Coke Florida's Security Requirements

The party to the Agreement providing goods and/or services to Coke Florida ("**Supplier**") agrees to, and represents and warrants that it will comply, and will cause all its contractors, vendors, and suppliers to comply, with the following Coca-Cola Beverages Florida, LLC ("**Coke Florida**") security requirements ("**Security Requirements**") and all applicable laws, including, without limitation, the Florida Information Protection Act and the Health Insurance Portability and Accountability Act, that are applicable to the goods and/or services (the "**Services**") provided by Supplier and Supplier's contractors, vendors, and suppliers to Coke Florida under the Agreement. Supplier agrees to be responsible to Coke Florida for Supplier's contractors', vendors', and suppliers' actions to the same extent as if Supplier itself performed the Services pursuant to the terms in the Agreement and these Security Requirements.

1. Security. In providing the Services, and at no additional cost to Coke Florida, Supplier will comply, and will cause its contractors, vendors, and suppliers to comply, in all respects with Coke Florida's Security Requirements and will meet or exceed industry standards and best practices for such types of Services provided hereunder, but in any event will at a minimum comply with Coke Florida's standards set forth in these Security Requirements. Without limiting the foregoing, Supplier will: (a) within ten (10) days of the parties signing the Agreement, submit to Coke Florida a completed Cloud Security Alliance Questionnaire substantially in the form attached hereto as Attachment 1; (b) receive approval in writing from Coke Florida for every new location of Supplier's application(s) provided and/or Coke Florida Confidential Information to be hosted by or on behalf of Supplier or its representatives; and (c) comply with the Coke Florida Hosting Security Guidelines set forth on Attachment 2 and the Coke Florida Data Classification Guide set forth in Attachment 3 attached hereto, as reasonably modified by Coke Florida from time to time.

2. Privacy. In the event Supplier and/or Supplier's contractors, vendors, and/or suppliers receives, stores, processes, or otherwise has access to any data constituting personal information under applicable data privacy or other laws, rules or regulations (including, without limitation, name, address, e-mail address, telephone number, cell phone number or date of birth), Supplier will comply, and cause its contractors, vendors, and suppliers to comply, with the Data Privacy Security Requirements set forth in Attachment 4.

3. SSAE-16 Audit and Security Reviews. Supplier will conduct, at least annually, an SSAE-16 audit (and such other audits and/or inspections as may be reasonably requested by Coke Florida and agreed to by Supplier). The audit scope will include the site, systems, application(s) and other systems managed, used, housed, and maintained by Supplier and Supplier's contractors, vendors, and suppliers (the "**Supplier Environment**"). Supplier will promptly furnish to Coke Florida all audit results. If, after reviewing any such audit results, Coke Florida reasonably determines that security problems exist relating to the Supplier Environment or any Coke Florida Confidential Information, Coke Florida will notify Supplier in writing (including by electronic mail), and Supplier will promptly explain and provide remediation plans to correct the problems at Supplier's sole cost and expense.

4. Coke Florida Security Assessment. Once every twelve (12) months, Coke Florida will have the right to perform, at Supplier's cost, by an independent third party chosen by Coke Florida and reasonably acceptable to Supplier, or through Coke Florida's own personnel, a security audit on the Supplier Environment. If such an audit identifies security concerns considered to be high risk by industry standards or in violation of the agreed upon Coke Florida Security Requirements, Supplier will promptly take whatever corrective actions are reasonably necessary to correct the problems at Supplier's sole cost and expense. Coke Florida will have the right to perform follow-up audits to ensure that all reasonably necessary corrective actions have been taken. If such follow-up audit concludes that Supplier has not adequately taken corrective actions to correct the problems at Supplier's cost, Supplier will: (a) promptly take whatever corrective actions are reasonably necessary (as specified by Coke Florida) to correct the problems at Supplier's cost, and (b) immediately reimburse Coke Florida for its costs incurred in connection with the audit. The rights and remedies afforded Coke Florida under this Section will continue until all reasonably necessary corrective actions have been taken, but in no event less than three (3) years following expiration or termination of the Agreement for any reason.

