COMPASS
GROUP®

North America Division

Information Systems Security Policy

Version 3.33

March 10, 2015

Contents

INTRODUCTION

The information created, processed, and used by Compass Group USA, Inc. (the "Company", including any and all divisions, subsidiaries and affiliated companies) is one of the most valuable assets.
Given the competitive nature of our business and market dynamics, these assets must be protected. The compromise of these assets could severely impact our customers, constitute a breach of regulations, and negatively affect the Company. This document defines the minimum set of requirements for protection of Company assets.

GENERAL INFORMATION

The Company has set a vision and is progressing on a path into the future of enhanced constituent support and service by maintaining a secure and available network of electronic data systems. These systems are interconnected via high-speed switches, routers, and firewalls to allow appropriate access to Company information stored on multiple file servers and databases. The goal is to maintain all of these components, along with the backup devices and supported client PCs, in a manner consistent with industry best practices.

OBJECTIVES

Contained in this document are the policies that direct the processes and procedures by which Compass Group USA, Inc. (the "Company", including any and all divisions, subsidiaries and affiliated companies) strives to maintain a secure and available data enterprise. By employing industry best practices along with proprietary processes we are working to provide due diligence in our best efforts to maintain the confidentiality, integrity, and availability of Company's data resources. This endeavor is truly a partnership, in that all parties involved have a significant stake and responsibility to comply with all agreed-upon policies and procedures to ensure the highest possible level of security. A single weak link anywhere in the chain, from the largest server, to any individual user running an unauthorized program, could compromise the integrity of confidential data or create a catastrophic loss. There are "hostile" applications that can inadvertently or deliberately be run on a PC and cause data destruction or disruption of service to others. The Information Technology Department is constantly working to harden systems against such attacks, and to implement services to screen out hostile mobile code and viruses, but it is still up to each individual user to comply with all revisions of published policies and procedures. Risk assumed by one is shared by all.

Scope

This document is applicable to all Company associates, contractors and suppliers of Compass Group USA, Inc. (the "Company", including any and all divisions, subsidiaries and affiliated companies) who use computer hardware, software or applications to create, manage, process, maintain or distribute Company information assets.

Policy Title:	ACCEPTABLE USE FOR INFORMATION TECHNOLOGY SYSTEMS

POLICY/PURPOSE

Information systems and technology include, but are not limited to all hardware and software provided or supported by the Systems & Technology group ("STG"). Use of the IT systems and technology includes the use of devices on Compass Group USA, Inc. (the "Company") network, systems or data stored on any media that is owned or maintained by the Company. It is the intent of this Policy is to ensure that all authorized users of systems and technology use them in an effective, efficient, ethical and lawful manner. Furthermore this policy intends to prevent company data from being deliberately or inadvertently stored insecurely on a device of carried over an insecure network where it could potentially be accessed by unsanctioned resources.

USERS COVERED BY THE POLICY

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

RESPONSIBILITY FOR ADMINISTRATION

The Systems & Technology Group ("STG"), Human Resources, and all levels of management are responsible for the administration of this Policy. The Information Systems Security ("ISS") Group, a department of STG, will perform regular audits to ensure compliance with this Policy.

ENFORCEMENT

STG will manage security policies, networks, applications, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed a security violation and will be reported to management. STG reserves the right to refuse, by physical and non- physical means, the ability to connect any device to its network. STG will engage in such action if such equipment is being used in a way that puts the Company's or client's systems, data, or users at risk.

Depending on the severity of the violation, a User may lose short-term or permanent access to the technology systems and devices, and Associates of the Company may be subject to discipline up to and including termination.

DETAILS OF POLICY

DEFINITION OF DEVICES

This policy applies, but is not limited, to all devices and accompanying media that fit the following classifications:

- Smart Phones
- Laptop & Desktop computers
- Servers
- Network devices or appliances
- Other mobile/cellular phones
- Tablet computers
- E-readers
- Portable media devices
- PDAs
- Portable gaming devices
- Ultra-mobile PCs (UMPCs)
- Notebook computers
- Any mobile devise capable of storing company data and connecting to a network

PROCEDURES

A. Mandatory Requirements when using Company Technology and Systems

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

2. Users are responsible for ensuring the proper safeguarding of confidential and or proprietary information, Sensitive Information and Personal Identity Information (as defined in Section 3) stored on any computers or devices issued to them. For example, Users must lock or log off the computer when it is not in use.

3. Any company device used to consume Compass Group USA, Inc. technology resources will have installed up-to-date anti-virus and anti-malware software deemed necessary by the STG department. This software is available by contacting the IT Helpdesk (PSG) at 1-888-295-7206 or 704-328-3149.

4. Associates using mobile devices and related software for network and data access will comply, without exception, with the Company IT Access & Password Policy.

5. 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.”

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

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

8. 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 (PSG) at 1-888-295-7206 or 704-328-3149.

9 In the event of a lost or stolen device, including possible misuse of computer resources it is incumbent on the User to report the incident to the **Compass Group Crisis Management Hotline at 1-877-710-6291.**

10. In the event of a lost or stolen mobile device, the device will be remotely wiped of all data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning.

    The remote wipe may destroy all data on the device, whether it is related to a Company business or personal mobile device. **The Compass Group Wireless Network Access & Mobile Device Wipe Waiver, which ensures that the User understands that their personal mobile device data may be erased in the rare event of a security incident or breach, must be signed by the User before connecting the device to corporate resources.**

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

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

4. Copying system configuration files for unauthorized use.

5. 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.

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

7. Sharing or downloading proprietary files without management approval.

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

9. Associates, contractors, and temporary staff will make no modifications to the hardware or software that change the nature of the device in a significant way (e.g. replacing or overriding the operating system or jail breaking the device) without the express approval of the STG department.

C. Acceptable Use of Confidential, Sensitive, and Personally Identity Information (PII)

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 purposes of this Policy, "Personal Identity Information" shall include, without limitation, social security numbers, driver's 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.

Personal information shall not be sent via e-mail, or posted on or transmitted over the internet without prior approval from ISS. Personal Information should never be stored on mobile electronic media (thumb drives, portable disk drives, CD's DVD's) or data storage files accessible company-wide or by the public. Users who share confidential information, Sensitive Information or Personal Identity Information in any medium and/or misuse any information they obtain in the course of their job responsibilities do so at the risk of disciplinary action, up to and including termination of employment.

Requests for data transfers of information described in sections C.1. through C. 3. will be made to STG who will review and implement in accordance with the *"Encryption of Data"* section of the *Information Systems Security Policy.* In addition, occasional requests to transfer data via e-mail may be performed only after approval by STG and in strict accordance with the *"Encrypting Data Files for Sending via E-mail"* procedure. These procedures are available on the Company web site here: *Encrypting Data Files for Sending via E-mail document*

D. Acceptable Use of Company E-Mail

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 Compass Group Owner's Management Suite (OMS) website https://www.compassmanager.com then click the "**administration & support**" tab then the "**MyAccess**" icon or contact IT Helpdesk (PSG) at 1-888-295-7206 or 704-328-3149 if you currently are unable to access the OMS website.

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

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. 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.

4. 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.

5. Mandatory Confidentiality Warning: All electronic communications sent from Company E-Mail servers will include a disclaimer approved by the Legal Department, either with an accompanying URL link or automatically appended to the bottom of all outgoing E-mails to recipients outside of the Company's E-mail server.

6. Use of Customer Electronic Systems: The use of a customer's or clients 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.

7. Suspected or Fraudulent Emails: 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 Emails from legitimate Emails, Users must adhere to the following guidelines:

7.1 Be suspicious of any Email with urgent requests for personal or financial information.

7.2 Refrain from using the links in an Email to access any website. 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.

7.3 Refrain from filling out forms in Email messages that request any sensitive, personal or financial information.

7.4 If a User is unsure about the legitimacy of an Email, he/she should contact the IT Helpdesk (PSG) at 1-888-295-7206 or 704-328-3149. Just because an E-mail has official logos does not mean that it is authentic

E. 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. 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.

3. 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.

4. 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.

5. 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 or copyright laws.

6. Suspected Fraudulent or Bogus websites: To ensure a Web browser is secure, check the beginning of the Web address. The address should begin with https:// rather than just http://. If a User is unsure about the legitimacy of a website, he/she should contact the IT Helpdesk (PSG) at 1-888-295-7206 or 704-328-3149.

F. Acceptable Use of All Social Media, Including Personal Activity

Social media sites include but are not limited to Facebook, Twitter, Linkedin, MySpace or forums, news groups, chat rooms, and also includes any blogging activity such as online diaries with articles, writings, photos, web links or other entities made through "Web logs". Only those Users who are expressly authorized to speak to the media or to the public on behalf of the Company may represent the Company on Social Media sites or any news group, chat rooms, forum or blogs. Users who are not authorized to speak on behalf of the Company, however, may personally participate on Social Media sites or 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 and must follow all Company policies, including, but not limited to, its policies against workplace harassment, discrimination and retaliation and should not discuss the Company its management, supervisor or co-workers in a manner that could defame any individual or damage any person's reputation.

1. Do not use Compass Group Logos or Make Endorsements. Do not use Compass Group logos or any other Compass Group images or iconography on Social Media sites. Do not use Compass

   Group's name to promote or endorse any product, cause, political party, or candidate. Associates' use of Compass Group logos in any medium must be approved by the Company, specifically Corporate Communications.

2 Respect Others' Property and Privacy . Do not reproduce or post reproductions of work without following the guidelines established by the author, owner, or vendor of such work and/or express permission from the author, owner, or vendor.

   Additionally, refrain from using third-party trademarks, logos, and slogans or disclosing any trade secrets without the third party's permission. If applicable, reference website or other sources when posting content to the internet.

   Do not use names, images, or photographs of client(s), Associates, former Associates, vendors, and/or customers without their express consent and prior approval.

3. Respect Company Time and Property. Compass Group computers and time at work are to be used for business-related purposes. Users should not use their Compass Group email accounts to access or identify themselves when engaging in any Social Media activity that is unrelated to their work, and are encouraged to obtain a personal email account for such activity.

4. Proper Identification. Users who are discussing Compass Group's products or services online

should identify themselves as Compass Group Associates, but should not suggest that Compass Group endorses their opinions in any way. An Associate who identifies himself or herself as a Compass Group Associate on a personal site, should use the following disclaimer wherever possible: "The views expressed in this post are my own and do not necessarily reflect the views of the Company".

5. Conflicts of Interest. Do not use Social Media to conduct business or commercial activities that interfere with your employment, compete with the Company's business, or conflict with your responsibilities to the Company.

6. Be Cautious. Remember that you are responsible for any content that you post on Social Media, and that such content may remain accessible to other Users even if it appears to have been deleted from the site where you first posted it. You should monitor your privacy settings carefully, remembering that such settings are subject to change and may not fully protect your content, and that even anonymously posted content may be traced back to you.

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."

FaceBook Disclaimer: The following disclaimer shall be displayed on each Company Facebook Site:
"The thoughts, views, beliefs and opinions expressed by followers "friends, likes" do not necessarily represent the positions, views, strategies, opinions, endorsement 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. Content is monitored and may be deleted, censored, or excluded by the page administrator. Compass Group is not liable for content created by followers, and the individual contributor is solely responsible for any risk involved with posting content he/she contributes. Posted comments, statements, and remarks may be reprinted."

G. Acceptable Use for Company & Personal Mobile Devices

Connectivity of all mobile devices will be centrally managed by the STG department and will use authentication and strong encryption measures. Although STG will not directly manage personal

devices, Users are expected to adhere to the same security protocols when connected to non-corporate equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the Company's infrastructure.

Associates should carry Mobile Computer Devices in hand-held baggage when using public transportation. Associates should not "check" Mobile Computer Devices for transportation by another party.
It is the responsibility of any Associate of the Company who uses a mobile device to access Company resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied.
It is imperative that any mobile device that is used to conduct company business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that User's account.
Based on this requirement, the following must be observed:

1. No Smart Phone/Tablet connection to File Shares.

2. No Smart Phone/Tablet connection to SharePoint unless the service is internet facing within the Company DMZ network and not on the internal corporate network.

3. No remote desktop from smart devices.

4. The only corporate service provided shall be e-mail, tasks, contacts, and calendar.

5. Access requests to Company-provided "mobile" Wi-Fi network will be approved for Users personal tablets or smart phones only after mandatory acceptance of the Company Wireless Access & Mobile Device Wipe Waiver available via the Compass Group Owner's Management Suite (OMS) website https://www.compassmanager.com/admin then click the MyAccess icon and the STG department has confirmed the device presents no risks to Company IT resources.

6. No access to the Company "internal" wireless network will be provided for Users personal devices.

7. Switching from "guest" wireless to the internal wireless networks and gaining unfettered internet access is prohibited.

Acceptable Disposal of End of Lease or End of Life Computer Device's

All company leased & purchased devices will have the appropriate disk cleansing processes applied before their final disposal. Company leased devices will be returned to STG who will perform an initial data cleansing process before sending to the vendor who will perform a secondary data eradication process before disposing of the device. For company purchased devices, the associate will ship the device to the vendor who will perform a three pass data eradication process on the device. (See the "IT Collection and Disposal Services document" for further details.)

Data cleansing and eradication process's for both leased and purchased devices will comply with the DoD 5220.22-M / NIST 800-88 specifications.

Separation/Termination of Employment Computer Devices and Smart Phones:

When an Associate's employment terminates, the Associate's manager must ensure that the Associate returns any Company-issued Computer Device or Smart Phone upon termination. Managers must also immediately inform the IT Helpdesk immediately at 1-888-295-7206 or 704-328-3149 of the Associate's departure from the Company.

Related Policies That May Require Coordination With This Policy:

This policy replaces the following, "Acceptable Use for Information Technology Systems", "Mobile Computers and Wireless Devices" and "Associate Code of Conduct for Social Media". A section "Acceptable Use for Company & Personal Devices" has been added.

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

Policy Title:	IT ACCESS AND PASSWORDS

POLICY/PURPOSE

It is the purpose of this Policy to communicate a mandatory set of standards applicable to all Associates and other authorized users who access any of the Compass Group USA, Inc.'s (the "Company") information technology facilities and systems.

ASSOCIATES COVERED BY THE POLICY

All Associates of the Company are covered by this Policy. Additionally, any individuals provided with authorized access to the Company's information technology facilities and systems are subject to the provisions of this Policy. For purposes of this Policy, the term "User" includes all Company Associates and other individuals authorized to access the information technology facilities and systems.

