NETWORK ACCESS AGREEMENT

1. GENERAL. The access and use of the Coca-Cola Beverages Florida, LLC's (**"CCBF"**) proprietary network of computer information systems (**"Systems"**) by a user and/or members of a user's organization, including consultants, employees and any other individuals or third parties that are granted access through it (**"User"**), are subject to the terms and conditions of this Network Access Agreement (this "**Agreement**") and all applicable laws.

2. SYSTEMS SECURITY.

a. Compliance with CCBF Policies and Standards

User agrees to configure all User computer systems used to access the Systems in accordance with: any technical standards provided to User in writing; and CCBF's Standards for Third Party Access, attached and incorporated herein by reference, or any modifications thereto provided to User in writing.

User represents that it has read and agrees to ensure that its employees, and anyone else granted access pursuant to this Section, will comply with CCBF's Information Protection Policy 4: Acceptable Use Policy, attached and incorporated herein by reference.

b. Access to User's Computer Systems by Third Parties

User represents that it has policies similar to those set forth herein with respect to granting access to User's computer systems to third parties. User agrees that during the term of this Agreement, it will not provide access to its computer systems to any business entities which compete with CCBF in the manufacture, distribution and/or sale of non-alcoholic beverages without CCBF's express written consent.

c. Access for Legitimate Purposes Only

User's access is provided solely for the legitimate business purposes of CCBF and User. Access to CCBF's Systems is monitored and recorded.

CCBF will maintain a database that catalogs the duration and scope of the access granted to User and the business purpose for such grant. Upon User's request, CCBF will provide User with a summary of such information as it relates to User ("**Scope Schedule**"). User agrees that it will comply at all times with the Scope Schedule (as amended from time to time).

CCBF may terminate User's access to the Systems for any misuse of such Systems by User or by individuals provided access by or through User.

User shall be liable for all damages caused by any individual obtaining access to the Systems through the User.

CCBF may require User, and if required User agrees, to ensure that all individuals obtaining access to the Systems through User agree to the terms of this Agreement prior to accessing the Systems.

d. Access Through User by Non-Employees

User shall not provide any access to the Systems to non-employees without the prior written consent of CCBF.

3. INFORMATION CONTAINED IN THE SYSTEMS.

a. Protection of CCBF's Information

User shall keep confidential all data and software programs and any other accessible materials contained in the Systems.

b. Non-Confidentiality and Use by CCBF of User Information

Unless CCBF has expressly agreed otherwise in any other agreement, any communication or material User transmits to or through the Systems, exclusive of any confidential information of CCBF, by electronic mail or otherwise, including any data, questions, comments, suggestions, or the like is, and will be treated as, non-confidential and non-proprietary. User acknowledges and agrees that anything it transmits may be used by CCBF, and its subsidiaries or affiliates, for any purpose, including, but not limited to, reproduction, disclosure, transmission, publication, broadcast and posting. Furthermore, CCBF is free to use any ideas, concepts, know-how, or techniques contained in any communication User sends to or through the Systems for any purpose whatsoever, including, but not limited to, developing, manufacturing and marketing products using such information.

c. Prohibited Information

User will not transmit any unlawful, threatening, libelous, defamatory, obscene, scandalous, inflammatory, pornographic or profane material or any material that could constitute or encourage conduct that would be considered a criminal offense, give rise to civil liability or otherwise violate any law.

4. DISCLAIMERS. User acknowledges and agrees that its use of the Systems is at its own risk. In no event will CCBF, and its subsidiaries, affiliates, officers and directors, be liable for any loss, liability, damages, costs or expenses that may arise under this Agreement

or out of User's access to the Systems. ACCESS TO THE SYSTEMS (AND ANY AND ALL HARDWARE, SOFTWARE AND OTHER COMPONENTS THEREOF) IS PROVIDED TO USER "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

5. INDEMNIFICATION; DUTY TO REPORT USE AND VIOLATIONS. User agrees to indemnify, defend and hold harmless CCBF (including its divisions, subsidiaries, officers, directors or affiliates) against any loss, liability, damages, cost or expenses of CCBF (including its divisions, subsidiaries, officers, directors or affiliates) at any time because of any claim, action or proceeding arising out of the access to the Systems or out of the breach of the terms and conditions of this Agreement by User or by any individual or entity granted access through User. User agrees to immediately notify CCBF of any material violation of this Agreement by anyone granted access through User. Upon CCBF's request, User shall promptly provide CCBF with a list of all individuals granted access to the Systems through User.