5. Incident Reporting/Action. If there is a violation of Supplier's security procedures or a potential security incident/infraction relating to the Supplier Environment, then Supplier will immediately (a) report the incident to Coke Florida in writing; (b) promptly provide a full investigative report along with the corrective action(s) reasonably necessary to prevent a future recurrence of such violation, security incident or infraction; (c) promptly take such corrective actions; and (d) take such other investigative actions and measures to ensure that such corrective actions are and will remain effective. This process will be integrated with Coke Florida's Computer Incidence Response Team Process attached hereto as Attachment 5; thereafter, Coke Florida will have the right to perform, at Coke Florida's cost, by an independent third party chosen by Coke Florida and reasonably acceptable to Supplier, or through Coke Florida's own personnel, a security audit. If such an audit concludes that Supplier has not adequately taken corrective action to prevent a future reoccurrence of such violation or security incident/infraction: (1) Supplier will promptly take whatever corrective actions are reasonably necessary to prevent future reoccurrence of such violation or security incident/infraction, and (2) Supplier will reimburse Coke Florida for all reasonable costs of the audit. The rights and remedies afforded Coke Florida under this paragraph will continue until all reasonably necessary corrective actions have been taken. Upon the occurrence of a security incident or investigation, or upon Coke Florida's request, Supplier, at its expense, will deliver to Coke Florida in electronic form information directly connected to the Coke Florida Confidential Information that resides in the server logs, Web logs, application logs, and/or security event logs ("**Logs**"). Supplier agrees to produce for Coke Florida written or electronic copies of said information from such Logs and to retain all such Logs during the Term of the Agreement and for a period of three (3) years thereafter.

6. Additional Data Security Breach Requirements. In the event of any unauthorized access to and acquisition of any information that identifies or can be used to identify an individual, including, without limitation: (a) name, (b) mailing address, (c) telephone or fax number, (d) e-mail address, and (e) identification number ("**Personal Information**") while left in the custody of Supplier or Supplier's contractors, vendors, or suppliers under the Agreement, which compromised the security, confidentiality or integrity of such Personal Information ("**Data Security Breach**"), Supplier shall reimburse Coke Florida for the direct costs, if any, incurred by Coke Florida in (a) preparation and mailing of notices to such affected individuals as Coke Florida may deem appropriate, (b) call center support and the provision of credit monitoring services to such individuals for a period not exceeding twelve (12) months, and (c) implementing remediation measures required under applicable law, provided that Coke Florida gives Supplier reasonable prior written notice of its intent to deliver such notice and provide such services and remediation measures. In addition to the foregoing, Supplier shall indemnify, defend, and hold Coke Florida harmless from and against any: (i) claim of identity theft or identity fraud brought against Coke Florida by any third party whose Personal Information was compromised by a Data Security Breach ("**Identity Theft Claim**") and Supplier shall pay any damages awarded against Coke Florida or included in any settlement agreement resulting from such Identity Theft Claim, but only to the extent that the alleged identity theft or identity fraud was caused directly by the Data Security Breach; and (ii) enforcement or administrative proceeding, or any judicial action brought against Coke Florida by any attorney general or other governmental regulatory agency or authority, which results from a Data Security Breach ("**Regulatory Claim**"), and Supplier shall pay any fines or penalties imposed upon Coke Florida as a result of any such Regulatory Claim, but only to the extent caused

directly from such violation by Supplier and/or Supplier's contractors, vendors, and/or suppliers. Coke Florida hereby grants to Supplier the option to control the defense and/or settlement of the claim or demand. In the event Supplier exercises such option: (i) Supplier shall not settle any claim requiring any admission of fault on the part of Coke Florida without Coke Florida's prior written consent, (ii) Coke Florida shall have the right to participate, at its own expense, in the claim or suit, and (iii) Coke Florida agrees to cooperate with Supplier as may be reasonably requested. In the event Supplier does not exercise its option to control the defense and/or settlement, then Supplier shall pay Coke Florida only those reasonable attorney's fees incurred with respect to the defense or settlement of the claim or portion thereof directly related to the Data Security Breach.