RESPONSIBILITY FOR ADMINISTRATION

The Systems & Technology Group ("STG"), Human Resources, and all levels of management are responsible for the administration of this Policy. The Information Systems Security ("ISS") Group, a department of STG, will perform regular audits to ensure compliance.

DETAILS OF POLICY

A. Enforcement

STG will manage security policies, networks, applications, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed a security violation and will be reported to management. STG reserves the right to refuse, by physical and non-physical means, the ability to connect any device to its network. STG will engage in such action if such equipment is being used in a way that puts the Company's or client's systems, data, or users at risk.

Depending on the severity of the violation, a User may lose short-term or permanent access to the technology systems and devices, and Associates of the Company may be subject to discipline up to and including termination.

B. Security Access Warnings, Monitoring, and Unauthorized Access

The following notice will be displayed, where possible, upon access to any Company-owned information technology facilities and systems.

"This Computer system is for authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel. If necessary appropriate action will be taken against individuals when misuse, and/or unauthorized use is detected. These actions could result in counseling, suspension or employment termination depending upon severity. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the

evidence of such monitoring to law enforcement officials."

The Company reserves the right to change this notice at any time.

C. SAP Considerations

Due to the sensitivity and confidentiality of the data stored in SAP, a separate Policy exists specifically outlining the guidelines for SAP access and control. A detailed "SAP Security Policy" is available from STG if further information is needed.

D. Controls for System Access

1. Access request forms for applicable systems must be submitted for new system users. For further information, contact the IT Helpdesk at 1-888-295-7206 or 702-328-3149.
2. Access levels to computer systems are conservatively granted and only the lowest level privilege necessary to fulfill a User's responsibilities will be granted. Access will be granted only to the information required for a User to perform his/her job.
3. Unique identification via a user ID and password is required for each individual User prior to the initiation of any user session such that the Company may ensure clear accountability for all actions performed by the User.

E. Wireless Guest Access Provisioning Guidelines

1. Guest Account User Name

The User Name of the guest will be created using the format firstname.lastname where firstname and lastname correspond to the actual name of the guest user.

2. Guest Account Password

The Password of the guest account will be a secure randomly generated password which will be generated by using the integrated "Generate Password" functionality in the Wireless Control System interface.

3. Additional Account Details

The requestor name (the person who initiated the request for an account created) and the company name which the account is being created for will be logged in the Description field in the Account Creation Area of the Wireless Control System interface in the format "Requestor Name – Company".

4. Account Validity Period

All accounts will be set to 14 days or less unless a specific reason is given and approved by the person creating the account. The reason provided will be added to the end of the description field in the Account Creation Area of the Wireless Control System interface.

Accounts will not be created without an expiration date unless explicitly approved by the Information Systems Security group.

F. Disabling Requirements

To help prevent unauthorized access to the Company's information technology facilities and system, the following security measures are required:

1. **Initiation of time-outs or screen lockout:** After a maximum of 30 minutes of inactivity, including background processing or executing activity, individual system user sessions will either time-out or initiate screen lockout using password-protected screen savers.

Note: Certain systems designed to perform background processing may be exempted from this requirement based on legitimate business needs, provided the computer device is in a secured environment.

2. **Disabling or Deleting User IDs:** User IDs for Users, consultants, and vendors must be disabled after a maximum of 90 days of inactivity, and then deleted after an additional maximum of 90 days of inactivity, as permissible. Functional IDs and emergency User IDs issued based on a determination of legitimate business need may be exempt from this requirement, if approved by management. Associates on Company-approved leave of absence may also be exempt from this requirement.
3. **Disabling User IDs after failed logins:** User IDs associated with a password must be disabled after a maximum of ten (10) consecutive failed login attempts. The User ID will not be re-enabled until a legitimate explanation for disablement is identified by STG.

G. Password Management

All Company information technology facilities and systems require entry and systematic verification of a User's password prior to the initiation of a user session. It is the responsibility of each User to protect his or her password.

1. **Confidentiality:** Users should never share passwords or give them over the phone. If anyone requests a User's password over the phone, the User must decline and immediately contact his/her supervisor and the IT Helpdesk at 1-888-295-7206 or 704-328-3149. If a password is suspected of having been compromised, the owner of the password must immediately inform his/her supervisor and the IT Helpdesk at 1-888-295-7206 or 704-328-3149.
2. **Password Expiration:** Passwords should be set to expire every 90 days.
3. **Setting Passwords:**
   a. Default and vendor-supplied passwords should be changed immediately.
   b. User IDs must not be identical to the corresponding passwords.
   c. Passwords must never be displayed or echoed in clear text on the screen.
   d. Users must select passwords, unless randomly generated.
4. **Length and Complexity of Passwords:**
   a. Passwords must contain at least eight (8) characters.
   b. Passwords must not contain the user's Account Name
   c. Passwords must contain characters from three of the following four categories:
      - Uppercase characters (A through Z)
      - Lowercase characters (a through z)
      - Base 10 digits (0 through 9)
      - Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

5. **Temporary Password Assignments:** In the event a user forgets his/her password, the following procedure must be followed;
   A user who forgets his/her password should utilize MyAccess, the corporate self-service password utility which will allow them to reset the password once they have correctly answered their security questions.
   If the user had not previously set up their security questions they must call the IT Helpdesk at 1-888-295-7206 or 704-328-3149 so the technician can confirm their identity and walk the through setting up their security questions and changing their password.
6. **Password Cracking:** Password cracking occurs when an individual uses a computer program, commonly known as a "password cracker," to identify an unknown or forgotten password to a computer or network device. A password cracker may also be used to help an individual "crack" or obtain unauthorized access to resources.
   It is a violation of this Policy for anyone to run any type of password cracking program or network penetration testing. Anyone found to be conducting or involved with password cracking may be subject to discipline up to and including termination.

H. Access to User Accounts and Passwords

Managers and/or supervisors requesting access to any User's accounts or passwords should seek approval from a Senior HR Consultant or Senior HR Director and then submit this approval along with the request to HR IT Security for further approval. For more information regarding access to user accounts and passwords, refer to the "Manager Access and Review of Associate Communications" Policy.

Related Policies That May Require Coordination With This Policy:

POLICY REFERENCE	SECTION
Manager Access and Review of Associate Information	Communications
Personnel Record Retention Policy	Admin and Recordkeeping
Progressive Counseling Policy	Performance Management SAP
Security Policy	Available from STG Workplace
Rules and Regulations Policy	Conduct and Work Rules

Policy Title:	MOBILE COMPUTER AND WIRELESS DEVICES

POLICY/PURPOSE

Mobile Computer and Wireless Devices (defined below) allow Associates to be more productive while away from the office. The use of such technology may create risks of information disclosure, and theft, and perhaps offer an unauthorized point of access to the Company network. To minimize the potential risks associated with the use of such technology, the Company has implemented this Policy.

ASSOCIATES COVERED BY THE POLICY

All Associates of the Company are covered by this Policy. Additionally, other users of Company- issued Mobile Computer and/or Wireless Devices are subject to the provisions of this Policy. Sections IV.B. and IV.C. of this Policy set forth the equipment considered Mobile Computer and Wireless Devices.

RESPONSIBILITY FOR ADMINISTRATION

The Systems & Technology Group ("STG"), Human Resources, and all levels of management are responsible for the administration of this Policy. The Information Systems Security ("ISS") Group, a department of STG, will perform regular audits of Mobile Computers and Wireless Devices use to ensure compliance with this Policy.

DETAILS OF POLICY

Enforcement

STG will manage security policies, networks, applications, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed a security violation and will be reported to management. STG reserves the right to refuse, by physical and non-physical means, the ability to connect any device to its network. STG will engage in such action if such equipment is being used in a way that puts the Company's or client's systems, data, or users at risk.

Depending on the severity of the violation, a User may lose short-term or permanent access to the technology systems and devices, and Associates of the Company may be subject to discipline up to and including termination.

Definition of Mobile Computer Devices

A Mobile Computer Device is electronic hardware that is lightweight and portable. For the purposes of this Policy, equipment considered to be Mobile Computer Devices includes, without limitation:

1. Smart phones
2. Laptop & Desktop computers
3. Tablet computers
4. Portable Media devices

5. Personal Digital Assistants (PDAs)
6. Portable gaming devices
7. Ultra-mobile PCs (UMPCs)
8. Notebook computers
9. E-Readers
10. Any mobile device capable of storing company data and connecting to a network

Definition of Wireless Devices

A Wireless Device is electronic hardware that allows transfer of information over a distance without the use of electrical conductors or wires. Equipment considered to be Wireless Devices includes, without limitation:

1. Cellular Telephones
2. Smart Phones
3. Personal Digital Assistants (PDAs)
4. Wireless Networking
5. Two-Way Radios
6. Tablet computers
7. E-Readers
8. Portable gaming devices
9. Ultra-mobile PCs (UMPCs)
10. Notebook computers
11. Any mobile device capable of storing company data and connecting to a network

Issuance of Mobile Computer Devices

Managers are responsible for reviewing and approving Associates‟ orders for Mobile Computer Devices before orders are placed. Delays in approving orders will delay the delivery of the Wireless Devices. Once the manager approves the request and submits the order to STG, STG will pre-install the required software, including an active and current virus scanner, before delivering the Device to the Associate. Should the manager or Associate need advice for selecting a Mobile Computer Device, he/she may contact the IT Helpdesk at 704.328.3149 or 1.888.295.7206.

Security Provisions

An Associate who has been issued a Mobile Computer Device is responsible for safeguarding equipment and data from theft and is required to comply with the following provisions:

1. In the event a Mobile Computer Device is stolen or misplaced, Associates must immediately contact the **Compass Group Crisis Management Hotline** at 1.877.710.6291.
2. Mobile Computer Devices must comply, to the extent possible, with the requirements of the “IT Access and Password Policy.”
3. Associates should carry Mobile Computer Devices in hand-held baggage when using public transportation. Associates should not “check” Mobile Computer Devices for transportation by another party.
4. Confidential, sensitive, or personal identity information should not be transported on Mobile Computer Devices unless the information is encrypted. For definitions of confidential, sensitive, personal identity information see section IV.F. of this Policy.
5. Associates should turn off Mobile Computer Devices and modems when not in use.

Confidential, Sensitive, and Personal Identity Information

For the purposes of this Policy, confidential, sensitive, and personal information are defined as follows:

1. Confidential Information: Without limitation, this information includes Company information that may be considered copyrighted materials, trade secrets, or financial information. All such property is the sole property of the Company.
2. Sensitive Information: Without limitation, this information includes 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: Without limitation, this information includes user ID‟s and passwords, social security numbers, driver's license numbers, state identification card numbers,credit or debit card numbers, bank account numbers, passport numbers, alien registration numbers, and health insurance identification numbers.

Use of Wireless Devices

Use of a Company-issued Wireless Device is a privilege and is provided to improve operations and service, and to enhance operating efficiencies. Wireless Devices should be used for business purposes only and should not be used as an Associate's primary mode of communication. They should be used only when such use is the most cost-effective way to conduct business.

Misuse of a Wireless Device and/or excessive use of a Wireless Device for personal business will result in revocation of its use and forfeiture of the Wireless Device**,** and may result in disciplinary action up to and including termination.

Issuance of Cell Phones

It is the responsibility of the Associate's immediate supervisor to determine if a cell phone is warranted. The purchase of cell phones, features and accessories will be limited to the approved catalog, which is available on the web at http://compasswireless.nrghd.com. The Company may issue a cell phone to an Associate provided at least one of the following two criteria is met:

1. The job function of the Associate requires considerable time outside of his/her assigned office or work area, and it is important to the Company that the Associate is accessible during those times.
2. The job function of the Associate requires him/her to be accessible outside of scheduled or normal working hours.

NOTE: Convenience is not a criterion for the determination of need.

Issuance of Blackberries

An Associate may be assigned a Company-issued Blackberry if it is a business necessity that he/she respond to e-mail immediately as a part of his/her job responsibilities, and the Associate is not able to do so with a laptop or desktop computer. If an Associate is able to perform his/her job function by responding to e-mail upon return to his/her laptop or desktop computer, Blackberry service is not warranted and should not be approved. If an Associate is issued a Blackberry and also has a Company-issued cell phone the Associate must forfeit the Blackberry and use the Blackberry for voice and data services. The existing Company- issued cell phone number may be transferred to the Blackberry.It is the responsibility of the Associate's immediate supervisor to determine if a Blackberry is warranted. An Associate may receive a Company-issued cell phone provided certain criteria below are met.

Criteria number one (1) **must** be met, in addition to **either** number two (2) or three (3).

Criteria:
1. The Associate works away from his/her desk 75% of the time; and
2. The Associate has direct contact with external clients and must be highly responsive to client communications at all times; or
3. The Associate must frequently communicate with teammates during client meetings.

NOTE: Convenience is not a criterion for the determination of need.

Issuance of Air Cards

While the Company recognizes that many Associates may find it convenient to have access to Wide Area Networks through the use of Air Cards (as with Blackberries), managers may only approve an Air Card when it is critical for meeting the demands of the business.

NOTE: Convenience is not a criterion for the determination of need.

Separation / Termination of Employment

1. Mobile Computer Devices: When an Associate's employment terminates, the Associate's manager must ensure that the Associate returns any Company-issued Mobile Computer Devices upon termination. Managers must also immediately inform the IT Helpdesk immediately at 1-888-295-7206 or 704-328-3149 to inform the Helpdesk of the Associate's departure from the Company.
2. Wireless Devices: When an Associate has retired, resigned, or been terminated from the Company, or has been transferred or promoted to a position that does not require the use of a Wireless Device, such Associate will not be permitted to keep Company-issued phones or transfer the established Company phone number to a personal account.

   Exceptions to this provision must be approved by senior level management.

Use of Company Wireless Devices in Motor Vehicles

The safe operation of motor vehicles is dependent upon a number of factors. One of the most important is staying focused on the task of driving. The use of any Wireless Device can be a distraction, and cause or contribute to an incident. While simple conversation may not significantly affect driving ability adversely, complex business-related or other conversation might disrupt an associate's ability to concentrate on driving conditions.
The use of Company-issued Wireless Devices in motor vehicles must never compromise safety.
Associates using Company-issued Wireless Devices must comply with the following requirements when operating Company, rental or personal vehicles.

