules:

APPROVAL REQUIRED

Mobile or remote access to any CU*Answers Computer Resource requires approval by the departmental supervisor and Network Services. CU*Answers reserves the right to deny remote access at any time if the device does not meet minimum secure access requirements. An employee who has not completed the 90 day probationary period is not allowed remote access to CU*Answers Computer Resources unless an exception is made by a corporate officer.

CONSENT TO REMOTE WIPE

All Users must consent to have their mobile access device, whether personal or CU*Answers issued, remotely wiped in the case of termination of employment, loss of the device, or suspicion of a security breach. CU*Answers is not responsible for any loss of personal information which may be stored on the device.

MINIMUM SECURITY STANDARDS

Any device used to connect remotely to CU*Answers Computer Resources must be secured by a password (or PIN if approved by Internal Networks). Remote access requires the device to maintain a secure, encrypted connection between CU*Answers Computer Resources and the local machine. Only approved mobile device management software may be installed on the user's PC for the purpose of updating the device with operating system updates and/or syncing of corporate data. Network Services may change standards at any time and without notice.

VPN

The use of VPN to connect to CU*Answers Computer Resources is strictly prohibited except for approved devices. Users are never allowed to connect using VPN on machines that are accessible to the general public. CU*Answers has the right to terminate any VPN connection at any time if the security of the connection is in question. VPN connections to CU*Answers Computer Resources are strictly limited for business purposes only. No VPN connection may be maintained for longer than five minutes unattended without security measures such as screen-locking employed. Users may never allow any unauthorized individual to access CU*Answers Computer Resources through a VPN connection.

LOCAL SAVE OF SENSITIVE INFORMATION

Employees are expressly forbidden to save sensitive information to any local machine that has mobile or remote access to CU*Answers Computer Resources.

LOST OR STOLEN DEVICE

If the local machine used to connect remotely to CU*Answers is lost or stolen, employees are required to immediately notify a security officer or a supervisor.

ENDPOINT SECURITY

As part of CU*Answers ongoing Data Leakage Control program, all devices shall be restricted to Read Only access for attached USB mass storage devices and optical media drives including but not limited to CD-ROM/CD-RW drives and DVD-ROM/DVD-RW drives. Data execute, write, and modify access is restricted. Where exceptions are made, member data must not be copied to, stored on, or moved by unencrypted USB mass storage or optical media. In order to have an exception, a form must be filled out and permission granted.