6. AUDIT RIGHTS. At any time during the term hereof, CCBF shall have the right to conduct an audit of User to confirm User's compliance with the terms and conditions of this Agreement. CCBF's audit rights hereunder shall include the right of CCBF (or its representatives) or an independent third party to test the security of User's computer systems.

7. TERMINATION; MODIFICATION. User acknowledges and agrees that CCBF has the right to immediately terminate this Agreement or any Logon ID access granted to any individual through User at any time with or without cause. CCBF may modify the terms and conditions of this Agreement at any time upon thirty (30) days' written notice to User. If User does not wish to continue its access to the Systems under such modified terms and conditions, User may terminate this Agreement by written notice delivered to CCBF prior to the effective date of the modification.

8. MISCELLANEOUS. This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes any prior understanding or agreement relating to the same subject matter. This Agreement shall be governed exclusively in accordance with the laws of the State of Florida. This Agreement may not be modified unless approved in writing by CCBF. User may not assign this Agreement without the express written consent of CCBF. CCBF may assign or otherwise transfer this Agreement without the prior consent of User. Failure by either party to enforce a provision of this Agreement shall not constitute a waiver of such party's rights under that or any other provision. The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision hereof. No changes to this printed form of Agreement will be effective unless approved in writing by CCBF's legal counsel. This Agreement may be executed simultaneously in two (2) or more counterparts, each of which will be considered an original, but all of which together will constitute one and the same instrument. Execution and delivery of this Agreement may be evidenced by facsimile transmissions and will be sufficient to bind the parties to the terms and conditions of this Agreement. If this Agreement has been translated from English and an inconsistency results between the English and non-English versions of this Agreement, the English version will prevail.

STANDARDS FOR THIRD PARTY ACCESS

User Access. The level of access to CCBF Systems that is granted to a third party end User by CCBF is at the sole discretion of CCBF and will correspond to the minimum level of access that allows the third party end User to accomplish his/her business purpose for utilizing CCBF Systems. Based upon the level and type of access, CCBF will determine if a third party end User will utilize a CCBF-owned workstation, a third-party-owned workstation, or an image of a CCBF standard workstation applied to a third-party-owned workstation to connect to CCBF Systems. In the event that a third-party-owned workstation is utilized, the workstation's configuration is subject to audit by CCBF and must meet the following conditions before connection to CCBF Systems is allowed: (a) current commercial anti-virus software is installed and a full system scan is performed; (b) current operating system patch levels are applied; and (c) malicious software and hacker tools are removed or disabled.

Development Systems. Prior to a third party organization connecting its computer systems that are used to provide development and/or application support services ("**Development Systems**") to CCBF Systems, the third party must: (a) completely isolate the Development Systems via a multi-layered router and firewall architecture from all other networks, with the exception of CCBF systems; (b) ensure that the connection between the Development Systems and CCBF systems is segmented using VLANs, uses Network Address Translation (NAT), and takes advantage of the latest industry standards and protocols for secure communication (i.e., VPN, SSL, etc.); (c) submit for CCBF's written approval a document setting forth the third party User's compliance with (a) and (b) above; and (d) receive written approval from CCBF of the document submitted per (c) above, which may be withheld at CCBF's sole discretion.

INFORMATION PROTECTION POLICY 4: ACCEPTABLE USE POLICY

1. Policy Purpose and Scope. This Acceptable Use Policy (**"Policy"**) defines the appropriate use of CCBF information and Systems by Users. It is a subset of the Information Protection Policies. This policy includes the information protection requirements common to all users of CCBF information and Systems. CCBF reserves the right to change the Policy at any time.

2. Policy Statement. All CCBF Systems and any CCBF information or messages stored on them, or created, sent or received using them, are the property of CCBF. It is each User's responsibility and obligation to ensure that Systems are used properly. All Users must annually review and agree to abide by this Policy. A violation of this Policy may result in disciplinary action up to and including termination of employment. Violation of this Policy may also be a violation of other CCBF policies or procedures, including, but not limited to, CCBF's Code of Business Conduct.

3. Business Use (ISO/IEC 17799 8.7.5). Systems are to be used to conduct CCBF business. Occasional personal use of CCBF Systems is permitted, however, as long as it does not: (a) impact the performance of activities related to the discharge of User's responsibilities to CCBF; (b) violate this Policy or any other CCBF policies or procedures; and (c) violate any applicable laws. Such occasional personal use is subject to all terms of this Policy, including monitoring.

4. Acceptable Use of Internet (ISO/IEC 17799 8.7.5).
4.1. Internet access originating from CCBF must go through a CCBF-approved Secure Access Zone (**"SAZ"**). Use of commercial Internet service providers to access the Internet from within CCBF is prohibited.
4.2. Users shall transmit Confidential Information as stated in the Data Classification Guide, attached and incorporated herein by reference.