7. Remediation Requirements. In the event of any Data Security Breach, Supplier shall implement, at no additional cost to Coke Florida, and cause all its contractors, vendors, and suppliers involved in the Data Security Breach to implement, such remediation actions specified by Coke Florida and, at a minimum, implementation of the following remediation actions: (a) security engineering tested procedures for Multi-Factor Authentication ("**MFA**") on all Office 365 ("**O365**") email administrators; (b) desktop support team initiated password resets for several users, including the users associated with the compromised email accounts; (c) enabled top-level domain filtering of suspicious domain names associated with the incident; (d) created O365 transport rule deleting messages with key features (i.e., unique, identifiable text) related to the phishing email; (e) deployed patches for different systems; and (f) developed materials for employee training and awareness of the risks of phishing emails and other cyber risks.

8. System Back-up; Data Storage and Disaster Recovery. Supplier will perform regular and no less than daily backups of the system and all Coke Florida Confidential Information and provide data recovery and archiving in accordance with the disaster recovery plan attached hereto as Attachment 6) (the "**Disaster Recovery Plan**"). If Coke Florida Confidential Information becomes lost or corrupted, Supplier will immediately restore the lost or corrupted Coke Florida Confidential Information from the latest backup maintained by Supplier. As part of the application(s) provided and at no additional cost to Coke Florida, Supplier will (a) implement and manage the Disaster Recovery Plan no later than the activation date; (b) within thirty (30) days of the activation date, and at least once every year thereafter during the Term of the Agreement, update and test the operability of the Disaster Recovery Plan; (c) upon Coke Florida's request, certify to Coke Florida that the Disaster Recovery Plan is fully operational; and (d) upon discovery by Supplier, immediately provide Coke Florida with a notice of any disaster or loss of Coke Florida Confidential Information and immediately implement the Disaster Recovery Plan upon the occurrence of any such event. In the event a disaster causes Supplier to allocate limited resources between or among Supplier's affiliates, Coke Florida will receive at least the same priority in respect of such allocation as Supplier's customers and affiliates and Supplier's other preferred commercial customers. Back-up information that is physically transferred offsite will be encrypted using at least 256-bit encryption. Off-site storage facilities housing backup media must be communicated to Coke Florida and protected according to Coke Florida's guidelines.

9. Secure Coding Guidelines. For development of any software code included in the application(s) provided under the Agreement, Supplier agrees to abide by the Secure Coding Guidelines set forth in Attachment 7.

10. Application/System Assessment including Websites. Supplier further grants Coke Florida the right to conduct an assessment of the Services, the Supplier Environment, Supplier's systems ("**System**") and any other equipment, software or systems maintained by or on behalf of Supplier or its contractors, vendors, suppliers, or subcontractors to provide the Services or to host or store any Coke Florida data prior to the activation date and thereafter during the Term of the Agreement. Any such assessment will be performed in accordance with the assessment methodology set forth in Attachment 8 attached hereto. Coke Florida is authorized to conduct the assessment utilizing hardware and/or equipment owned or leased by Coke Florida. Both parties agree that any high-risk findings will be mitigated by Supplier, at Supplier's sole cost and expense, before the System and Services are put into production.

11. Single Sign-On. Coke Florida may request that Supplier make available to Coke Florida and Participants a "single sign-on capability" ("**SSO Capability**") for service. Such SSO Capability would facilitate a log-in process onto service from the website of Coke Florida, or the website of Coke Florida's third-party website provider, that would eliminate the need for a Participant to re-enter user identification data and/or passwords after the Participant's initial visit to service. Coke Florida and Supplier agree to abide by the terms of Single Sign-On set forth in Attachment 9 attached hereto.

