SUBJECT: ACCEPTABLE USE FOR INFORMATION TECHNOLOGY SYSTEMS	ORIGINATING DEPT: Systems and Technology Group ("STG")	SECTION: Communications

DATE ISSUED: 01.15.09	SUPERSEDES: New - replaces E-mail and Internet Services Policy	PAGE: 1 OF 9
INITIATED BY: STG	APPROVED BY: Human Resources and Legal	

I. POLICY/PURPOSE

It is the intent of this Policy is to ensure that all authorized users of information technology systems use it in an effective, efficient, ethical and lawful manner. Information technology systems include all hardware and software provided or supported by the Systems & Technology Group ("STG"). Use of the information technology systems includes the use of data/programs stored on Compass Group USA, Inc. (the "Company") computing systems, data/programs stored on tape, disk, CD, or any other storage media that is owned or maintained by the Company. The complete *Information Systems Security Policy* is available from the Information Systems Security Group ("ISS").

II. USERS COVERED BY THIS POLICY

This Policy applies to all Associates employed by the Company and external users who have been authorized access to the Company's information technology systems.

III. RESPONSIBILITY FOR ADMINISTRATION

STG, Human Resources ("HR"), and all levels of management are responsible for the administration of this Policy. ISS Group will perform regular audits to ensure compliance.

IV. PROCEDURES

A. Enforcement

Failure to comply with this Policy is a security violation and will be reported to management. Depending on the severity of the violation, a user may lose short-term or permanent access to the technology systems, and Associates of the Company may be subject to discipline up to and including termination.

B. Confidential, Sensitive, and Personal Identity Information

1. **Confidential Information:** Users shall not disclose, via E-mail, Internet, or any form of electronic communication, any confidential or proprietary information regarding Company activities to any party that does not have authority from Company management to access the information and a need to know. This includes, but is not limited to, copyrighted materials, trade secrets, and financial information. All such information is the sole

property of the Company. In addition, users shall refrain from sending confidential, proprietary, or private Company information via electronic mail or over the Internet/Intranet.

Users shall observe confidentiality obligations with respect to Company software, documentation and all forms of internal information. This information cannot be sold and/or transferred to any non-Company party for any purposes without written authorization by Company management.

2. **Sensitive Information: "**Sensitive Information" should not be sent via E-mail, posted on or transmitted over the Internet, or stored on mobile electronic storage media (such as thumb drives) or on data storage files accessible company-wide or by the public. For the purposes of this Policy, "Sensitive Information" shall include, without limitation, classified Company management or financial reports, communication of a litigious nature, employee relations investigative information, or other information that could reveal the Company's private business information or create litigious exposure.

3. **Personal Identity Information:** For the purposes of this Policy, "Personal Identity Information" shall include, without limitation, social security numbers, drivers license numbers, state identification card numbers, credit or debit card numbers, bank account numbers, passport numbers, alien registration numbers, health insurance identification numbers, user IDs and passwords. Personal identity information shall not be sent via E-mail, or posted on or transmitted over the Internet without approval from ISS. Personal Identity Information should never be stored on mobile electronic storage media (such as thumb drives) or on data storage files accessible company-wide or by the public.

C. Requirements for Using Company Technology and Systems

1. Only users authorized by their immediate manager or department head may use Company technology resources.

2. Company technology resources shall be used for business purposes only.

3. Users shall refrain from installing or using software on Company-issued computers and devices (i.e., desktops, workstations, mobile computer devices, PDAs and cell phones) that is not pre-approved and installed by the Company. For questions regarding approved/non-approved software contact the Information Technology ("IT") Helpdesk at 1-888-295-7206 or 704-328-3149.

4. Users are responsible for ensuring the proper safeguarding of confidential or proprietary information, Sensitive Information, and Personal Identity Information stored on any Company computers or devices issued to them. For example, users must lock or log off the computer when it is not in use.

5. Users must report any breach in computer security, including possible misuse of computer resources to the **Compass Group Crisis Management Hotline** at 1.877.710.6291.