1. Refrain from placing calls while operating a Company vehicle, unless absolutely necessary and a hands-free or headset option is available.
2. If a call is received while driving, the phone should not be answered until the vehicle is safely off the highway and stopped, unless the Wireless Device is equipped with a hands-free device or headset.
3. Refrain from composing e-mails and text messages while the vehicle is in motion.
4. When an Associate finds it necessary to review voice mail and/or use other Company- issued Wireless Devices, the Associate must pull off the road into a designated parking area. The parking area must not be on or near the traveled roadway.

5. Refrain from attempting to pull over and to park in the breakdown lane on interstates or limited access highways to use a Wireless Device as this presents a dangerous merge situation with other vehicles traveling at high speeds.

State and Local Laws and Regulations

Where state and/or local law prohibit the use of Wireless Devices, hands-free technology and/or headsets, the Company requires that Associates adhere to the laws and regulations prohibiting such use. Associates who receive citations due to violating these laws and regulations will be held liable for any monetary or other consequences. The Company will not provide assistance, monetary or other, to an Associate who receives a citation.

Any violation of this Policy may result in disciplinary action, up to and including termination. For information regarding the use of Wireless Devices in Company motor vehicles, refer to the "Use of Wireless Devices in Company Motor Vehicles" Policy.

Related Policies That May Require Coordination With This Policy:

IT Access and Passwords
Acceptable Use for Information Technology Systems
IT Network Policy

Policy Title:	IT NETWORK CONNECTIVITY

POLICY/PURPOSE

This policy describes how third parties, divisions, subsidiaries and affiliated companies electronically connect to Compass Group USA, Inc. networks to transact business.

ASSOCIATES COVERED BY THE POLICY

This policy applies to all Compass Group USA, Inc. (the "Company", including any and all divisions, subsidiaries and affiliated companies) associates, temporary service personnel, and consultant/contractor personnel engaged by the Company to implement and support Information Technology Network Services

RESPONSIBILITY FOR ADMINISTRATION

The Compass Group IT Network Department will ensure they adhere to the policy. The IS Security Department will perform timely audits to ensure compliance.

ENFORCEMENT

Non-compliance with this policy is a security violation and will be reported to management. Depending on the severity of the infraction, a user could lose short term or permanent access to the system, be sent to counseling, suspended or terminated.

DETAILS OF POLICY

A. Definition of Terms

Extranet	An extranet is a private network that uses the Internet protocol and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or any other business.
Circuit	For the purposes of this policy, circuit refers to the method of network access, whether it's through traditional Broadband/DSL, Frame Relay etc., or via VPN/Encryption technologies.
MPLS	Multiprotocol Label Switching (MPLS) is a mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path.
ESB	An enterprise service bus (ESB) is a software architecture model used for designing and implementing the communication between mutually interacting software applications
Third Party	A business that is not a part of Compass Group USA, Inc. (the "Company",including any and all divisions, subsidiaries and affiliated companies.

B. General Scope

Connections between third parties that require access to non-public Company resources fall under this policy, regardless of whether a telecommunication circuit (such as frame relay, MPLS, Broadband, or DSL) or ESB (Enterprise Service Bus) is used for the connection.

C. Proprietary Information Awareness

Regardless of actual connectivity to company resources and in order to protect the company's proprietary and confidential information, vendors, suppliers and any external consultants may be required to sign the Company Non-Disclosure Agreement.

D. Security Review

All proposed and existing extranet connectivity must go through a security review with the IS Security department .The reviews are to ensure that all access requests match the business requirements in a best possible way, and that the principle of "least access" is followed.

E. Business Case

All proposed and existing extranet connections must be accompanied by a valid business justification, in writing, from the sponsoring department to the IT Network Services Department. Project or service approval must be completed by the sponsor and forwarded to the IT Network Department after validation they shall forward the justification to the IS Security Department for sign off.

F. Point Of Contact

The Sponsoring department must designate a person, normally the STG Project Director/Manager to be the Point of Contact (POC) for the extranet connection. The POC acts on behalf of the Sponsoring department, and is responsible for ensuring all appropriate parties (IT Network Department, IS Security Department) have been involved and appropriate sign off established.

G. Establishing Connectivity

The POC will then seek approval through all appropriate parties then submit a request via the Release Management Process, failure to provide a fully completed and authorized Change Control will result in the request being denied.

Prior to any physical connection between a third party and the company's network the following steps must have been approved and taken;

Connectivity assessment of third party
Authorized and approved Justification
Verification and approval via Release Management Process

All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will The Company rely upon the

third party to protect the Company's network or resources.

H. Modifying or Changing Connectivity and Access

All changes to access must be accompanied by a valid business justification and are subject to security review. All changes must be done in accordance with Release Management Process.

I. Terminating Access

When access is no longer required the POC must notify both Release Management and the IT Network Department. These connections will be terminated immediately via the Release Management Process.

J. Peer to Peer Network or Applications

Due to the high potential for data compromise these types of services are not permitted on the Compass Group USA, Inc. (the “Company”, including any and all divisions, subsidiaries and affiliated companies) network unless explicitly approved by the Compass Group IS Security Department.

K. Enforcement

Non-compliance with this policy is a security violation and will be reported to management. Depending on the severity of the infraction, a user could lose short term or permanent access to the system, and would be subject to disciplinary action up to and including termination.

Policy Title:	DATA CENTER

POLICY/PURPOSE

This section defines the policies used to secure Compass Group USA, Inc. (the "Company", including any and all divisions, subsidiaries and affiliated companies) Data Centers.

ASSOCIATES COVERED BY THE POLICY

The Data Center area is restricted to operational/ support associates and vender support personnel.

RESPONSIBILITY FOR ADMINISTRATION

The IS Security Department in conjunction with the IT Technical Services Department

DETAILS OF POLICY

To maintain proper computer room security and safety, the following polices must be in place.

Restricted Access

The Data Center area is to be locked at all times.
A system is necessary allowing only authorized personnel to gain entry to the area.
Those persons needed to operate, supervise, or provide maintenance to the area and its equipment.
Additionally a record, of all who gain entry to the Data Center, together with the time of entrance and departure, will be kept, using a sign-in/out log or a Computer ID card door-opening system that has such features.
Tours of the data center by Company associates, vendors, or customers must be authorized and approved by the Data Center Supervisor.

Operational Responsibilities

Location of fire alarms, extinguishes, and controls for firefighting systems. Emergency power-off procedures.
Escalation procedures for Security Alert escalation. Emergency procedures for notifying the emergency services.

Data Center Environment

Equipment must be regularly maintained and where applicable certified for use. The following points must be observed

Low Profile at the Data Center

The Data Center must maintain a low profile. No signs directing persons to the center should be displayed.

Power Supply

The Data Center area must have its own connected to the main power source for the building. A backup UPS (uninterrupted power supply) or a fail-safe device is required to prevent system outages if the main power fails. A battery or self-starting generator should be available to provide emergency power for work lights, room ventilation, and air conditioning.

Air Conditioning

The Data Center must have its own back-up air conditioning system.

Construction Hazards

The Data Center must not be adjacent to any natural gas or liquid-transporting pipes, high voltage lines, or magnetic radiation sources.

Fire Precautions

Fire extinguishers should be the safest possible, and appropriate to the type of fire that may occur. All materials used in constructing the Data Center must be fireproof where possible.

Smoke Detectors

Smoke detection equipment must be installed

Temperature and Humidity Gauges

Temperature and humidity gauges must be installed

Enforcement

Any noncompliance with these requirements will constitute a security violation and will be reported to management; this may result in short-term or permanent loss of access to company Information Technology Systems.
If necessary appropriate action will be taken against associates, temporary service, consultant or contractor personnel when misuse, and/or unauthorized use is detected. These actions could result in counseling, suspension or employment termination depending upon severity.

Policy Title:	**DATABASES**

POLICY/PURPOSE

This policy outlines the requirements for database security and securely storing and retrieving database credentials, for use by a program that will access a database running on one of the Compass Group USA, Inc. (the "Company", including any and all divisions, subsidiaries and affiliated companies) systems.
Computer programs running on the Company's networks often require the use of one of the many internal database servers. In order to access one of these databases, a program must authenticate to the database by presenting acceptable credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

ASSOCIATES COVERED BY THE POLICY

This policy applies to all Company associates, temporary service personnel, and consultant/contractor personnel engaged by the company, or external sources authorized to access Company electronic facilities

RESPONSIBILITY FOR ADMINISTRATION

It is the responsibility of all levels of management of the Information Technology Department furthermore the IS Security Department will perform timely audits to ensure compliance to the policy.

DETAILS OF POLICY

Definitions of Terms

Audit Trail	In computing, the term is used for an electronic log used to track computer activity.
Computer language	A language used to generate programs.
Credentials	Something you know (e.g., a password or pass phrase), and/or something that identifies you (e.g., a user name, a fingerprint, voiceprint, retina print). Something you know and something that identifies you are presented for authentication.
Entitlement	The level of privilege that has been authenticated and authorized. The privileges level at which to access resources.
Executing body	The series of computer instructions that the computer executes to run a program.
File Systems	A file system is the way in which electronic files are named and where they are placed logically for storage and retrieval.
Hash	An algorithmically generated number that identifies a datum or its

location.

LDAP	Lightweight Directory Access Protocol, a set of protocols for accessing information directories.
Module	A collection of computer language instructions grouped together either logically or physically. A module may also be called a package or a class, depending upon which computer language is used.
Name space	A logical area of code in which the declared symbolic names are known and outside of which these names are not visible.
Production	Software that is being used for a purpose other than when software is being implemented or tested.
Scripts	A script is a computer program or sequence of instructions. Transaction Integrity A sequence of information exchange and related work, which assures the data, is not altered by any un-authorized process.

Scope

This policy applies to all software that will access a Company, multi-user production database.

General

In order to maintain the security of Company's internal databases, access by software programs must be granted only after authentication with credentials. Database credentials must not be stored in a location that can be accessed through a web server.

The following policy statements must be observed when deploying/configuring or maintaining databases within the Company IT infrastructure.

- Install known vendor security patches as soon as vulnerabilities are announced
- Document where detailed Security topics for each database can be found.
- Always use a database certified to industry security standards.
- Use different passwords for database administrator and system administrator.
- The database should be started under a dedicated user e.g. Oracle, If possible this account should be locked.
- Passwords and usernames should not be passed in clear text over the network.

Even if a system is evaluated to a certain security level, it still requires careful configuration, monitoring and organization processes for it to be considered "secure" in a real production environment.

Storage of Data Base User Names and Passwords

Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable.

Database credentials may reside on the database server. In this case, a hash

number identifying the credentials may be stored in the executing body of the program's code.

Database credentials may be stored as part of an authentication server, such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.

Database credentials may not reside in the document tree of a web server.

Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.

Passwords or pass phrases used to access a database must adhere to the Access and Password Policy.

Retrieval of Database User Names and Passwords

If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.

The scope into which you may store database credentials must be physically separated from the other areas of your code; e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.

For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

Access to Database User Names and Passwords

Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.

Database passwords used by programs are system-level passwords as defined by the Access and Password Policy.

Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Access and Password Policy.
This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

Transaction Integrity

The following statements must be observed in order to preserve transaction integrity. Database engines protect data integrity with their *rollback*/*rollforward* recovery mechanisms.

The *two*-phase *commit* commands can guarantee the integrity of distributed databases, if used correctly in applications.Referential integrity in relational databases is enhanced by the use of

triggers (Sybase, SQL Server, and Oracle).

Audit Trail

Where possible the Audit Trail facility must be enabled. Administrators should document non-standard installations.
Logs should be stored so they can be analyzed for security breaches or strange behavior.

File Systems and Scripts

Database administration scripts should only be readable by the database administrator.
Create a group (e.g. oracle) for those users who need access to database toolsdirectly. File and directory permissions must be set restrictively for the databases home directory and where the configuration and executable files are kept.
Set ownership/permissions of files and devices restrictively - only the database should be able to read or write these devices and files

Enforcement

Any noncompliance with these requirements will constitute a security violation and will be reported to management; this may result in short-term or permanent loss of access to company Information Technology Systems.
If necessary appropriate action will be taken against associates, temporary service, consultant or contractor personnel when misuse, and/or unauthorized use is detected. These actions could result in counseling, suspension or employment termination depending upon severity.

Related Policies That May Require Coordination With This Policy:

Acceptable Use for Information Technology Systems
IT Access and Passwords
SAP Policy

Policy Title:	**ENCRYPTION OF DATA**

POLICY/PURPOSE

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

ASSOCIATES COVERED BY THE POLICY

This policy applies to all Compass Group USA, Inc. (the "Company", including any and all divisions, subsidiaries and affiliated companies) associates, temporary service personnel, and consultant/contractor personnel engaged by the company, or external sources authorized to access Company electronic facilities

RESPONSIBILITY FOR ADMINISTRATION

All Information Technology and Information Systems departments will ensure they adhere to the standards defined. The IS Security Department will perform regular audits to ensure compliance.

DETAILS OF POLICY

Definition of Terms

Encryption	The conversion of data into a form called ciphertext that cannot be easily understood by unauthorized people.
Decryption	The process of converting encrypted data back into its original form, so it can be understood.
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric Cryptosystem	A method of encryption in which two different keys is used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

Generall

Proven, standard algorithms such as AES, Triple-DES, RSA, or SHA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. The Company's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by IS Security Department.

The U.S. Government restricts the export of encryption technologies. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

Company Specific

The following methods of encryption shall be adopted and deployed where appropriate.

VPN	Employing Triple-DES encryption (Remote Network Connections) SSL Web based
SSH	Unix remote connections PGP E-mail and or FTP sessions
S/MIME	Digital Certificates for E-mail AS2 ESB file transfers
WPA2	Minimum Security Protocol for secure Wi-Fi

Enforcement

Any noncompliance with these requirements will constitute a security violation and will be reported to management; this may result in short-term or permanent loss of access to company Information Technology Systems.
If necessary appropriate action will be taken against associates, temporary service, consultant or contractor personnel when misuse, and/or unauthorized use is detected. These actions could result in counseling, suspension or employment termination depending upon severity.

Related Policies That May Require Coordination With This Policy:

VPN Policy
Acceptable Use for Information Technology Systems
Servers, Desktops and Workstations

Policy Title:	SAP SECURITY

POLICY/PURPOSE

A standard security approach is required for Company associates within Compass Group USA, Inc. (the "Company", including any and all divisions, subsidiaries and affiliated companies) who have authorized access to the SAP system. The main objective is to implement a tightly controlled security policy to eliminate any possibilities of business corruption.
This document provides the framework for SAP Security. It also provides the necessary guidelines defining roles, responsibilities and actions.