5. Acceptable Use of Electronic Mail (ISO/IEC 17799 8.7.4).
5.1. Users must prepare e-mails with the same degree of accuracy, care and propriety that they would use in the creation of traditional written communications. Users shall be aware that statements made through electronic communications may be legally binding.
5.2. Users shall not use e-mail to perform the following activities: (a) send or forward chain letters; or (b) send or forward security related messages not originating from the Information Security Organization (e.g., computer virus warnings), unless done in support of an investigation.
5.3. The use of manual or "auto-forward" rules to send CCBF business e-mail outside of the CCBF System is not permitted. "Auto forward" rules are defined as any setting in an e-mail system that can be used to automatically forward incoming e-mail to another e-mail address.
5.4. If an e-mail message containing Confidential Information is received in error, the receiver must notify the sender of the error and delete the message.
5.5. Users must immediately contact CCBF's legal counsel upon receipt of a message that contains illegal or anti-competitive business-related information or information that violates CCBF's policies or procedures. CCBF's legal counsel will assist Users in preparing an appropriate response so as to safeguard CCBF from being accused of illegal or anti-competitive conduct.

6. Acceptable Use of Communications Devices (ISO/IEC 17799 8.7.5).
6.1. Use of a mobile phone to disclose Highly Restricted information (as defined in the attached Data Classification Guide) is prohibited.
6.2. Users shall exercise caution when discussing Confidential Information in a public setting.
6.3. The host of a conference call shall ensure that only authorized individuals are connected to the call via the use of distributed pass codes for entry to the conference call. It is suggested to roll call attendees prior to the commencement of discussion.

7. Further Use Restrictions (ISO/IEC 17799 12.1.5, 8.7.5).
7.1. Users may not use any CCBF System in a manner that would violate this Policy or any other CCBF policy or procedure or any law or regulation; in a manner that would reflect badly upon CCBF, such as by pirating

software, stealing copyright material, stealing passwords, hacking, participating in the viewing or exchange of pornography or other obscene materials, or engaging in any other unethical or wrongful conduct; to load, download or store games or non-CCBF related or other unauthorized executable files; yo download or store non-CCBF related files such as MP3, MPEG, AVI, JPG, etc.; to participate in non-CCBF related business activities; to participate in gambling; for the purpose of solicitation, such as requesting contributions or soliciting memberships to non-CCBF approved charitable organizations or soliciting political candidates; for attempted financial gain resulting from knowledge of Confidential Information; in a manner that would cause a reasonable person to be defamed, offended, harassed or disrupted, such as by uploading, downloading or transmitting sexual comments or images, racial or ethnic slurs or other comments or images that would offend someone on the basis of race, gender, national origin, sexual orientation, religion, political beliefs or disability; to enable unauthorized third parties to have access to or use any CCBF Systems or otherwise jeopardize the security of any CCBF Systems; to publicly comment or speculate on CCBF performance, policies or actions; to post Confidential Information on any public Internet sites (such as chat rooms, discussion forums and newsgroups), unless it is part of their assigned job function; or in a manner that would significantly impact the performance, capacity or integrity of any CCBF System.

7.2. User's possession, development or intentional use of viruses, hacker tools or other malicious software is prohibited.

7.3. Only software authorized by CCBF shall be installed on any CCBF System. Users shall not install software onto any CCBF System without the approval of CCBF.

7.4. Users must not attempt to circumvent the security of any CCBF System.

8. CCBF's Right to Monitor Systems (ISO/IEC 17799 9.7.2).

8.1. Subject to applicable law, CCBF may monitor any CCBF System and any User's use of any CCBF system. Any monitoring, such as interception of communications or monitoring of Internet usage, will take place only where required in CCBF's legitimate interest. These interests include: ensuring effective and/or secure operation of any System; keeping records of transactions in which CCBF is involved; ascertaining employee / User compliance with applicable laws and CCBF policies or procedures; or detecting or preventing crime.

8.2. Monitoring will be in accordance with applicable CCBF procedures and applicable legal requirements. Any data gathered as a result of monitoring activities will be processed in accordance with applicable law and may be disclosed outside CCBF in support or as part of investigations or legal proceedings.

8.3. Except as protected by applicable law, communications on CCBF Systems are not private. Passwords and User IDs are designed to protect CCBF's business information from unauthorized access, not to provide Users with personal privacy in any communications.

9. User Responsibilities.

9.1. Clear desk policy (ISO/IEC 17799 7.3.1)

9.1.1. Confidential Information must be protected according to the attached Data Classification Guide and in accordance with applicable contractual agreements.