6. Company requires and supports standard anti-virus software on all Company computers. Users shall only use Company-approved anti-virus software. This software is available by contacting the IT Helpdesk (PSG) at 1-888-295-7206 or 704-328 3149.

7. Users shall ensure that anti-virus software is set to auto update by performing routine checks on a frequent basis. For information on the proper way to perform such checks, contact the IT Helpdesk (PSG) at 1-888-295-7206 or 704-328 3149. IT will provide these updates automatically where possible.

8. Users shall refrain from opening or downloading files or programs that are attached to electronic mail ("E-mail") from unknown, suspicious, or untrustworthy sources. Delete such attachments immediately then permanently delete by emptying the computer's "Recycle Bin."

9. Users shall delete spam, chain and other junk E-mail without forwarding it.

10. Users shall avoid hard drive sharing with read/write access unless there is a legitimate business requirement to do so.

11. Users are responsible for backing up critical data on the desktop or laptop on a regular basis and store the backup in a safe place**.** For assistance with backing up data, contact the IT Helpdesk at 1-888-295-7206 or 704-328 3149.

D. Unauthorized Practices While Using Company Information Technology and Systems. Users are prohibited from doing any of the following:

1. Attempting to access any data or programs he/she is not authorized to use or for which he/she does not have explicit consent from the source of the data or programs.

2. Divulging dialup or dial back modem phone numbers.

3. Sharing or divulging to any third party computer passwords or account details.

4. Making unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

5. Copying system configuration files for unauthorized use.

6. Purposely harassing other computer users; degrading the performance of systems; depriving an authorized user access to Company resources; obtaining extra resources beyond those allocated; circumventing computer security measures; or gaining access to a system without authorization.

7. Downloading, installing or running security programs or utilities that reveal computer security weaknesses (e.g. password-cracking programs).

8. Copying confidential, proprietary, Sensitive, or Personal Identity Information onto a USB/DVD/CD or memory stick without prior management approval.

9. Sending Sensitive or Personal Identity Information in E-mail or as an attachment to E-mail.

10. Sharing or downloading proprietary files without management approval.

11. Using specialist software that deletes or wipes data from hard drives on laptops or desktops without approval from ISS.

E. Acceptable Use of Company Electronic Mail Systems

Only users authorized by management may utilize electronic communication tools. Approval for access to E-mail must be specifically granted by the user's departmental head. It is the responsibility of each manager or department head to determine what forms of electronic communication and types of services his/her Associates require for performing their job responsibilities. These requirements are to be formally requested through the IT Helpdesk at 1-888-295-7206 or 704-328-3149.

Each user who utilizes electronic communication equipment and systems is required to safeguard Company information and assets by understanding and complying with this Policy.

ISS is responsible for installing security measures to protect the Company's systems and information from corruption and intrusion.

1. **E-Mail Activity:** ISS regularly reviews information and statistics on users' E-mail activity. The information is reviewed for possible user misuse, for growth trends for capacity planning, or for any other reason deemed necessary by the Company. At any time and without prior notice, the Company reserves the right to examine electronic communications, directories, and files for any reason. *(See the "Manager Access and Review of Associate Communication" Policy for more information.)*

2. **Confidentiality of Messages:** The electronic communication equipment and systems are the property of the Company and are provided to assist all users when conducting Company business. Additionally, all messages composed, sent, or received on the equipment/systems are, and shall

remain, the property of the Company. Users should not assume the confidentiality of any electronic communication, including messages that are active or have been deleted.

Electronic communication should be considered confidential and should be accessed only by the intended recipient. Users are not authorized to retrieve or read any electronic communication that is not intended for their review.

3. **Use in Recruiting:** Users, including those in the HR, Resource Network, and Diversity departments, may not provide information that includes any E-mail address or fax number in any announcement or advertisement for a position vacancy. The announcement or advertisement may, however, include the Company's Website with a specific link to the website where the position description exists.

4. **Personal Messages:** E-mail should be used primarily for legitimate business purposes; however, brief and occasional E-mail messages of a personal nature may be sent and received.