ASSOCIATES COVERED BY THE POLICY

All authorized Company associates who have access to the SAP system

RESPONSIBILITY FOR ADMINISTRATION

The BASIS IT Technical Services Team is responsible for ensuring that this policy is maintained to ensure that;

- Only authorized Company associates have the correct access levels in order to perform their work.
- Unauthorized Company associates are unable to gain access to the SAP system or to certain data and any potential security breaches are detected.

Security of the R/3 system is also dependent on the security of the operating system under which it operates; The Unix IT Technical Services Team holds this responsibility.
The IS Security Department will perform timely audits to ensure compliance of policy.

DETAILS OF POLICY

User Management

The BASIS IT Technical Services Team must ensure that the security policy and procedures are maintained and all instructions are followed. All access levels must be tightly controlled and monitored across all clients. They are responsible for maintaining user profiles and authorizations, restricting access according to their job roles.

Any security breaches or unusual patterns must be reported to the IS Security Department.

Technical Support Access Privileges

The BASIS IT Technical Services Team is declared as privilege users and has elevated access in order to maintain and support all functions in the system:

SAP System Ids

OSSIN* (SAP service accounts) should be locked at all times and are to be unlocked for online support and/or Early Watch sessions from SAP.

SAP * is used for client copies and is defined in the system code itself.

SAPCPIC is an internal logon and is used solely to call external programs. This should not be locked or deleted.

Users Ids

Users are client specific and they must be separately defined for each client in the system.

All user ids must be unique and adopt the format as defined in the Access and Password Policy.

User ids **SHOULD NOT** be shared.

Passwords

All password creation will conform to the Access and Password Policy.

User Authorizations

Authorizations should be explicitly assigned via profiling at job function, company code and transaction.

User cannot execute transactions unless he/she has been given the defined authorization for the system.

Individuals can be held responsible for actions that they perform using the system.

Process

All requests for new user setups and user profile amendments should be logged via the ticketing system Remedy.

Requests can be made employing electronic online services, consult with the Helpdesk for further information.

Account creation will be managed via the BASIS IT Technical Services Team.

New users where possible must have completed relevant SAP training courses prior to being set up.

Role approvers must approve user setup and/or profile amendments prior to granting the requested authorization.

User ids that have become locked due to incorrect logon attempts should not be reactivated until investigation and a satisfactory explanation. Reactivation will be performed by the BASIS IT Technical Services Department.

The BASIS IT Technical Services team is notified automatically of staff terminations.

SAP Audit

All production SAP accounts will be reviewed on a monthly basis.

- Standard Dialog Accounts are disabled after 90 days of inactivity.
- Standard Dialog Accounts are deleted after 180 days of inactivity.
- Contractor Dialog Accounts are deleted after 90 days of inactivity.
- New Dialog Accounts never used in 90 days are deleted.
- CPM only accounts are deleted after 365 days of inactivity.
- Users will be deleted immediately upon leaving the company

OSS Development keys must be controlled and monitored on a regular basis.

Segregation of Duties

Where practical, the creation of new profiles and their allocation to users should be performed by different individuals.

SAP System Security

Users should logoff SAP completely when away from their desks, furthermore workstations connected to SAP should conform to the Disabling Requirements (Section C) of the Access & Password Policy which helps to prevent any unauthorized users gain access to the system.
Users are restricted to logging on just once to the SAP R/3 system.
In addition the application has the timeout non-active sessions set to 90 minutes.

SAP Security Control

Security forms are to be completed for all requests as these determine access levels.
BASIS IT Technical Services Team is responsible for applying relevant authorizations & profiles to the user master record.

SAP Security

Users must only be logged onto SAP once. However, once logged on, they can use up to 6 sessions.

Monitoring SAP Security

The BASIS IT Technical Services Team is to ensure that these controls are properly maintained on a regular basis. Audit trails, where possible, must be followed and investigated. In addition the monitoring of user profiles must take place to ensure that no unauthorized changes have been made.

Enforcement

Any noncompliance with these requirements will constitute a security violation and will be reported to management; this may result in short-term or permanent loss of access to company Information Technology Systems.
If necessary appropriate action will be taken against associates, temporary service, consultant or contractor personnel when misuse, and/or unauthorized use is detected. These actions could result in counseling, suspension or employment termination depending upon severity.

Related Policies That May Require Coordination With This Policy:

Databases
IT Access and Passwords
Acceptable Use for Information Technology Systems

Policy Title:	PCI COMPLIANCE

POLICY/PURPOSE

Protection of customer credit card information is important to Compass Group and its clients. Security of cardholder data is governed by the Payment Card Industry ("PCI") Security Standards Council. This Policy outlines the responsibility and standards related to protection of credit and debit card numbers and other customer information in accordance with PCI data security standards. All references to credit cards in this Policy are also applicable to debit card transactions.

ASSOCIATES COVERED BY THE POLICY

This Policy applies to all Company locations accepting credit or debit cards as a form of payment.

RESPONSIBILITY FOR ADMINISTRATION

The PCI Steering Committee and all levels of management.

ENFORCEMENT

Non-compliance with this Policy is a security violation and will be reported to management. Depending on the severity of the infraction, a user may lose short term or permanent access to the system, and/or be subject to disciplinary action up to and including termination.

DETAILS OF POLICY

PROCEDURES TO ENSURE COPLIANCE

It is the Company's policy to comply with the security standards published by the PCI Security Standards Council. Company locations must ensure that the following 6 Goals of PCI DSS and the 12 associated requirements are in place to comply with PCI data security standard requirements:

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

ADDITIONAL PROCEDURES

To reduce overall risk to Compass there are additional company specific procedures that must be adhered to:

1. Compass Group locations accepting credit cards must operate in a secure network environment.

a. Locations utilizing high-speed internet access must be secured by a Compass approved router and/or firewall. Wireless network configurations are considered high risk and shall be carefully evaluated. Isolated networks for the credit card processing application are preferred.

b. Old copies of databases, spreadsheets, and other documents that contain credit/debit card data are to be securely erased.

2. All Compass locations accepting debit or credit card payments must utilize a PA-DSS (Payment Application - Data Security Standard) certified payment application (e.g. point of sale software, catering order software, cashless software, kiosk software). New merchant identification numbers (MIDs) will not be issued to locations using a non-certified payment application.

3. No Compass Associate shall permit any alteration to a location's payment application or computing/network environment without first notifying ***creditcards@compass-usa.com*** for evaluation and approval**.**

4. All vendor agreements involving credit or debit card payments shall provide for the vendor to protect cardholder data in compliance with all applicable laws, regulations and PCI data security standards. If the vendor provides a credit or debit card payment solution, the vendor's solution must maintain certification with the PCI Security Standards Council.

5. Client agreements that involve locations in which the credit or debit card payment system interfaces or interconnects with a client system should include a provision that requires the client to reasonably cooperate with Compass to ensure Compass's compliance with PCI data security standards.

Policy Title:	POINT OF SALE CREDIT CARD AND DEBIT CARD MASKING

POLICY/PURPOSE

Protection of customer credit card information is important to Compass Group and its customers, and it is the law. This Policy outlines the responsibility and standards related to protection of credit and debit card numbers and other customer information. All references to credit cards in this Policy are also applicable to debit card transactions.

ASSOCIATES COVERED BY THE POLICY

Associates responsible for securing customer credit and debit card information at all Company locations accepting credit or debit cards as a form of payment.

RESPONSIBILITY FOR ADMINISTRATION

The Treasury Department and all levels of management are responsible for the administration of this Policy.

DETAILS OF POLICY

A. Standard

Compass Group locations must follow all policies and laws related to securing customer credit card information. This includes properly masking customer credit card numbers and expiration dates on customer receipts. All merchant copies must also be masking pursuant to the standard set forth below.

There are no exceptions to the following standard. Only the last 4 digits of a customer credit card number may be displayed. The rest of the credit card number and expiration must be masked. An example is:

Card Number: XXXX-XXXX-XXXX-2009
Expiration: XX/XX

No actions are permitted that would alter the configuration of a POS system such that the above standard is not followed.

B. Responsibility

District Managers and location management are responsible for regular reviews of Point of Sale receipts to ensure proper masking.

In the event a POS system is masking improperly or if there is other suspicious activity related to the POS, location management shall not allow use of such POS system until the issue has been remedied by the POS vendor or location management.
Location management is responsible for contacting the appropriate POS vendor for immediate remediation if assistance from the vendor is required. Location management

shall also immediately send email notification to CCReceipts@compass-usa.com in any event of a POS system remediation.

C. PROCEDURES TO ENSURE COMPLIANCE

1. **Internal Controls Review –** On an annual basis, every District Manager should perform a review of each location.

2. **Location Audits** – In addition to the annual Internal Controls Audit, Compass IT Security will periodically perform a site audit and observe the credit card receipt to ensure that it is properly masked

3. **Cash Reconciliation Procedures** – The cash reconciliation procedures at the end of each day shall include a spot check of the credit card receipts and batch reports to ensure that POS systems are properly masking information.

4. **Unit Manager Training Manuals –** The Unit Manager Training Manuals shall include training regarding the law and Compass Group Procedures relating to POS Credit Card Masking

5. **Cashier Training** – Cashiers shall be trained regarding the law and Compass Group Procedures relating to POS Credit Card Masking. Cashiers shall be trained to perform spot checks of credit card receipts at the start of business each day.

6. **Standard Installation Procedures** – For all new POS system installations, the location management must follow the standard installation procedures, including the requirement that all registers are verified to be masking properly. All new credit card setups must ensure that both the customer and merchant receipt copies are masking properly by running a test transaction and faxing both copies to the Compass Group Treasury Department at 980-235-6300.

Policy Title:	IT SECURITY AUDITING

POLICY/PURPOSE

To provide the authority for members of the Compass Group USA, Inc. (the "Company", including any and all divisions, subsidiaries and affiliated companies) IS Security Department to conduct an IT Security Audit on any system at the company.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents to ensure conformance to company information technology security policies
- Monitor user or system activity where appropriate and in accordance with the other Information Security Policies.
- Evaluate the vulnerability of the IT infrastructure

ASSOCIATES COVERED BY THE POLICY

This policy applies to all Company associates, temporary service personnel, and consultant /contractor personnel engaged by the Company, or external sources authorized to access Company electronic facilities

RESPONSIBILITY FOR ADMINISTRATION

The IS Security Department will be responsible for administering this policy.

DETAILS OF POLICY

This policy explains the steps for collecting data generated by computer and network activity, which may be useful in analyzing and responding to security incidents.

Collection

Audit data should include any attempt to achieve a different security level by any person, process, or other entity in a computer or network. This includes login and logout, super user access, and any other change of access or status. It is especially important to note "anonymous" or "guest" access to servers; this shall include the close scrutiny of File Transfer accounts.

The following items must be observed when auditing all company servers and networks.

- Audit trail logs and programs and utilities must be protected. They should only be accessible by security personnel.
- Reporting on vulnerabilities of computer and network resources.
- Unsuccessful login attempts should be logged and notified where possible.
- Important events should raise an alarm or high priority message automatically. Where possible, specify auditing on a per subject and per object basis.

- Each entry in the audit log should contain at least: Username or UID, date & time, terminal id, error level (success or failure) and event description.
- Logs should be kept on read-only media where possible.
- Logs should also be forwarded to a secure machine instead of locally on each machine, where possible.
- Logs should be archived when possible to allow for future analysis.
- Avoid storing logs on shared file systems. All machines should have their clocks synchronized to guarantee the validity of audit log timestamps.

Monitoring

Audit log files will be checked and monitored on a timely basis, in addition and where possible security software shall be implemented that automatically monitors the information, requirements, and practices specified in the Acceptable Use for Information Technology Systems section of this policy. This includes the automatic consolidation and correlation of events, and where appropriate, reporting to a centralized console any suspicious events and alerts.

Levels of Access

When requested, and for the purpose of performing an audit, any access needed will be provided to members of the IS Security Department.
This policy covers all computer and network devices owned or operated by the company. This policy also covers any computer and network device that are present on company premises, but which may not be owned or operated by the company.

This access may include:

- User level and or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on company equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.) Access to interactively monitor and log traffic on company networks.

Enforcement

Any noncompliance with these requirements will constitute a security violation and will be reported to management; this may result in short-term or permanent loss of access to company Information Technology Systems.
If necessary appropriate action will be taken against associate's, temporary service, consultant or contractor personnel when misuse, and/or unauthorized use is detected. These actions could result in counseling, suspension or employment termination depending upon severity.

Related Policies That May Require Coordination With This Policy:

Acceptable Use for Information Technology Systems
IT Access and Passwords
Databases
SAP Security

Policy Title:	IT SECURITY INCIDENT RESPONSE

POLICY/PURPOSE

The purpose of this Policy is to outline how Compass Group (the "Company") provides a coordinated, effective and cohesive approach to privacy and information security incidents ranging from unauthorized intrusions into systems to the mishandling of data in such a way that the privacy, integrity, or availability of confidential information is at risk.

ASSOCIATES COVERED BY THE POLICY

This policy applies to all Company associates, temporary service personnel, and consultant/contractor personnel engaged by the Company, or external sources authorized by the Company who have been identified and requested to participate in an incident response situation. The Incident Response Responsibility Matrix and work flows, supporting documents to this Policy, identifies the process, departments and key stakeholders. Information Systems Security ("IS Security"), Human Resources ("HR") or Legal will be the overall process owner, to be determined on a case by case basis depending upon the underlying security incident.

RESPONSIBILITY FOR ADMINISTRATION

The Systems and Technology Group ("STG") and all levels of management.

ENFORCEMENT

Non-compliance with this Policy is a security violation and will be reported to management. Depending on the severity of the infraction, a user could lose short term or permanent access to the system, and/or be sent to counseling, suspended or terminated.

DETAILS OF POLICY

A. Identification

Incident Reporting

Report all security incidents to **Compass Group Crisis Management Hotline** (1.877.710.6291), which will escalate the incident to the relevant department to obtain clear and documented details of what information will be captured.

B. Assessment

1. Preliminary Investigation

A preliminary investigation will be undertaken involving the appropriate departments, confirming incident details and gathering all critical information. For example, what systems and data have been compromised, financial loss, business disruption, etc.