12. Payment Card Industry. In the event that Supplier collects credit card information in connection with its Services, Supplier agrees to comply with VISA's, MasterCard's and any other payment card association's rules and regulations, including, but not limited to, their respective data security program and disaster recovery requirements. Supplier agrees to provide data security reports as required by the respective associations, pay to such association any fines and penalties in the event Supplier fails to comply with such data security requirements, provide full cooperation and access to permit such credit card association to conduct a security review of Supplier's policies and procedures. Coke Florida reserves the right to terminate the Agreement in the event that a credit card association finds that Supplier has failed to cure any non-compliance with its data security requirements within thirty (30) days after notice of non-compliance within the agreed upon timeframe for remediation and such non-compliance or failure will be deemed a material breach under the terms of the Agreement.

13. Breach of Coke Florida's Security Requirements. Any breach by Supplier of any terms or conditions of Coke Florida's Security Requirements will be deemed a breach by Supplier of the Agreement and any orders or SOWs entered into by the parties. Coke Florida may, in addition to any other remedies it may have at law and inequity and pursuant to the Agreement, terminate the Agreement and any orders or SOWs upon such a breach by Supplier of these Security Requirements with notice to Supplier.

Attachment 1

Cloud Security Alliance Questionnaire

Information Security and Controls Risk Management Process for Third-Party Due Diligence

Please follow the instructions below to complete the assessment:

1. *Complete the identification questions below on this page.*
2. *Complete the Questionnaire based on the CSA CAIQ (beginning on the next page).*
    a. *Answer all of the Response questions "Yes" or "No" or "N/A". Please answer ONLY with "Yes" or "No" or "N/A".*
    b. *You must use the 'Additional Information' field to provide supporting information to all 'No' or 'N/A' responses.*
    c. *For further clarification, please see https://cloudsecurityalliance.org/research/cai/.*
3. *Save the completed questionnaire with the filename **3PQ <vendor name>.docx**.*
4. *Return the questionnaire to your Coke Florida project manager, who will submit it to Information Security and Controls.*

RESPONDER NAME: _____

RESPONDER JOB TITLE: _____

RESPONDER EMAIL: _____

RESPONDER PHONE: _____

DATE: _____

Domain	Control Group	CID	Consensus Assessment Questions	Answer	Additional Information
Compliance					
Compliance	Audit Planning	CO-01.1	Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?		
Compliance	Independent Audits	CO-02.1	Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?		
Compliance		CO-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?		
Compliance		CO-02.3	Do you conduct regular application penetration tests of your cloud infrastructure as prescribed by industry best practices and guidance?		
Compliance		CO-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?		
Compliance		CO-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?		
Compliance		CO-02.6	Are the results of the network penetration tests available to tenants at their request?		
Compliance		CO-02.7	Are the results of internal and external audits available to tenants at their request?		
Compliance	Third Party Audits	CO-03.1	Do you permit tenants to perform independent vulnerability assessments?		
Compliance		CO-03.2	Do you have external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks?		
Compliance	Contact / Authority Maintenance	CO-04.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?		

Compliance	Information System Regulatory Mapping	CO-05.1	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?		
		CO-05.2	Do you have capability to logically segment and recover data for a specific customer in the case of a failure or data loss?		
Compliance	Intellectual Property	CO-06.1	Do you have policies and procedures in place describing what controls you have in place to protect tenants' intellectual property?		
Compliance	Intellectual Property	CO-07.1	If utilization of tenants services housed in the cloud is mined for cloud provider benefit, are the tenants IP rights preserved?		
Compliance	Intellectual Property	CO-08.1	If utilization of tenants services housed in the cloud is mined for cloud provider benefit, do you provide tenants the ability to opt-out?		
Data Governance					
Data Governance	Ownership / Stewardship	DG-01.1	Do you follow a structured data-labeling standard (ex. ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?		
Data Governance	Classification	DG-02.1	Do you provide a capability to identify virtual machines via policy tags/metadata (ex. Tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country, etc.)?		
Data Governance		DG-02.2	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (ex. TXT/TPM, VN-Tag, etc.)?		
Data Governance		DG-02.3	Do you have a capability to use system geographic location as an authentication factor?		
Data Governance		DG-02.4	Can you provide the physical location/geography of storage of a tenant's data upon request?		
Data Governance		DG-02.5	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?		