9.1.2. Authentication credentials, such as tokens or passwords, must not be stored in the open.

9.1.3. Confidential Information, when printed, shall be cleared from printers, copiers and fax machines according to the attached Data Classification Guide.

9.2. Clear Screen Policy (ISO/IEC 17799 7.3.1)

9.2.1.Workstations and servers shall be configured with a password-protected screen-saver. The screen-saver must require the entry of a password after a workstation or server console has been left idle for fifteen (15) minutes.

9.3. Password Management (ISO/IEC 17799 9.2.3)

9.3.1. Users shall change their password from the initial System default upon the first use of their User ID.

9.3.2. Users shall create strong passwords that are a minimum of six (6) characters in length and be comprised of letters, numbers and special characters.

9.3.3. Passwords shall not be easily associated with CCBF or User (*e.g.*, social security number, employee number, address, numerical equivalent of name, family names, pet names). Passwords shall not contain words

from a dictionary, movie, geographical location, mythology, CCBF products, customers or application names. Also, passwords shall not be based upon month/year combinations.
9.3.4. Users shall change passwords at least every forty-five (45) days.
9.3.5. Passwords shall not be saved using the AutoComplete feature, or other automated password storage mechanism, in Web browsers and applications.
9.3.6. Default access codes shall be changed immediately upon receiving a new voicemail account.
9.3.7. Voicemail passwords shall be a four (4) character minimum. These passwords shall not be directly associated with the phone extension or User. Passwords shall not be comprised of date of birth, anniversaries, portions of social security numbers or sequential numbers.

9.4. User Account Management (ISO/IEC 17799 9.3.1)
9.4.1. All access to CCBF Systems containing Confidential Information shall be controlled by an authentication method involving a minimum of a unique User ID/password combination.
9.4.2. All activity performed under a User ID is the responsibility of the individual assigned to that User ID. Users shall not share their User ID/password with others or allow other Employees to use their User ID/password. Users are not permitted to perform any actions under any User ID other than their own, or a group or shared User ID to which they have been granted access. The use of generic IDs (such as temp or guest), unless specifically assigned to an individual and documented, is not permitted. Group or shared IDs must have a designated owner, in writing, accountable for all actions performed under the group or shared ID.
9.4.3. User's access rights shall be reviewed every ninety (90) days in order to maintain effective access control. User IDs that have not been accessed for ninety (90) days shall be disabled, and shall be deleted at one hundred eighty (180) days.
9.4.4. Privileged access rights to CCBF Systems, including administrative access to laptops and workstations, is restricted to authorized personnel with a business need. Privileged access rights must be reviewed every ninety (90) days.
9.4.5. All Users that have access to privileged access rights (such Administrator or Root) shall have their own personal User IDs for normal business use. Privileged Users must use their personal User IDs for conducting non-privileged activities. Wherever possible, privileged Users must login to a CCBF system using their personal User ID prior to invoking a privileged User ID.

9.5. Laptop Protection
9.5.1. Users shall ensure that their laptops are physically secured using cable locks or other techniques when unattended.

9.6. Virus Control (ISO/IEC 17799 8.3.1)
9.6.1. External storage media (floppy disks, CDs, CDR-Ws, zip disks, etc.) that have been out of the control of User shall be scanned before use.
9.6.2. If a virus is suspected on a CCBF System, Users shall disconnect the System from all other systems immediately, notify their local HelpDesk and assist in the removal of the virus prior to any re-connection to other Systems. It is the responsibility of Users, with appropriate technical assistance, to ensure that the virus has been successfully removed before resuming communications on any Systems.
9.6.3. Users shall scan all files downloaded from the Internet or received via E-mail from outside CCBF for viruses using the CCBF-approved anti-virus software. Attachments contained in messages from unknown senders should not be opened.
9.6.4. All Systems must use current CCBF-approved anti-virus software. Systems shall be scanned upon each boot-up, and the anti-virus software shall remain running throughout the computing session. The complete hard drive shall be scanned at least weekly.

9.7. Reporting Security Incidents (ISO/IEC 17799 6.3.1-3)
9.7.1. Users shall report known or suspected information security incidents to CCBF.
9.7.2. If a User suspects a security weakness or system vulnerability, that individual shall notify the Information Security Organization immediately. Only individuals in an information security or audit role shall test security weaknesses. User is forbidden to test the security weakness without the permission, direction and involvement of the Information Security Organization. User shall not publicize the discovered vulnerability or weakness.

9.7.3. Users shall report known or suspected violations of the Information Protection Policy to the Information Security Organization.