A preliminary investigation will be undertaken involving the appropriate departments, confirming incident details and gathering all critical information. For example, what systems and depending upon the nature of the data compromise, determination of the appropriate departments to

become involved will be made. Incidents typically involve IS Security, Legal, HR, Corporate Communications, Treasury, Operations, and client representation. As supporting documentation to this Policy, the *Incident Response Process,* defines specific protocol for departmental involvement.

2. Primary Investigation

Once the preliminary investigation is complete, the IS Security team, in coordination with other appropriate departments/parties, will determine if a primary investigation will be required. IS Security will then contact the appropriate parties (client's IT departments, field operations, etc.) and perform an incident validation and assessment. This may also involve an approved third party IT incident assessment and response provider, depending on the findings thus far.

As part of the primary investigation, the IS Security team, in coordination with appropriate departments/parties, will make the following determinations:

- **Response Tactics** – how best to address the incident and what parties should be involved in the response.
- **Senior Management Approval** – approval in coordination with the following departments (dependent upon incident) but in general. STG, Legal, HR, Corporate Communications, Treasury, Senior Operators.
- **Fully Define Scope of incident** – establish and identify source of compromise, determine timeframe and what specifically is at risk.

As part of the supporting documentation to this Policy, the *Incident Response Process* defines the primary investigation in greater detail.

C. Containment

1. Isolate Problems

IS Security will immediately identify all areas of intrusion, working in coordination with an approved third party IT incident assessment and response provider.

2. Reporting the Incident

Depending upon the nature of the data compromise IS Security will determine reporting requirements in consultation with relevant departments, such as Legal, Corporate Communications, Treasury, etc.

D. Remediation

1. Resolution

IS Security will facilitate agreement to the remediation plan among all relevant departments/parties, coordinate all agreed-upon remediation steps to the incident, and ensure all appropriate parties are engaged.

2. Lessons Learned

Following the incident, all involved departments will engage in a lessons learned session in an attempt to improve processes and prevent future incidents.

Policy Title:	SERVERS, DESKTOPS AND WORKSTATIONS

POLICY/PURPOSE

All computer operating systems are subject to problems that don't become evident until they have been in common use for some time. Manufacturers periodically release service packs and patches to repair what has been found. Additionally, there are services and features that may be useful in certain, low risk environments, but for the majority of installations they create unreasonable security and operational risks. As users and specialists in the Information Technology field discover various vulnerabilities, recommendations are made to make adjustments to operating systems to alleviate these problems.
This policy outlines how the server infrastructure is managed, maintained and secured.

ASSOCIATES COVERED BY THE POLICY

This policy applies to all Compass Group USA, Inc. (the "Company", including any and all divisions, subsidiaries and affiliated companies) associates, temporary service personnel, and consultant/contractor personnel engaged by the company who configure, maintain or support company IT infrastructure.

RESPONSIBILITY FOR ADMINISTRATION

It is the responsibility of all levels of management of the Information Technology Department furthermore the IS Security Department will perform timely audits to ensure compliance to the policy.

DETAILS OF POLICY

Definition of Terms

Server
A server is a computer containing programs that collectively serve the needs of an enterprise rather than a single user, department, or specialized application. It also provides services to other programs in the same or other computers.
The basic server protection level depends mainly on type of server, usage, location and classification of information handled. Hence, different kinds of servers require different protection levels. The servers that this policy broadly refers too are Business/Application, Directory, File and File Transfer, E-mail, Print and Authentication based.
Servers that facilitate communications will be covered in the Network Policy.

Workstation/Desktop
The terms are used to mean any individual personal computer (PC) connected to the company network; this in turn shares the resources of one or more large servers. Since they are PCs, they can also be used independently of Company servers.

Web Servers
A Web Server is the computer program (housed in a computer) that serves requested pages or

files. A Web *client* is the requesting program associated with the user. The Web browser in your computer is a client that requests HTML files from Web servers.

New Server Prerequisites

In light of the need for remediation of identified problems, and the severe security risks posed by ignoring them, no server will be permitted to be connected to the company's production network until it has been sufficiently protected. After the hardening of the computer operating system has occurred the server will go through the Promotion to Production process. Procedures will be defined for each unique computer operating system the company incorporates in its Information Technology infrastructure. Current best security practices for each platform will be adopted, these will minimally include, vendor/manufacturer recommendations together with specifications from authoritative security organizations such as SANS and CERT.

Server Patch Maintenance

A policy and procedure will be developed to allow quick dissemination of the current best practices for servers to ensure the production systems are kept in top condition. However, no patch or fix will be applied to any production system until it has been carefully tested on a development server.

For critical computer operating system security vulnerability announcements and the management thereof, the Information Technology Department will develop internal working practices to address Security Patching.

Workstations and Desktops

Currently the company standard and support offering for workstation and desktop operating systems are Microsoft Windows XP and Windows 7. Generally workstations and desktops are subject to the same vulnerabilities experienced by the Microsoft Servers. Therefore, all new workstations must be subject to the same policies and procedures as the servers to harden them. In addition, there are many applications and personal computer settings that can cause weaknesses in the integrity of the desktop, and even other systems on the company network. To create uniformity of setup and to ensure that known weaknesses have been resolved it will be necessary to create a standardized image for workstations and desktops. Reference should be made to the Acceptable use for Computer Resources Policy prior any download or install of additional software.

Securing Servers

To secure a server, the recommendation is a three-part approach. It requires implementing security practices and procedures in these areas:

- planning and executing the deployment of servers
- configuring servers to help make them less vulnerable to attack
- maintaining the integrity of the deployed servers

This helps to improve security in two major ways:

- Maximize security on each network server host, which provides a backup in case of failure of perimeter defenses. Host security is also a first-line of defense against internal threats, which generally have a higher probability of occurrence than external threats.
- They prepare you to better recognize and recover from security breaches.

Web Servers

The Internet is one of the most important ways for the company to publish information, interact with users, and establish an e-business presence. However, if we are not rigorous in securely configuring and operating a Web site, we leave our organization vulnerable to a variety of security problems. Due to the importance of this area further policy has been defined. Compromised Web sites have served as the entry point for intrusions into an organization's internal networks for the purpose of accessing confidential information. Our organization could face business losses or legal action if an intruder successfully violates the confidentiality of customer data. Denial-of-service attacks can make it difficult, if not impossible, for customers to access our Web sites.

The practices recommended below are designed to help mitigate the risks associated with these and several other known security problems. They build upon and assume the implementation of all practices described in section.

All public facing Web Sites shall include a link to the “Web Site Terms of Use and Privacy Policy”.

Security issues

There are three main security issues related to the operation of a Web site. Improper configuration or operation of the Web server can result in the inadvertent

- information assets of our organization
- information about the configuration of the server or network that could be exploited for subsequent attacks
- information about who requested which documents from the server sensitive customer or user information

If the host used for our Web server were compromised. This could allow intruders to;

- change the information stored on the Web server host machine,particularly the information you intend to publish
- execute unauthorized commands or programs on the server host machine including ones that the intruder has installed
- gain unauthorized access to resources elsewhere in your organization's computer network
- launch attacks on external sites from your server host machine, thus concealing the intruders' identities, and perhaps making your organization liable for damages

Security improvement approach

To improve the security of your Web site, this three-step approach should be adopted:

1. Install a secure, fully patched server with an up to date anti-virus client.
2. Properly configure Web server software and the underlying Web server host operating system
3. Maintain the Web server's integrity by ensuring monthly patches are applied as necessary

Enforcement

Any noncompliance with these requirements will constitute a security violation and will be reported to management; this may result in short-term or permanent loss of access to company Information Technology Systems.

If necessary appropriate action will be taken against associate’s, temporary service, consultant or contractor personnel when misuse, and/or unauthorized use is detected. These actions could result in counseling, suspension or employment termination depending upon severity

Related Policies That May Require Coordination With This Policy:

Internet and Networking Components
Acceptable Use for Information Technology Systems
Website Terms of Use and Privacy Policy

Policy Title:	**VIRTUAL PRIVATE NETWORK**

POLICY/PURPOSE

The purpose of this policy is to provide guidelines for Remote Access IPSec Network (VPN) connections to the Compass Group USA, Inc. (the "Company", including any and all divisions, subsidiaries and affiliated companies network.

ASSOCIATES COVERED BY THE POLICY

This policy applies to all Company associates, temporary service personnel, and consultant/contractor personnel engaged by the company, or external sources authorized to manage, support and maintain the VPN.

RESPONSIBILITY FOR ADMINISTRATION

The Infrastructure & Operations Department will ensure they adhere to the standards defined. The IS Security Department will perform regular audits to ensure compliance.

DETAILS OF POLICY

Definition of Terms

VPN	A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. A virtual private network can be contrasted with a system of owned or leased lines that can only be used by one company. The idea of the VPN is to give the company the same capabilities at much lower cost by using the shared public infrastructure rather than a private one.
Tunneling	Using the public network as part of a private secure network. The "tunnel" is the particular path that a given company message or file might travel through the Internet.
Split Tunneling	Simultaneous direct access to a non- Compass Group USA network (such as the Internet, or a home network) from a remote device (PC, Laptop, PDA, SmartPhone, etc.) while connected into Compass Group USA's corporate network via a VPN tunnel.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Virtual Private Network, and simultaneously connected to another home or client network via another network interface or wi-fi connection.

Policy Requirements

It is the responsibility of associates with authorized VPN connectivity to ensure that unauthorized people are not allowed to access Company networks.
Mandatory password authentication to the VPN is required.

All VPN network traffic will be routed through corporate firewall to ensure VPN users are only granted limited network access to specific network addresses and ports; not full access to the corporate network.
All computers connected to the Company internal networks via VPN or any other technology must use the most up-to-date anti-virus software. Consult the IT Helpdesk (PSG) if you are unsure of the status of the computer you use.

Only VPN client software issued by the Company IT Helpdesk may be used.

By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the Company's network, and as such are subject to the same rules and regulations that apply to Company owned equipment. Their machines must be configured to comply with the IS Security Departments guidelines.

Enforcement

Any noncompliance with these requirements will constitute a security violation and will be reported to management; this may result in short-term or permanent loss of access to company Information Technology Systems.
If necessary appropriate action will be taken against an associate's, temporary service, consultant or contractor personnel when misuse, and/or unauthorized use is detected. These actions could result in counseling, suspension or employment termination depending upon severity.

Related Policies That May Require Coordination With This Policy:

IT Network Connectivity
Encryption of Data

Policy Title:	TERMS OF USE AND PRIVACY POLICY

POLICY/PURPOSE

To communicate the Terms of Use and Privacy Policy to all users of a Website owned by Compass Group USA, Inc. (the "Company", including any and all divisions, subsidiaries and affiliated companies).

ASSOCIATES COVERED BY THE POLICY

All Company Associates and all non-associates obtaining access to Company Websites are covered by this Policy.

RESPONSIBILITY FOR ADMINISTRATION

All Information Technology and Information Systems departments managing a Company or affiliate's Website are responsible for the administration of this Policy and will ensure they post this Policy on their respective Websites.

DETAILS OF POLICY

PROCEDURES

The following shall be posted on each Company Website: TERMS OF USE AND PRIVACY POLICY

1. Introduction

This page states the "Terms of Use and Privacy Policy" under which a user ("you") may use our Website (the "Site"). Therefore, please read this page carefully. Your authorization to use the Site is conditioned on your agreement with and acceptance of this Terms of Use and Privacy Policy. By using this Site, you are indicating your acceptance to be bound by this Terms of Use and Privacy Policy and any future revisions thereto. We may revise this Terms of Use and Privacy Policy at any time by updating this posting (with any such revisions being immediately after being posted on the Site). Your continued or subsequent use of the Site after such revisions have been made will constitute your acceptance of such revised Terms of Use and Privacy Policy. For this reason, you should visit this page periodically to review this Terms of Use and Privacy Policy. As used in this Terms of Use and Privacy Policy, the terms "Company," "we," "us" and "our" refer to Compass Group USA, Inc. and its subsidiaries and affiliates. To the extent the websites of any third party, our subsidiaries or our affiliates contain terms of use and/or privacy policies that may apply to this Site and are inconsistent with any terms in this Terms of Use and Privacy Policy, the language in this Terms of Use and Privacy Policy shall control for this Site.

2. Site Content

You acknowledge that the Site contains information, data, software (whether applications, scripts, plug-ins or applets), photographs, graphics, text, sound, images and other material (collectively, the "Content") that are protected, individually and collectively, by copyright, trademark, patent or other proprietary rights of the Company or third parties. You may not modify, remove, delete, augment, add to, publish, transmit, and participate in the transfer or sale of, create derivative works from, or in any way exploit any of the Content, in whole or in part, except as expressly allowed by this Terms of Use and Privacy Policy or applicable law (including, without limitation, U.S. copyright, trademark and patent law). Subject to the terms and conditions of this Terms of Use and Privacy Policy, we grant you a non-exclusive, non-transferable, limited right to access, use and display this Site and the materials thereon. You agree to comply with all laws relating to copyrights, trademarks or patents, in your use of this Site, and to prevent unauthorized copying of the Content. Concerning certain, designated Content, you maymake a single copy of the Content, provided that the copy is made only for your personal, informational and non-commercial use and that you do not alter or modify the Content in any way. You must not delete or alter any notices contained in the Content, such as all copyright notices, trademark legends, or other proprietary rights notices. Except as provided above, you may not upload, post, reproduce, modify or distribute in any way the Content without obtaining permission of the owner of the copyright or other proprietary right. Your access and use of the Site in accordance with this Terms of Use and Privacy Policy does not give you any right or interest in any Content or other information available on the Site, which at all times shall remain the property of the Company or other owner.