Data Governance	Handling / Labeling / Security Policy	DG-03.1	Are policies and procedures established for labeling, handling and security of data and objects which contain data?		
Data Governance		DG-03.2	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?		
Data Governance	Retention Policy	DG-04.1	Do you have technical control capabilities to enforce tenant data retention policies?		
Data Governance		DG-04.2	Do you have a documented procedure for responding to requests for tenant data from governments or third parties?		
Data Governance	Secure Disposal	DG-05.1	Do you support secure deletion (ex. degaussing / cryptographic wiping) of archived data as determined by the tenant?		
Data Governance		DG-05.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?		
Data Governance	Nonproduction Data	DG-06.1	Do you have procedures in place to ensure production data will not be replicated or used in non-production environments?		
Data Governance	Information Leakage	DG-07.1	Do you have controls in place to prevent data leakage or intentional/accidental compromise between tenants in a multi-tenant environment?		
Data Governance		DG-07.2	Do you have a Data Loss Prevention (DLP) or extrusion prevention solution in place for all systems which interface with your cloud service offering?		
Data Governance	Risk Assessments	DG-08.1	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status?)		
Facility Security					
Facility Security	Policy	FS-01.1	Can you provide evidence that policies and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?		

Facility Security	User Access	FS-02.1	Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification?		
Facility Security	Controlled Access Points	FS-03.1	Are physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?		
Facility Security	Secure Area Authorization	FS-04.1	Do you allow tenants to specify which of your geographic locations their data is allowed to traverse into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?		
Facility Security	Unauthorized Persons Entry	FS-05.1	Are ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises monitored, controlled and isolated from data storage and process?		
Facility Security	Offsite Authorization	FS-06.1	Do you provide tenants with documentation that describes scenarios where data may be moved from one physical location to another? (ex. Offsite backups, business continuity failovers, replication)		
Facility Security	Offsite equipment	FS-07.1	Do you provide tenants with documentation describing your policies and procedures governing asset management and repurposing of equipment?		
Facility Security	Asset Management	FS-08.1	Do you maintain a complete inventory of all of your critical assets which includes ownership of the asset?		
Facility Security		FS-08.2	Do you maintain a complete inventory of all of your critical supplier relationships?		
Human Resources Security					
Human Resources Security	Background Screening	HR-01.1	Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification?		

Human Resources Security	Employment Agreements	HR-02.1	Do you specifically train your employees regarding their role vs. the tenant's role in providing information security controls?		
		HR-02.2	Do you document employee acknowledgment of training they have completed?		
Human Resources Security	Employment Termination	HR-03.1	Are Roles and responsibilities for following performing employment termination or change in employment procedures assigned, documented and communicated?		
Information Security					
Information Security	Management Program	IS-01.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?		
Information Security	Management Support / Involvement	IS-02.1	Are policies in place to ensure executive and line management take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution?		
Information Security	Policy	IS-03.1	Do your information security and privacy policies align with particular industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?		
		IS-03.2	Do you have agreements which ensure your providers adhere to your information security and privacy policies?		
		IS-03.3	Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?		
Information Security	Baseline Requirements	IS-04.1	Do you have documented information security baselines for every component of your infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc.)?		
Information Security		IS-04.2	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?		
Information Security		IS-04.3	Do you allow your Coke Floridas to provide their own trusted virtual machine image to ensure conformance to their own internal standards?		

Information Security	Policy Reviews	IS-05.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?		
Information Security	Policy Enforcement	IS-06.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?		
Information Security		IS-06.2	Are employees made aware of what action might be taken in the event of a violation and stated as such in the policies and procedures?		
Information Security	User Access Policy	IS-07.1	Do you have controls in place ensuring timely removal of systems access which is no longer required for business purposes?		
Information Security		IS-07.2	Do you provide metrics which track the speed with which you are able to remove systems access which is no longer required for business purposes?		
Information Security	User Access Restriction / Authorization	IS-08.1	Do you document how you grant and approve access to tenant data?		
Information Security		IS-08.2	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?		
Information Security	User Access Revocation	IS-09.1	Is timely de-provisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or third parties?		
Information Security		IS-09.2	Is any change in status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?		
Information Security	User Access Reviews	IS-10.1	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?		
Information Security		IS-10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?		