9.8. Information Classification Categories (ISO/IEC17799 5.2.1)
9.8.1. All electronic and hard copy CCBF information shall be classified in accordance with CCBF information classification categories. CCBF information in any format (e.g., hard copy or electronic) shall be protected by all Employees and third parties at the level commensurate with its value as determined by the assigned classification.

10. Telecommuting and Home Office.
10.1. Mobile Computing and Telecommuting (ISO/IEC 17799 9.8.1)
10.1.1. Users are responsible for the security and care of mobile computing asset, including, but not limited to, laptops, Personal Digital Assistants (PDAs) and Blackberrys, issued to them by CCBF. If the mobile computing asset is lost, stolen or destroyed and the individual responsible for that asset is found negligent in its protection, that individual may be held financially responsible for the cost incurred by CCBF to replace the asset. Users shall immediately report the loss of CCBF information assets to their local security organization.
10.1.2. Users are not permitted to store CCBF-related information on personally owned systems or any other equipment not provided by CCBF, unless approved by CCBF and securely configured to protect Confidential Information.
10.1.3. Direct access to the Internet (e.g., cable modem or DSL) from a non-CCBF owned facility (e.g., from home or while traveling) must either go through a CCBF-approved SAZ or be protected via anti-virus and access control technology such as personal firewalls.

10.2. Remote Access (ISO/IEC 17799 12.2.2)
10.2.1. Users shall only use CCBF-approved and securely configured systems to access any CCBF System. Use of home PCs, personal laptops or other non-CCBF Systems are prohibited unless approved by CCBF and securely configured to protect CCBF Classified Information.
10.2.2. All remote access points into CCBF's environment shall be protected by a CCBF-approved SAZ and approved by CCBF. The use of unauthorized modems or remote access solutions, including wireless network access, is not permitted.
10.2.3. All remote access Users shall be authenticated in a CCBF-approved SAZ prior to accessing any CCBF System, including web-based applications, located in CCBF's internal network.
10.2.4. Prior to establishing direct remote connectivity to CCBF's internal network, or prior to remotely accessing any CCBF System as a privileged user, remote access Users shall be authenticated with two-factor authentication. Two-factor authentication is a combination of any of the following: 1) something you know (e.g., password), 2) something you have (e.g., token), and 3) something you are (e.g., biometrics).
10.2.5. Remote control software is prohibited from installation on any Systems unless authorized by CCBF.

10.3. Security of Equipment Off-premise (ISO/IEC 17799 7.2.5, 6.1.3)
10.3.1. The Information Protection Policy applies to all Systems and information regardless of location.
10.3.2. Authorized System, Confidential Information and media taken outside CCBF premises, shall be controlled, secured and protected to ensure protection against theft, destruction or unauthorized disclosure and use according to the attached Data Classification Guide.

DATA CLASSIFICATION GUIDE

Classification Definitions

- **NOT CLASSIFIED**: All nonpublic CCBF information does not require classification. Some information will not impact CCBF if it is disclosed to unauthorized individuals or if its integrity is impaired. However, all nonpublic CCBF information is subject to CCBF review or disclosure procedures to mitigate potential risks of inappropriate disclosure.
- **CONFIDENTIAL:** Information, that if disclosed to unauthorized individuals outside CCBF, altered, misused or destroyed, may have a substantial adverse impact to CCBF. A negligible adverse impact will occur if the information is disclosed to unauthorized individuals, within CCBF. Access to this information shall be granted on a need to know basis as based on job function, department, and an acceptable level of security risk. Access to this information requires prior approval of CCBF or an officer of CCBF.
  Classified Systems must comply with CCBF technical security standards (or equivalent).
- **HIGHLY RESTRICTED:** Information that, if disclosed to unauthorized individuals (outside CCBF or within CCBF), altered, misused or destroyed, will directly cause damage to CCBF's market share and/or market capitalization. This information, if not adequately protected, may result in non-compliance with applicable laws and regulations. Access to this information shall be granted to an individual on a need to know basis. Access to this information requires prior approval of the Chief Information Officer of CCBF.
  Classified Systems must comply with CCBF technical security standards (or equivalent).
- **PERSONAL INFORMATION:** Personal Information is any information that identifies an individual or relates to an identifiable individual. Information in this category shall be used only for legitimate business purposes and may require an extra level of protection and a higher duty of care based on applicable law or regulation. Access to this information shall be granted to an individual on a need to know basis. Access to this information requires prior approval of the Chief Information Officer of CCBF.
  Refer to the CCBF Privacy Policy for additional information.
  Classified Systems must comply with CCBF technical security standards (or equivalent).