3. Privacy Policy

a. Information Gathered By the Company. In general, we gather information about all of our users collectively, and not on an individual basis, for purposes such as determining which parts of our Site users access most frequently. This information helps us determine which parts of our Site are most beneficial for users, and how we can continually create a better overall experience for you. We only use such data in the aggregate and anonymously.

b. Information About You Specifically. In some instances, we allow you to provide us with specific information about you, such as your name, address, email address, telephone number or other pertinent information. If you elect to provide us with your personal information, we may use that information to make you aware of employment opportunities with the Company, to provide you with certain of our publications or to notify you of other information regarding the Company. If you provide us with your personal information, but later decide you no longer want us to send you any information about us, simply contact us at the address set forth in the "Contact Us" section of the Site.

c. General Information Disclosure. Except as described in this Terms of Use and Privacy Policy, we do not disclose information about your individual visits to our Site, or personal information that you provide, such as your name, address, email address, telephone number, etc., to any persons or firms, except (i) when we believe the law requires it or to protect the Company, our users or others and (ii) to recruiters when you are providing your personal information in order to receive information about employment opportunities with us. We employ other companies and individuals to perform functions on our behalf, such as hosting our Web servers, analyzing data, and providing customer service. These other companies will have access to your personal information as necessary to perform their functions, but they may not share that information with any third party.

d. Cookies. To enhance your experience on our Site, we use a feature on your Internet browser called a "cookie". Cookies are small files that your Web browser places on your computer's hard drive. They are used for a variety of reasons, such as remembering user names and passwords and preferences, tracking click streams, and for load balancing. By using cookies, we can deliver faster service, consistent, updated results, and a more personalized experience on our Site. Your browser gives you the option to reject cookies. However, setting your browser to reject cookies generally hinders the browser's performance and will adversely affect your experience while using our Site.

e. Children. We do not specifically collect information about children. We believe that children should get their parents' consent before giving out personal information. If you are concerned about your child's use of the Site, we encourage you to use Web filtering technology to supervise your child's access to the Site. We also encourage you to participate in your child's experience with the Site.

f. Concerns About Our Privacy Policy. If, at any time, you have questions or concerns about our commitment to privacy, please feel free to contact us at the address set forth in the "Contac Us" section of the Site.

4. Disclaimers and Limitations on Liability

YOU EXPRESSLY AGREE THAT USE OF THE SITE IS AT YOUR SOLE RISK. NEITHER W E, NOR OUR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, AFFILIATES OR OTHERS (COLLECTIVELY, THE "PROVIDERS"), W ARRANT THAT (i) USE OF THE SITE WILL BE UNINTERRUPTED OR ERROR-FREE; (ii) THE INFORMATION, CONTENT, ADVICE OR OPINIONS PROVIDED ON OR THROUGH THE SITE IS ACCURATE, COMPLETE, RELIABLE OR CURRENT; OR (iii) THE SITE AND ITS SERVER ARE FREE OF COMPUTER VIRUSES OR OTHER HARMFUL MECHANISMS. IF YOUR USE OF THE SITE OR THE CONTENT RESULTS IN THE NEED FOR SERVICING OR REPLACING EQUIPMENT OR DATA, W E ARE NOT RESPONSIBLE FOR THOSE COSTS.

THE SITE, AND YOUR ACCESS TO IT, IS PROVIDED ON AN "AS IS," "AS AVAILABLE" BASIS AND W E SPECIFICALLY DISCLAIM W ARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. NO ORAL OR W RITTEN INFORMATION GIVEN BY US OR ANY PROVIDER SHALL CREATE ANY WARRANTY.

UNDER NO CIRCUMSTANCES SHALL W E OR ANY OTHER PARTY INVOLVED IN CREATING, PRODUCING OR DISTRIBUTING THE SITE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, GOODW ILL, USE, DATA OR OTHER INTANGIBLE LOSSES (EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) THAT RESULT FROM YOUR USE OF OR INABILITY TO USE THE SITE OR ANY LINKED W EBSITE. BECAUSE THE LAW IN SOME STATES DOES NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, LIABILITY IS LIMITED TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW.

YOU AGREE TO INDEMNIFY AND HOLD HARMLESS THE COMPANY, AND ITS OFFICERS, EMPLOYEES, AGENTS, DIRECTORS, SUCCESSORS AND ASSIGNS, FROM AND AGAINST ALL CLAIMS, DAMAGES, LOSSES, EXPENSES, COSTS, REASONABLE ATTORNEYS' FEES AND LIABILITIES THAT ANY OF THEM MAY SUSTAIN ARISING DIRECTLY OR INDIRECTLY OUT OF YOUR USE OF THE SITE OR ANY INFORMATION OR CONTENT CONTAINED ON THE SITE.

5. Links to Third-Party Websites

Occasionally, we may make available a link to a third party's Website. These links will let you leave the Site. The linked sites are not under our control and we are not responsible for the contents or security of any linked site or any link contained in a linked site, or any changes or updates to such sites. We are not responsible for Webcasting or any other form of transmission received from any linked site. We provide the links to you only as a convenience. We do not endorse, and make no warranty or representation regarding, any such site or its use or contents. Links do not imply that we are affiliated with, or are legally authorized to use any trademark, trade name, logo or copyright symbol displayed in or accessible through the links.

6. Unsolicited Submissions

We are pleased to hear from our customers and site users and welcome your comments regarding our Company and the Site. If you send us comments, suggestions, ideas, concepts or other information (collectively, the "Submissions"), the Submissions shall be deemed, and shall remain, our property, and we may use, copy, display, distribute, adapt, transfer or dispose of Submissions in any way and for any purpose as we may, in our sole discretion, determine appropriate. None of the Submissions shall be subject to any obligation of confidence on our part, and we shall not be liable for any use or disclosure of any Submissions.

7. Applicable Law

We maintain the Site from our offices within North Carolina, United States of America. We make no representation that the Content in the Site is appropriate or available for use in any jurisdiction, and access to them from locations in which such Content is illegal is prohibited. Those who may choose to access the Site from other jurisdictions do so on their own initiative and are responsible for compliance with applicable local laws. You may not use or export the Content in violation of US export laws and regulations. Any claim relating to the Site or the Content shall be governed by the internal laws of the state of North Carolina, without reference to its choice of law provisions, and shall be resolved solely through proceedings held within the state of North Carolina.

8. Termination

This Terms of Use and Privacy Policy is effective until terminated by either party. If you no longer agree to be bound by this Terms of Use and Privacy Policy, you must cease all further use of and access to the Site, and any notification of termination or other rejection of this Terms of Use and Privacy Policy is conditioned on such cessation. Subject to applicable law, we reserve the right to suspend or deny, in our sole discretion, your access to all or any portion of the Site with or without notice. You agree that any termination of your access to the Site may be effected without prior notice. Further, you agree that we shall not be liable to you or any third-party for any termination of your access to the Site.

9. General Information

This Terms of Use and Privacy Policy constitutes the entire agreement between us (i.e., you and the Company) and governs your use of and access to the Site. You agree to be bound by this Terms of Use and Privacy Policy, as well as any modifications thereof after we have posted the modified Terms of Use and Privacy Policy on the Site. Our failure to exercise or enforce any right or provision of this Terms of Use and Privacy Policy on any occasion shall not constitute a waiver of such right or provision. If any provision of this Terms of Use and Privacy Policy is found by a court of competent jurisdiction to be invalid, the parties agree that all other provisions of this Terms of Use and Privacy Policy remains in full force and effect. You agree that regardless of any statute or law to the contrary, any claim or cause of action that you or anyone claiming through you may

make, arising out of or related to use of the Site or this Terms of Use and Privacy Policy, must be filed within one year after such claim or cause of action arose or be forever barred.

10. Copyright Complaints

We respect the intellectual property of others, and we ask our users to do the same. If you believe that your work has been copied and is accessible on the Site in a way that constitutes copyright infringement, you may notify us by providing us a written notice that includes the following information:

- An electronic or physical signature of the person authorized to act on behalf of the owner of the copyright interest.
- A description of the copyrighted work that you claim has been infringed, including the URL (i.e., Web page address) of the location where the copyrighted work exists or a copy of the copyrighted work.
- Identification of the URL or other specific location on the Site where the material that you claim is infringing is located.
- Your address, telephone number and email address.
- A statement by you that you have a good faith belief that the disputed use is not authorized by the copyright owner, its agent, or the law.
- A statement by you, made under penalty of perjury, that all information in your notice is accurate and that you are the copyright owner or authorized to act on the copyright owner's behalf.

You should send your notice of copyright infringement concerning the Site to us at the address set forth in the "Contact Us" section of the Site. We have the sole discretion to determine what action, if any, we believe is necessary in response to a complaint of infringement, such as investigation of the complaint or removal of the allegedly infringing material.

Policy Title:	VULNERABILITY MANAGEMENT

POLICY/PURPOSE

This policy outlines the requirements for vulnerability management to ensure both the company's computer systems are in a secure configuration and the latest security software updates have been applied. Weutilize a three stage vulnerability management program. The first stage entails a weekly scan of externally available websites deemed to be business critical. The second phase is a rigorous process of patching the systems within the corporate network to obviate any security related vulnerabilities. The third phase is an annual vulnerability assessment conducted by an objective 3rd party vendor.

ASSOCIATES COVERED BY THE POLICY

This policy applies to all "Company" computer systems and networks as well as any 3rd party company that stores, processes, or transmits any "Company" data that is deemed to be sensitive or falls under any state or federal privacy statutes.

RESPONSIBILITY FOR ADMINISTRATION

It is the responsibility of the IS Security Department to review weekly reports and escalate any issue that is a security risk to the server/application owner for resolution.

DETAILS OF POLICY

Definitions of Terms

Read Only	A user only has access to "Read" any given report but does not have the ability to alter or disable the weekly scans.
VA	Vulnerability Assessment is an internal or external scan to assess how vulnerable a system may be to an electronic attack.
Internal Network	Refers to systems that are accessible from inside the network.
External Network	Refers to systems that are accessible via the internet.
Third Party	A business that is not a part of Compass Group USA, Inc. (the "Company", including any and all divisions, subsidiaries and affiliated companies.

Scope

This policy applies to any internal or external computer network system that contains "Company" data as well as any 3rd party that we transfer data To or From on a regular basis.

General

We currently utilize Qualys and Altiris for vulnerability management. These tools automate the lifecycle of network auditing and vulnerability management across the enterprise, including network discovery and mapping, software inventory, patching, delivery and license management. A 3rd party vendor performs our annual Vulnerability Assessment (VA) to ensure objectivity.

User Authorizations

Users and Groups can be set up to receive weekly reports for the computer systems they are responsible for.
Authorizations should be explicitly assigned via job function.
User cannot alter or disrupt any scheduled weekly scans as their access is Read- Only.
Individuals can be held responsible for actions that they perform while using the system.

Qualys Process and Security

All requests for new user setups to access Qualys weekly scan reports should be sent to securityengineering@compass-usa.com.
Account creation will be managed via the Information Security Department.
All reporting and access to reports will be configured by the Information Security Department
Scheduling the time and frequency of the Qualys scan is flexible and will be configured by the Information Security Department. The timing of the scan should be scheduled as to not interrupt business operations.
When scanning a 3rd party vendor or partner, permission must be acquired from the vendor or partner prior to scanning.

Users should logoff of the Qualys portal when away from their desks; furthermore workstations connected to the Qualys portal must conform to the Disabling Requirements (Section E) of the IT Access & Password Policy which helps to prevent any unauthorized users gain access to the system.
In addition, the Qualys application has the ability to timeout non-active sessions; this is currently set at 10 minutes.

Altiris Process and Security

All workstations have the Altiris client installed as part of the corporate image.
Servers on our internal network receive it via group policy. Servers placed in the DMZ must be configured manually.
All reporting and access to reports will be carried out by the Altiris team.
Workstation patching takes place on the 2nd Wednesday of each month as patches are released the previous day.
A pilot group of servers are also patched that Wednesday. If no issues are discovered then the DEV and QAS servers are patched Thursday and Friday with the PRD servers being patched on Saturday.

All critical and important patches for Microsoft, Adobe, Java, Apple and Google are applied. If there is high alert that results in a patch release outside the normal schedule the IT Security team will review and if deemed necessary that patch will be deployed via Altiris as soon as it is available.

Vulnerability Assessment

A vulnerability assessment is the process of identifying, quantifying, and prioritizing the vulnerabilities in a system.
When a Vulnerability Assessment is conducted on either an internal or external there are 2 levels of assessment that will affect and potentially disable the computer or networking system. The first and most commonly used setting is Non-Intrusive. This setting will ensure that the system you are scanning for vulnerabilities is not affected in any adverse way as to prevent functionality or user access.
The second and more risky setting is to use Intrusive mode. There are numerous ramifications from using the intrusive setting. User access can be prevented and entire computer systems and networks can be taken offline. In addition, restoring the affected systems can be a lengthy process.

Limitations

Vulnerability assessments can only be conducted if you have the proper access and permission to scan the systems under review. When conducting a vulnerability assessment you must first research and confirm that you have "logical" access to the systems. Meaning that the system(s) being scanned for vulnerabilities is accessible either over the internet or the local area network.

Enforcement

Any noncompliance with these requirements will constitute a security violation and will be reported to management; this may result in short-term or permanent loss of access to company Information Technology Systems. If necessary appropriate action will be taken against associates, temporary service, consultant or contractor personnel when misuse, and/or unauthorized use is detected. These actions could result in counseling, suspension or employment termination depending upon severity.

Related Policies That May Require Coordination With This Policy:

IT Access and Passwords
Acceptable Use for Information Technology Systems
PCI Compliance
IT Security Auditing

Policy Title:	DOMAIN NAMES AND WEBSITE CONTENT POLICY

POLICY/PURPOSE

It is the purpose of this Policy to set forth the requirements of any Associate who, on behalf of Compass Group USA, Inc. (the "Company") or its affiliate, purchases, registers, or otherwise acquires a Domain name ("Domain"), and/or develops or updates a Company Website or any portion thereof during the course of his/her employment with the Company.

ASSOCIATES COVERED BY THE POLICY

All Associates of the Company are covered by this Policy.

RESPONSIBILITY FOR ADMINISTRATION

The Information Systems Security ("ISS") Group, Human Resources, and all levels of management are responsible for the administration of this Policy.

DETAILS OF POLICY

PROCEDURES

A. Domain Name Registration

An Associate who purchases, registers, or otherwise acquires a Domain on behalf of the Company or its affiliates in the course of his/her employment understands and shall agree that all rights, title and interests in and to the Domain, including all intellectual property rights related to it, shall be owned by the Company, regardless of whether the Associate uses personal funds for the purchase of the Domain. The Associate shall not, at any time, purchase, register, or otherwise acquire a Domain under his/her name.

The Associate shall identify the Company's administrative and technical contact for Domain name registration as **"securityadmin@compass-usa.com, 2400 Yorkmont Road Charlotte, NC 28217."** The Associate shall provide ISS with details prior to registering the Domain. At ISS's request, the Associate shall agree promptly to assign the Domain registration to the Company.
The Associate shall not purchase, register, or otherwise acquire a Domain name that contains a Company trade name without approval from Company management. The Associate shall not knowingly request registration of a Domain, whether visible or imbedded, that contains any defamatory, inaccurate, abusive, obscene, libelous, slanderous, or threatening content, and/or that violates any federal, state or local law, and/or that infringes upon any third party's intellectual property rights.