Information Security		IS-10.3	Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?		
Information Security	Training / Awareness	IS-11.1	Do you provide or make available a formal security awareness training program for cloud-related access and data management issues (i.e., multi-tenancy, nationality, cloud delivery model segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?		
Information Security		IS-11.2	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?		
Information Security	Industry Knowledge / Benchmarking	IS-12.1	Do you participate in industry groups and professional associations related to information security?		
		IS-12.2	Do you benchmark your security controls against industry standards?		
Information Security	Roles / Responsibilities	IS-13.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities vs. those of the tenant?		
Information Security	Management Oversight	IS-14.1	Are Managers responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility?		
Information Security	Segregation of Duties	IS-15.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?		
Information Security	User Responsibility	IS-16.1	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?		
Information Security		IS-16.2	Are users made aware of their responsibilities for maintaining a safe and secure working environment?		
Information Security		IS-16.3	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?		

Information Security	Workspace	IS-17.1	Do your data management policies and procedures address tenant and service level conflicts of interests?		
Information Security		IS-17.2	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?		
Information Security		IS-17.3	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?		
Information Security	Encryption	IS-18.1	Do you have a capability to allow creation of unique encryption keys per tenant?		
Information Security		IS-18.2	Do you support tenant generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate. (E.g. Identity based encryption)?		
Information Security	Encryption Key Management	IS-19.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?		
Information Security		IS-19.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?		
Information Security		IS-19.3	Do you have a capability to manage encryption keys on behalf of tenants?		
Information Security		IS-19.4	Do you maintain key management procedures?		
Information Security	Vulnerability / Patch Management	IS-21.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?		
Information Security		IS-20.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?		
Information Security		IS-20.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?		
Information Security		IS-20.4	Will you make the results of vulnerability scans available to tenants at their request?		

Information Security		IS-20.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?		
Information Security		IS-20.6	Will you provide your risk-based systems patching timeframes to your tenants upon request?		
Information Security	Antivirus / Malicious Software	IS-21.1	Do you have anti-malware programs installed on all systems which support your cloud service offerings?		
Information Security		IS-21.2	Do you ensure that security threat detection systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted timeframes?		
Information Security	Incident Management	IS-22.1	Do you have a documented security incident response plan?		
Information Security		IS-22.2	Do you integrate customized tenant requirements into your security incident response plans?		
Information Security		IS-22.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?		
Information Security	Incident Reporting	IS-23.1	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?		
Information Security		IS-23.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?		
Information Security	Incident Response Legal Preparation	IS-24.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes & controls?		
Information Security		IS-24.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?		
Information Security		IS-24.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?		
Information Security		IS-24.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?		

Information Security	Incident Response Metrics	IS-25.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?		
Information Security		IS-25.2	Will you share statistical information security incident data with your tenants upon request?		
Information Security	Acceptable Use	IS-26.1	Do you provide documentation regarding how you may utilize or access tenant data and/or metadata?		
Information Security		IS-26.2	Do you collect or create metadata about tenant data usage through the use of inspection technologies (search engines, etc.)?		
Information Security		IS-26.3	Do you allow tenants to opt-out of having their data/metadata accessed via inspection technologies?		
Information Security	Asset Returns	IS-27.1	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?		
Information Security		IS-27.2	Is your Privacy Policy aligned with industry standards?		
Information Security	e-Commerce Transactions	IS-28.1	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to traverse public networks? (ex. the Internet)		
Information Security		IS-28.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate to each other over public networks (ex. Internet-based replication of data from one environment to another)?		
Information Security	Audit Tools Access	IS-29.1	Do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)		
Information Security	Diagnostic / Configuration Ports Access	IS-30.1	Do you utilize dedicated secure networks to provide management access to your cloud service infrastructure?		
Information Security	Network / Infrastructure Services	IS-31.1	Do you collect capacity and utilization data for all relevant components of your cloud service offering?		
Information Security		IS-31.2	Do you provide tenants with capacity planning and utilization reports?		