5. **Conflicts of Interest:** Users may not use E-mail to conduct any other business or commercial activities to the extent that such business or commercial activities interfere with the Associate's employment, is competitive with the Company's business, or may be construed as a conflict of interest. As such, Users shall not subscribe to mailing lists or mail services for personal use.

6. **Company Bulletin Boards:** The Company provides electronic bulletin boards for general Company and/or business information distribution. Information or messages posted to these bulletin boards must be related to business or the Company. The Company reserves the right to refuse posting of, or immediate removal of non-approved bulletin messages. Solicitation for personal or non-business purpose is strictly prohibited.

   If a User wishes to post information to the Company electronic bulletin board that is not related to business or the Company, the message must be approved in advance by HR. Non-approved messages may not be sent via electronic communication services to these bulletin boards.

7. **Mandatory Confidentiality Warning:** All electronic communications sent from Company E-Mail servers include the following disclaimer automatically appended to the bottom of all outgoing E-mails to recipients outside of the Company's E-mail server:

   *"**DISCLAIMER Important!** This message is intended for the above named person(s) only and is **CONFIDENTIAL AND PROPRIETARY**. If you are not the intended recipient of this E-mail and have received it in*

error, please immediately notify the sender by return email and then delete it from your mailbox. This message may be protected by the attorney-client privilege and/or work product doctrine. Accessing, copying, disseminating or re-using any of the information contained in this E-mail by anyone other than the intended recipient is strictly prohibited. Finally, you should check this email and any attachments for the presence of viruses, as the sender accepts no liability for any damage caused by any virus transmitted by this email. Thank you."

8. **Use of Customer Electronic Systems:** The use of a customer's or client's electronic system for communication purposes is governed by this Policy. Users must adhere to the confidentiality provisions of this Policy and refrain from transmitting any of the Company's confidential and/or proprietary information, Sensitive Information, or Personal Identity Information via customer or client systems. Specific questions regarding use of such systems should be directed to ISS or HR.

F. Acceptable Use of Company Internet Systems

Users who are authorized to access the Internet should use the Internet for legitimate Company business only. The Company recognizes, however, that Users may need to access the Internet for personal business. Brief and occasional personal use is acceptable, provided such use is not excessive.

Excessive use of the Internet for personal business during work hours is considered outside a User's scope of employment or services and, depending on the severity of the infraction, a user may lose short-term or permanent access to the Internet, and Associates of the Company may be subject to disciplinary action up to and including termination. "Excessive use" is determined by the user's immediate manager or department head, and HR.

1. **Right to Privacy and Internet Activity:** ISS regularly reviews information and statistics on the users' Internet activity. The information is reviewed for possible user misuse, growth trends for capacity planning, or for any other reason deemed necessary by the Company. At any time and without prior notice, the Company reserves the right to examine Internet use, electronic communication, directories and files for any reason. Users, therefore, should not assume a right to privacy. *(See the "Manager Access and Review of Associate Communication" Policy for more information.)*

2. **News Groups, Chat Rooms and Forums:** Only those users or officials who are expressly authorized to speak to the media or to the public on behalf of the Company may represent the Company within any news group, chat room or forum. Users who are not authorized to speak on behalf of the Company, however, may

participate in forums, news groups or chat rooms in the course of business when relevant to their duties, but they shall do so as individuals speaking for themselves.

3. **Personal Interest/Gain:** The Internet shall not be used for any personal monetary interests or gain. Personal Internet use shall not cause the Company to incur a direct cost in addition to the general overhead of an Internet connection.

4. **Intentional Misuse:** Users shall not intentionally use the Internet devices to disable, impair, or overload performance of any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

5. **Software Licensing Agreements:** The Company insists upon strict adherence to software vendors' licensing agreements. When at work or when Company computing and/or network resources are employed, copying of Software in a manner that is not consistent with the vendor's license agreement is prohibited. Participation in pirated software bulletin boards and similar activities represents a conflict of interest to the Company, and is therefore prohibited.

6. **Reproduction of Work:** Reproduction of works posted on the Internet or otherwise available electronically must be done so in accordance with the guidelines established by the author/owner/vendor.