B. Website Development and Content

An Associate who creates, develops, invents, improves, and/or updates a Company Website or any portion thereof, during the course of his/her employment shall provide such services as an employee of the Company. Therefore, all rights, title and interests in, the Company Website, and the content therein, including all copyright and other intellectual property rights, shall be owned by the Company.

An Associate shall not knowingly include content in any Company Website, whether visible or imbedded, containing any matter that is defamatory, inaccurate, abusive, obscene, libelous, slanderous, or threatening content, and/or violates any federal, state, or local law, and/or that infringes upon any third party's intellectual property rights.

If an Associate is uncertain of the origins of any elements of text, graphics, photos, designs, trademarks, other artwork, or computer programs he/she uses in the Company Website, such Associate must first confirm with the manager of the project that the elements are owned by the Company, that the elements are in the public domain, and/or that the Company has permission from the rightful owner to use such elements.

C. Failure to Comply with Policy

Any Associate who fails to comply with any provision of this Policy will be subject to disciplinary action up to and including termination. Further, the Company will pursue necessary legal action, including criminal prosecution, against any Associate who obtains, copies, or reproduces proprietary Website content for personal gain, benefits, or other personal interests, or otherwise contrary to the Company's best interests.

Related Policies That May Require Coordination With This Policy:

POLICY	REFERENCE SECTION
Integrity in the Workplace	Conduct and Work Rules
Manager Access and Review of Associate Information	Communications
Progressive Counseling	Performance Management
Workplace Rules and Regulations	Conduct and Work Rules

Policy Title:	DISASTER RECOVERY POLICY

POLICY/PURPOSE

The purpose of this policy is to minimize the loss of vital data and critical business processes that are supported by IT resources which includes personnel, networking and hardware/software requirements. This policy will ensure business critical data is protected against prolonged service interruptions, including large scale disasters, by the development and testing of disaster recovery/business continuity (DR/BC) plans.

This policy defines and outlines the general procedures that should be taken for each business department or unit to be prepared for dealing with various types of disasters that can affect the organization, especially the organizations Information Technology (IT) infrastructure. This policy addresses both recoverable business interruptions (i.e. service interruptions) and a more comprehensive business continuity plan for use in total loss situations such as major large scale disasters, by the development, implementation, and testing of disaster recovery/business continuity (DR/BC) plans. The two principal goals of disaster recovery/business continuity planning are:

- To resume to normal operations critical processes as quickly as possible with minimal impact to the business.
- To restore data while retaining its integrity.

The Disaster Recovery/Business Continuity policy will assist departments to:

- Identify IT resources that are needed to support business critical processes.
- Implement useful plans to protect against identified threats and mitigate/manage risk.
- Implement and test emergency procedures for prioritized processes following various types of major business interruptions.

ASSOCIATES COVERED BY THE POLICY

This policy applies to all Compass Group USA, Inc. (the "Company", including any and all divisions, subsidiaries and affiliated companies) associates, temporary service personnel, and consultant/contractor personnel engaged by the Company to implement and support Information Technology Network Services

RESPONSIBILITY FOR ADMINISTRATION

The Compass Group IT System Security Department will work with the Business Continuity Project Manager to ensure associates adhere to the policy. The IT Security Department will request annual updates to business and technical departments documented plans to ensure compliance.

ENFORCEMENT

Non-compliance with this policy is a security violation and will be reported to management.

DETAILS OF POLICY

A. Definition of Terms

Disaster Recovery (DR) is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a major business interruption.

Business Continuity (BC) A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection. For IT related infrastructure continuity the organizational disaster recovery plan (DRP) should be referred to since Disaster Recovery and Business Continuity are jointly related.

B. Scope

This policy applies to all departments and business sectors that operate, manage, or use IT services or equipment to support critical business functions.

C. Disaster Recovery and Business Continuity Steering Committee Review

All proposed Business Impact Analysis documents submitted as critical processes must go through a viability review with the **Disaster Recovery and Business Continuity Steering Committee Review**. The reviews are to ensure that all proposed recovery requests match the business requirements deemed as a priority that require to be recovered within a 5 (five) day time frame.

D. Responsibilities of each business group

1. **Participate in a Business Impact Analysis (BIA) as a precursor to developing departmental DR/BC plans.** A formal risk assessment interview should be conducted between the DR/BC Administrator and the functional manager every year in order to verify the department's high priority processes and the operational and financial vulnerabilities to these processes. Approval of the final version of the BIA is required from the DR/BC Steering Committee to participate in the annual Corporate DR exercise.
2. **Develop Disaster Recovery/Business Continuity plans**. Departments dependent on any type of IT services including voice telecommunications for carrying out their missions must develop DR/BC plans. Interdependencies shared with other departments should be taken into consideration as well as alternate methods of processing of data during a disaster.
3. **Train associates to execute the recovery plans. Training will consist of:**

   Education: Making employees "aware" of the need for a disaster recovery/business continuity plan.

Informing all associates of the existence of the plan and providing procedures to follow in the event of an emergency so associates are knowledgeable of how the plan will be executed. Training all personnel with responsibilities identified in the plan to perform the DR/BC procedure and providing the opportunity for recovery teams to practice disaster recovery/business continuity skills.

4. **Test disaster recovery/business continuity plans annually.** The IT department is required to test the core infrastructure plan every year while departments categorized as critical by the BIA'S approved by the DR/BC Steering Committee are required to test their plan at least every other year. Departments shall correct any deficiencies revealed by the test. The annual simulated DR exercise will ensure that the plans can be implemented in emergency situations and that management and staff understands how it is to be executed. The type and extent of testing adopted by a business will depend on: Criticality of business functions.

   Budget availability.

   Complexity of information system and components.

5. **Annually certify the updating and testing of the disaster recovery/business continuity plan.** Department heads are responsible for the oversight of their respective business's management and use of IT resources. An annual disaster recovery/business continuity plan confirmation letter must be submitted with the annually updated DR/BC plan by October 31 of each year. By way of this signed confirmation letter, the head of each business confirms to the DR/BC steering committee that a DR/BC plan has been reviewed, updated, and tested.

6. **The Disaster Recovery and Business Continuity Administrator may audit disaster recovery/business continuity plans.**
   The DR/BC Administrator may audit business DR/BC plans and tests for compliance with industry policies, regulations and standards. Technical departments are expected to submit their updated recovery procedures on a quarterly basis. DR contracts are updated annually on an as-needed basis as Compass Groups environment continues to change and grow.

7. **Maintain and update disaster recovery/business continuity plans annually.**
   Technological advances and changes in the business requirements of departments will necessitate periodic revisions to policies, standards, and guidelines. Each department or business unit is responsible for routine maintenance of their recovery procedures to keep them current. Departments shall update disaster recovery/business continuity plans at least annually and following any significant change to their computing or telecommunications environment. The plans should be submitted to the DR/BC Administrator in STG at a minimum on an annual basis.

Policy Title:	**VENDOR ENGAGEMENT POLICY**

POLICY/PURPOSE

The purpose of this Vendor Engagement policy ("the Policy") is to help Compass assess the security controls in place at a vendor to safeguard data entrusted to the vendor.

a. The vendor relation manager should request that the vendor complete the Vendor Assessment Questionnaire (VAQ)

b. The completed questionnaire should be forwarded to the IT Security Engineers

c. An IT Security Engineer will review the questionnaire and give feedback regarding the vendor's risk factors.

ASSOCIATES COVERTED BY THIS POLICY

All Associates of the Company are covered by this Policy.

RESPONSIBILITY FOR INTERPRETATION AND ADMINISTRATION

Associates looking to engage a vendor that will be processing data for or on behalf of Compass shall request the vendor to complete the questionnaire. Although the Security Department is responsible for the overall interpretation and administration of the questionnaire, each individual manager remains responsible for ensuring the vendor responds with a completed questionnaire.

DETAILS OF POLICY

CG Vendor Engagement.xlsm

Policy Title:	**CORPORATE RECORDS RETENTION POLICY**

POLICY/PURPOSE

The purpose of this Records Retention Policy ("the Policy") is to establish guidelines for the appropriate handling, maintenance, and disposition of records consistent with the business operations and legal obligations of Compass Group USA, Inc. and its subsidiaries, affiliates, divisions, and sectors ("the Company"). The proper handling, maintenance, and disposition of records is necessary to:

a. Ensure compliance with applicable federal, state, and local laws and regulations;
b. Ensure the availability and accessibility of information required for business operations;
c. Protect the legal rights of the Company; and
d. Assist with audits, investigations, and/or legal actions.

ASSOCIATES COVERTED BY THIS POLICY

All Associates of the Company are covered by this Policy.

RESPONSIBILITY FOR INTERPRETATION AND ADMINISTRATION

The Legal Department, in conjunction with other appropriate corporate departments as necessary, shall be responsible for interpreting and administering this Policy. The Legal Department shall ensure the Policy is reviewed annually or at other regular intervals as deemed appropriate by the Company. Although the Legal Department is responsible for the overall interpretation and administration of the Policy, each individual manager remains responsible for ensuring day to day compliance with this Policy within his/her department or account.

DETAILS OF POLICY

DEFINITIONS

A **"Record"** includes any information, regardless of its physical characteristic, that is created or received by the Company and should be preserved because of its informational value to the Company and its business operations. Records include paper documents as well as electronic files, whether on hard drives or other storage media, as well as publications, books, microfilm/microfiche, videos, audio recordings, maps, drawings, computer printouts, pictures, compact discs, databases, and all other forms of electronic media.

"**Non-Record Material**" includes information that has no ongoing documentary or informational value to the Company. Information and documentation falling into this category need not be retained beyond the immediate purpose for which they were created. Examples include:

a. Extra copies of documents that have been kept for convenience or reference and have no further documentary or evidential value;
b. Publications, trade journals, and magazines that require no action and have no further value to the Company;
c. Correspondence, memos, drafts, and interoffice communications, including emails, text messages, and voice mails, relating to matters that have been concluded where those materials have no informational value to the Company and its business operations;
d. Drafts of documents on which no action was taken and where no follow-up is required; and
e. Personal correspondence, emails, and documents not relating to Company business.

A **"Legal Hold"** is the requirement to suspend disposal of Records and Non-Record Material for legal matters such as investigations, litigation, or audits. See Section IX.

RECORD RETENTION SCHEDULE

A Record Retention Schedule setting forth the retention periods for various types of records has been developed in coordination with various departments of the Company and is attached as Attachment 1. If a type of document is not listed or there are questions about this Schedule, the Legal Department shall be consulted to determine the appropriate retention period and whether this schedule should be amended to include such documents. All documents in issue during this inquiry period should NOT be destroyed. If a Record should be retained pursuant to this Policy, it is important that all necessary steps are taken to preserve it to ensure it is not destroyed through the normal Record Retention Schedule. Should an Associate have questions about this requirement, he/she should contact the Legal or IT Department.

PAPER RECORDS OFF-SITE STORAGE

The Company utilizes off-site storage facilities managed by third-party vendors to store various types of paper records. These records remain at all times governed by this Policy. No boxes of records may be sent off-site without approval from a unit manager or department head. In order for a manager to approve paper records for storage in an off-site facility, the records must be properly boxed such that each box of records is marked with a description of its contents and with a "destruction date". For further guidance on the proper procedure to store documents off-site, please refer to the Administrative Services Off-Site Record Storage Policy and Procedures. Off-site boxes should not be approved by a unit manager or department head for off-site storage without this information. Effective immediately, any box of records sent to off-site storage without a description of its contents and a destruction date noted will be rejected for storage and returned to the sender.

The destruction date for any box sent to storage should be the same day as the date that the last document in the box may be destroyed pursuant to the Record Retention Schedule accompanying this Policy. For purposes of administrative ease and to ensure that no document is retained for an excessive period of time beyond its individual destruction date, all records stored in the same box should have destructions dates within 1 (one) year of each other. The destruction of all paper records sent to off-site storage facilities should be consistent with the procedures outlined in Section IX and X of this Policy. However, if a unit manager or department head has approved paper records to be sent to an off-site storage facility in a box properly labeled with its contents and a destruction date, then additional manager approval to destroy the contents of the box on or after its marked destruction date is not required.

Please note that NO records subject to a Legal Hold as outlined in Section IX should be sent to a third party facility under any circumstances.

ELECTRONIC DATA

Associates must be particularly mindful of electronic data and files and review their electronic files and data regularly and delete them where appropriate according to this Policy. Electronic data and files, whether on external media, network storage, or hard drives, are considered Company Records or Non-Record Materials that are subject to this Policy. The IT Department shall maintain a procedure to destroy electronic records according to the Record Retention Schedule established by this Policy. Destruction shall be complete, using software that prevents such destroyed files from being reconstructed or retrieved.

LEGAL HOLD PROCEDURE

The Company deviates from the application of the record retention period when there is a requirement to retain Records and other Non-Record Materials for legal matters. This process is called "Legal Hold." The legal requirement to suspend disposal of Records and Non-Record Materials generally arises when the Company receives notice of litigation or a governmental investigation or audit (or when one of the foregoing is reasonably anticipated). If an Associate knows or has reason to suspect a Legal Hold might relate to the Record or Non-Record Material in question, the Associate should check before disposing of or deleting information.

Legal Hold Priority and Scope - A Legal Hold overrides all relevant record retention periods and the Annual Records Review. **Note that Legal Holds may apply to more than just Records: they may apply to Non-Record Materials, convenience copies, and other materials (e.g., samples and prototypes) that are reasonably related to the subject of the Legal Hold.** If in doubt about the subject of a Legal Hold, contact the Legal Department.

Handling Suspended Records and Materials - Records and Non-Record Materials subject to a Legal Hold shall be preserved until the Legal Department indicates in writing that the Legal Hold is no longer in effect. After a Legal Hold for a particular Record or category of Records has been removed, the retention period reverts to what it would have

originally been. If the retention period for a particular Record has expired after a Legal Hold has been lifted, that Record can be destroyed in accordance with section IX below. **It is important to note that records may be implicated in more than one legal hold at a time.** If one Legal Hold has been removed, but another Legal Hold covering the same Record is still in effect, the Record must be preserved.

Requested Legal Holds - Associates should inform the Legal Department if they are aware of a special circumstance requiring the retention of certain documents beyond the scheduled retention period.

