SUBJECT:	ORIGINATING DEPT:	SECTION:
IT ACCESS AND PASSWORD	Systems and Technology Group ("STG")	Communications

DATE ISSUED: 01-15-09	SUPERSEDES: 02/15/07	PAGE: 1 OF 4
INITIATED BY: STG	APPROVED BY: Human Resources and Legal	

I. 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.

II. 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.

III. 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.

IV. PROCEDURES

A. Enforcement

Non-compliance with this Policy is a security violation and will be reported to management. Depending on the severity of the violation, a User may lose short-term or permanent access to the Company's information technology facilities and systems, and may be subject to disciplinary action 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 the property of Compass Group USA, Inc. (the "Company") and is for authorized users only. Users of this system have no expectation of privacy. All users are subject to having all of their activities on this system monitored and recorded by Company personnel. Necessary, appropriate action will be taken against a user if misuse and/or unauthorized use of the system is detected. User misuse may result in disciplinary action up to and including termination and denial of access for further use. Anyone using this system

expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible criminal activity, Company personnel may provide such evidence to law enforcement officials. In addition, Company personnel may terminate a user's access to this computer system for any reason, at any time."

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 all systems must be submitted for new system users and shall be kept on file with STG_for all existing 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 job 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. 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 deleted after 100 days of inactivity. 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 five (5) consecutive failed login attempts. The User ID will not be re-enabled until a legitimate explanation for disablement is identified by STG.

F. Password Requirements

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. **Setting Passwords:**
   a. Default and vendor-supplied passwords must 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.

3. **Length and Complexity of Passwords:**
   a. Passwords must not contain leading or trailing blanks.
   b. Passwords must not contain more than two (2) consecutive identical characters.
   c. Passwords must contain at least eight (8) alpha numeric characters.

4. **Temporary Password Assignments:** In the event a user forgets his/her password, the following procedure must be followed:

   a. A user who forgets his/her password must call the IT Helpdesk at 1-888-295-7206 or 704-328-3149 to receive a new, temporary password.
   b. At the request of the IT Helpdesk, an IT technician will assign a new, temporary password. Neither the Helpdesk Associate nor the technician is permitted to divulge the new temporary password to the user requesting the password.
   c. Using the Company Associate phone directory, the IT Helpdesk will look up the User's name and telephone number, then contact the User at the listed telephone number to confirm his/her identity. The IT Helpdesk will then convey the password to the User by phone.

5. **Password Cracking:** Password cracking occurs when an individual uses a computer program, commonly know 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.

G. Access to User Accounts and Passwords

Managers and/or supervisors requesting access to any User's accounts or passwords should contact ISS for approval. ISS must seek prior approval from Human Resources. Such requests for access shall only be accepted from managers and supervisors. 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	Administration and Recordkeeping
Progressive Counseling Policy	Performance Management
SAP Security Policy	Available from STG
Workplace Rules and Regulations Policy	Conduct and Work Rules