G. Suspected Fraudulent E-mails or Websites

Individuals exist who send fake emails or set up fake Websites that mimic well-known companies for the purposes of tricking the recipient into divulging his/her Personal Identity Information. This practice is known as "phishing." The E-mail will contain a link directing the individual to a site that will request personal and financial information. Users must not access these links. Since it is often difficult to discern fraudulent E-mails from legitimate E-mails, Users must adhere to the following guidelines:

1. Be suspicious of any E-mail with urgent requests for personal or financial information. "Phisher" E-mails are typically NOT personalized while valid messages from a bank or e-commerce company generally are.

2. Refrain from using the links in an E-mail to access any Web page. Instead, attempt to verify the legitimacy of the business. Contact the Company using a phone number that you have located (not one given in the E-mail) or type the web address for the company directly into the browser.

3. Refrain from filling out forms in E-mail messages that request personal and financial information.

4. To ensure a Web browser is secure, check the beginning of the Web address. The address should begin with https:// rather than just http://. Just because an E-mail has official logos does not mean that it is authentic.

5. If a user is unsure about the legitimacy of an E-mail or Website, he/she should contact the IT Helpdesk at 1-888-295-7206 or 704-328-3149.

H. Acceptable Use of Web Logs

"Blogging" is the practice of posting entries in a Web log. A Web log, usually shortened to "Blog," is a web-based publication consisting primarily of periodic entries, or articles, regarding a particular subject, normally in reverse chronological order.

Users must adhere to the following when using Blogs in the course of Company business:

1. **Other parties' legal rights:** Refrain from using, posting or copying third-party materials protected by copyright laws. If protection is in question and the User believes "fair use" rights may allow for such use, posting, or copying, he/she must ensure, without reservation, that the materials are not protected. Refrain from using third-party trademarks, logos, and slogans, as well as disclosing any trade secrets without the third party's permission.

2. **Company confidential and proprietary information:** Refrain from disclosing or discussing Compass' confidential or proprietary information in a Blog. This includes any information covered under a non-disclosure agreement.

3. **Questionable material or material that may be considered offensive or inflammatory by some:** Sexually explicit material, images, stories, cartoons or jokes or links to websites containing or referencing such material are inappropriate for the Company's community Blogs. This applies to unwelcome propositions, sexual advances, requests for dates, and love letters. Refrain from posting articles that contain discussions on race, ethnicity, sexual orientation, national origin, disability or religious or political beliefs, or that disparage others based on any of these.

4. **User Posts:** Users have sole responsibility for material they post. The Company, however, reserves the right to prohibit an User from contributing to a Company Blog, and to remove inappropriate content, or to terminate a Compass Blog at any time, without notice.

5. **BLOG DISCLAIMER: The following disclaimer shall be displayed on each Company Blog:**

   "The thoughts, views, beliefs and opinions expressed in this Blog are those of the individual contributor and do not necessarily represent the positions, views, strategies, opinions or advice of Compass Group USA, Inc. Advertising, spam, flaming, sexually explicit or offensive language

are not permitted. Unlawful, threatening, libelous, defamatory, obscene, profane, discriminatory, racist, homophobic or sexist comments are prohibited. All posted comments, statements, and remarks ("Blog Content") will be open to the public and may be reprinted. Blog Content may be monitored, moderated and/or filtered by the site administrator. Compass Group reserves the right to delete, censor, or exclude any Blog Content it determines in its sole discretion to be inappropriate, detrimental, or disruptive. The posting of Blog Content does not constitute an endorsement by Compass Group. Compass Group is not liable for Blog Content, including any errors or misrepresentations, and the individual contributor is solely responsible for any risk involved with the posting of Blog Content he/she contributes."

Related Policies That May Require Coordination With This Policy:

POLICY REFERENCE	**SECTION**
Information Systems Security	Available from STG
Integrity in the Workplace	Conduct and Work Rules
Management Access and Review of Associate Information	Communications
Progressive Counseling	Performance Management
Sexual Harassment	Conduct and Work Rules
Workplace Harassment	Conduct and Work Rules
Workplace Rules and Regulations	Conduct and Work Rules