There are potentially significant penalties for failure to preserve Records and other Non-Record Materials relevant to litigation or governmental investigations or audits. All Associates should be vigilant to ensure no Records or other Non-Record Materials subject to a Legal Hold are inadvertently disposed of or discarded. Failure to make good faith efforts to comply with this Policy may result in disciplinary action, up to and including termination.

DESTRUCTION

The destruction of Records should be authorized jointly by a District/Regional Manager or Department Head. Each Regional/District Manager or Department Head is responsible for the safe and secure destruction of confidential records by methods that do not permit the recovery, reconstruction, and future use of confidential information.

In particular, paper records containing confidential information should be shredded and/or pulped, not simply thrown out with other classes of records or with miscellaneous trash. Electronic media and other non-paper media containing confidential information shall be destroyed or erased so that this information cannot practicably be read or reconstructed. Confidential destruction performed by an approved commercial vendor shall be subject to such contractual obligations as required by the Legal Department. In no case shall such contractual arrangements introduce standards, policy, or procedures less protective of confidential records than those rules which are described in this Policy. For further instructions regarding the destruction of documents, please refer to the Administrative Services Off-Site Storage Policy and Procedure.

If there are questions or concerns regarding what Records should be destroyed pursuant to this Policy, the questions should be directed to the Legal Department and the destruction of the Records at issue should be stayed until the question is resolved.

ANNUAL RECORDS REVIEW

Associates are required annually to review all of their Records and Non-Record Materials between February 1st and March 1st to ensure compliance with this Policy. This annual review period is established to ensure that this Policy is regularly being adhered to and should not be interpreted as limiting an Associate from disposing of Record and Non- Record Materials throughout the year in accordance with this Policy.

During the annual records review period, Associates shall identify all Records and Non- Record

Materials in all mediums (including paper and electronic) that are eligible for disposal pursuant to this Policy. Associates shall then dispose of all Records and Non- Record Materials that are eligible for disposal (meaning that the applicable record retention period has expired and that the record is not subject to a Legal Hold). Whether a Record or Non-Record Material is on-site or off-site does not change the fact that it is subject to the retention schedule and the requirements for this Policy.

EXCEPTIONS

Requests for exceptions to this Policy should be submitted first to the Legal Department and must be supported by sufficient justifications for the requested exception. When directed by the Legal Department, Records should be retained and not disposed of, notwithstanding the record retention periods set forth herein, in the event they may be needed for litigation or a governmental investigation. **No exceptions will be made to the retention of documents subject to a Legal Hold.**

Related Policies That May Require Coordination with This Policy:

POLICY	REFERENCE SECTION
Management of Associate Information	Administration & Recordkeeping
Recording of Hours	Administration & Recordkeeping
Criminal History Record Checks	Pre- and Post-Employment
Pre-Employment Information	Pre- and Post-Employment
Corporate Off-Site Record Storage	Administration & Recordkeeping

ATTACHMENT 1

RECORD RETENTION SCHEDULE

DOCUMENT TYPE	RETENTION PERIOD
ACCOUNTING/FINANCE (URT = Until Released by Tax)	
Account Analysis	7 years
Accounts Charged Off, Credit and Collections correspondence, and Bankruptcy	7 years
Accounts Payable Invoices and Credits-Paid Voucher File including copies of the voucher check, vendor's invoices, and related correspondence	7 years
Accounts Payable Ledger	Permanent
Accounts Receivable Ledger Cards and Statements (after date of payment), trial balances and aging schedules	15 years
Amortization and Depreciation Records	Permanent
Bank Statements, Reconciliations, and Transfer Records and Stop Payment Requests / Lists	15 years
Books of Original Entry, such as Cash Receipts Journal, Cash Disbursements Journal, Voucher Register and Journal Entries	7 years
Budget and Comparison Reports	3 years
Checks (Outstanding and/or cancelled) – A/P, Expense and Payroll; Void Check Listing; Outstanding Check Listing	15 years
Capital Appropriation Records	7 years
Capital Asset Records	7 years
Check Register	Permanent
Check Requisition	7 years

ATTACHMENT 1 CONTINUED
RECORD RETENTION SCHEDULE

DOCUMENT TYPE	RETENTION PERIOD
Claim Files (after resolution)	6 years
Cost Reports and Statements	7 years
Donations	7 years
Estimates & Projections	3 years
Excise tax records	7 years
Financial Statements – Monthly, Quarterly, Annual (Internal)	10 years
Financial Statements-Certified by Public Accountant	Permanent
General Ledger and Trial Balance	15 years
Payroll Register	15 years
Petty Cash Records	7 years
Physical Inventory Count Report (annual, semi-annual, or cycle counts)	7 years
Profit & Loss Statements	Permanent
Purchasing Card Records, including receipts and documentation	7 years
Purchase Orders	7 years
T&E Expense Reports	7 years
Valuation Computations	7 years
Work papers Supporting Internal Audits	7 years
FWork papers Supporting Monthly, Quarterly and Annual inancial Statements	7 years

ATTACHMENT 1 CONTINUED
RECORD RETENTION SCHEDULE

DOCUMENT TYPE	RETENTION PERIOD
TAX RECORDS	
Income Tax Returns and work papers	15 years
Income Tax Provision and work papers	7 years
Federal and State Tax Audit files	7 years
Acquisition/Disposition/Merger Agreements, Due Diligence, and related documents	Permanent
Pre-acquisition returns and related support	15 years from date of acquisition
Employment Tax Returns and supporting work papers	7 years
Information Reporting (1099s & other misc. tax filings)	7 years
Abandoned Property Tax Returns and supporting work papers (including all notification letters and responses)	10 years
Sales Tax Returns and work papers	10 years
Property Tax Returns and work papers	7 years
Tax Periodicals – Hardcopy (analysis, law changes, etc.)	2 years
Back up Disks of Tax Software	10 years
HUMAN RESOURCES	
Upon separation, the terminated Associate's medical files and reference checks will be merged with the general Personnel file and will be maintained with terminated files. I-9 Forms will be retained in a separated terminated I-9 file.	
Accident/Injury-Related Documents:	
• OSHA – Required Filings & Reports	6 years
• Specific Accident/Injury Reports	5 years after incident **or** 30 years if injury involving hazardous substance

ATTACHMENT 1 CONTINUED
RECORD RETENTION SCHEDULE

DOCUMENT TYPE	RETENTION PERIOD
Affirmative Action Plan Documents Open – While Active plus 3 years	Closed – 3 years
Attendance Records (Time Cards, Schedules, etc.)	4 years
Background Check Results (whether hired or not)	3 years after termination or 1 year if not hired
Bonus/Incentive/Commission Plan Documents	7 years after superseded
Collective Bargaining Agreements	7 years after termination
Drug Screens (rejected candidates)	1 year
Employment Applications/Resumes Received & Maintained, Related Applicant Flow Data & Job Postings	3 years
EEO-1 and VETS 100 Filings	2 years
EEOC or State HRC Case Files	See Legal
Associate Contracts/Employment Agreements	7 years after termination
Associate Fidelity Bond Records	3 years after termination/completion
Associate Benefit Files (includes FMLA paperwork, retirement, pension, beneficiary, enrollment forms, change of status forms, etc.)	6 years

Associate Personnel Files: Employment Application Agreement(s) Resume Test (if applicable) Promotion Records Progressive Counseling Records Individual Employment Contracts Profile Documents Tax Withholding Forms Direct Deposit Authorizations New Hire Input Document Offer Letter Performance Appraisals Old Attendance Records	6 years after termination
Associate Medical Files: FMLA Requests STD Applications Drug Screen Results Medical Examination Results Doctors Notes Any Medical Records	6 years after termination **Records on exposure to toxic chemicals must be kept for duration of employment plus thirty (30) years
Employment Reference Checks. (These records should be placed alphabetically (by Associate name) in one file for all Associates in the operation).	6 years after termination or 1 year if not hired
Garnishments	10 years after settled/satisfied
Employment-Related Investigation Files (NOT to be maintained in Associate personnel file. These are confidential Company documents and many are covered by attorney-client and work product privileges)	6 years after termination
INS Form I-9 Employment Eligibility Verification Form (These records should be placed alphabetically (by Associate name) in one file for all Associates in the operation).	3 years after date of hire or 3 years after date of termination, whichever is later

ATTACHMENT 1 CONTINUED
RECORD RETENTION SCHEDULE

DOCUMENT TYPE	RETENTION PERIOD
Insurance Records or employee termination, whichever is longer	7 years after plan termination
Interview Notes/Records not hired, 1 year	6 years from date of hire. If
Job Descriptions	5 years after superseded
Payroll Records (Including time cards)	7 years
Recruitment Records (Advertisements/EE Agency Requests)	1 year
Relocation Records	7 years after move date
Retirement/Pension/RRSP Plan Documents	6 years after duration of plan
Salary Administration Plan Documents / Compensation Policy	5 years
Settlements/Releases/Waivers involves ongoing obligations on the part of the Company	10 years unless agreement
Tax Withholding Forms (State or Federal W-2s / W-4s)	7 years
Training Manuals/Handbooks	2 years after superseded
Unemployment (Worker Security) Files	7 years
Work Permits/Minor Age Verification Documentation majority or termination, whichever is earlier	3 years after the age of
Workers' Compensation Files (NOT to be maintained in Associate personnel file)	7 years after closed

ATTACHMENT 1 CONTINUED
RECORD RETENTION SCHEDULE

DOCUMENT TYPE	RETENTION PERIOD
INFORMATION SYSTEMS	
E-mail (Microsoft Exchange, OWA Webmail & BlackBerry) * Note: Company does not have automatic e-mail deletion	Daily Backup – 7 day retention of backup tapes
Voicemail (Digital Voicemail only / Cisco Unity)	Bi-weekly Backup – 7 day retention of backup tapes
LEGAL	
Contracts - original executed copy	15 years after termination
Government Agency Investigations, Lawsuits and Claims	10 years after conclusion
Company Uniform Franchise Offering Circulars	Permanent
Company Franchise Agreements (as franchisor)	10 years after expiration
External branded franchise agreements and license agreements	3 years after termination
Intellectual Property – Trademarks, Copyrights, Patents	6 years after expiration
Corporate Documents (Articles of Incorporation, Bylaws, etc.)	Permanent
Acquisition/Disposition documents and related work product	Permanent
Licenses & Permits – federal, state & local	6 years after expiration
Surety Bond	7 years
Compass Policies and Procedures and related documents	3 years after superseded

ATTACHMENT 1 CONTINUED
RECORD RETENTION SCHEDULE

DOCUMENT TYPE	RETENTION PERIOD
PLANT AND PROPERTY RECORDS	
Environmental:	
• Agency inspection forms	5 years or as statute requires
• Employee training	5 years after term (or as statute requires)
• Materials/waste storage and use records (e.g., SARA Title III)	10 years
• Material Safety Data Sheets	Use + 30 years
• Proprietary inspection forms	1 year (or as statute or manual requires)
• OSHA Log and documents	5 years
Property deeds, easements, licenses, rights of way, leases	3 years after divestiture
Title papers to owned vehicles	Until sold
Vehicle operation & maintenance	3 years
MISCELLANEOUS	
Advertising Copy, Exhibits, Press Releases and Handouts, Public Information Activity	3 years
Postage reports/stamp requisition, meter records, Airborne log	1 year

ATTACHMENT 1 CONTINUED
RECORD RETENTION SCHEDULE

DOCUMENT TYPE	RETENTION PERIOD
Sign in/out register	1 year
Bills of lading	5 years
Damage claims	5 years after date of claim
Receipts for registered mail and express packages	1 year
Shipping & Receiving reports and instructions	1 year
Security Incident Reports	3 years

GLOSSARIES AND ABBREVIATIONS

Abbreviation	Meaning
ACL	Access Control List
BC	Business Continuity
BDC	Backup Domain Controller: A copy of PDC information is kept on a "backup" machine to ensure high availability and spread network/system load in LAN Manager domains.
BIA	Business Impact Analysis
CA	Certification Authority
CERT	Computer Emergency Response Team at Carnegie Melon University USA, acts as a central distribution point for help on security matters.
Cracker	A cracker is someone who breaks into someone else's computer system, often on a network; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. A Cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or because the challenge is there.
Cryptography	The translation of information (known as plaintext) into a coded form (known as cypher text) using a key. Cryptography is mostly used to protect the privacy of information (i.e. limit who can access the
DB	Database
DBA	Database Administrator
DHCP	Dynamic Host Configuration Protocol
DMZ	A demilitarized zone is a small network inserted as a "neutral zone" between a company's private network and the outside public network.
DNS	Domain name service allows the resolution of hostnames to IP addresses and vice versa in large networks.
DR	Disaster Recovery
EDI	Electronic data interchange
ERP	Enterprise resource planning
ESB	Enterprise Service Bus
Firewall	A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext transfer protocol, the principal protocol used by the WWW
LAN	Local area network
IT	Information Technology
NAT	Network address translation
MID	Merchant Identification
NFS	Network file system
NIS	Network information service
NIS+	New hierarchical, more secure version of NIS
NTFS	New Technology File System

GLOSSARIES AND ABBREVIATIONS CONTINUED

OS	Operating System
PBX	A private branch exchange is a telephone system within an enterprise
PA-DSS	Payment Application – Data Security Standard
PCI	Payment Card Industry
PDC	Primary Domain Controller: The principal NT server containing user account information in a domain.
PGP	Pretty Good Privacy is a popular program used to encrypt and decrypt e-mail over the Internet
POS	Point of Sale
Proxy	A service, which is normally used to provide indirect, accesses a particular Internet service. Proxies eliminate the need for direct access to the Internet for normal clients.
PSG	Processing Support Group, the IT Helpdesk
Router	A router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination.
SANS	The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization.
SMTP	Simple Mail Transfer Protocol
Spam	Spam is unsolicited e-mail on the Internet
SNMP	Simple Network Management Protocol
SSH	Secure Shell, a secure replacement for telnet, rlogin, rcp, rsh among other things.
SSL	Secure socket layer
Switch	A switch is a network device that selects a path or circuit for sending a unit of data to its next destination
TCP/IP	**T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol: This suite of protocols, originally developed for the Internet, is now the standard enterprise network protocol.
Triple-DES(3DES)	Triple Data Encryption Standard. Each block of data is encrypted 3 times.
VPN	A virtual private network is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the
WAN	Wide area network
WWW	World Wide Web