Information Security	Portable / Mobile Devices	IS-32.1	Are Policies and procedures established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?		
Information Security	Source Code Access Restriction	IS-33.1	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?		
Information Security		IS-33.2	Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?		
Information Security	Utility Programs Access	IS-34.1	Are utilities that can significantly manage virtualized partitions (ex. shutdown, clone, etc.) appropriately restricted and monitored?		
Information Security		IS-34.2	Do you have a capability to detect attacks which target the virtual infrastructure directly (ex. shimming, Blue Pill, Hyper jumping, etc.)?		
Information Security		IS-34.3	Are attacks which target the virtual infrastructure prevented with technical controls?		
Legal					
Legal	Nondisclosure Agreements	LG-01.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?		
Legal	Third Party Agreements	LG-02.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed and stored and transmitted?		
Legal		LG-02.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?		
Legal		LG-02.3	Does legal counsel review all third party agreements?		
Operations Management					

Operations Management	Policy	OP-01.1	Are policies and procedures established and made available for all personnel to adequately support services operations roles?		
Operations Management	Documentation	OP-02.1	Is Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure Configuring, installing, and operating the information system?		
Operations Management	Capacity / Resource Planning	OP-03.1	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?		
Operations Management		OP-03.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?		
Operations Management	Equipment Maintenance	OP-04.1	If using virtual infrastructure, does your cloud solution include hardware independent restore and recovery capabilities?		
Operations Management		OP-04.2	If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?		
Operations Management		OP-04.3	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?		
Operations Management		OP-04.4	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?		
Operations Management		OP-04.5	Does your cloud solution include software / provider independent restore and recovery capabilities?		
Risk Management					
Risk Management	Program	RI-01.1	Is your organization insured by a 3rd party for losses?		

Risk Management		RI-01.2	Do your organization's service level agreements provide tenant remuneration for losses they may incur due to outages or losses experienced within your infrastructure?		
Risk Management	Assessments	RI-02.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?		
Risk Management		RI-02.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?		
Risk Management	Mitigation / Acceptance	RI-03.1	Are risks mitigated to acceptable levels based on company-established criteria in accordance with reasonable resolution time frames?		
		RI-03.2	Is remediation conducted at acceptable levels based on company-established criteria in accordance with reasonable time frames?		
Risk Management	Business / Policy Change Impacts	RI-04.1	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?		
Risk Management	Third Party Access	RI-05.1	Do you provide multi-failure disaster recovery capability?		
		RI-05.2	Do you monitor service continuity with upstream providers in the event of provider failure?		
		RI-05.3	Do you have more than one provider for each service you depend on?		
		RI-05.4	Do you provide access to operational redundancy and continuity summaries which include the services on which you depend?		
		RI-05.5	Do you provide the tenant the ability to declare a disaster?		
		RI-05.6	Do you provide a tenant triggered failover option?		

		RI-05.7	Do you share your business continuity and redundancy plans with your tenants?		
Release Management					
Release Management	New Development / Acquisition	RM-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities?		
Release Management	Production Changes	RM-02.1	Do you provide tenants with documentation which describes your production change management procedures and their roles/rights/responsibilities within it?		
Release Management	Quality Testing	RM-03.1	Do you provide your tenants with documentation which describes your quality assurance process?		
Release Management	Outsourced Development	RM-04.1	Do you have controls in place to ensure that standards of quality are being met for all software development?		
Release Management		RM-04.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?		
Release Management	Unauthorized Software Installations	RM-05.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?		
Resiliency					
Resiliency	Management Program	RS-01.1	Are Policy, process and procedures defining business continuity and disaster recovery in place to minimize the impact of a realized risk event and properly communicated to tenants?		
Resiliency	Impact Analysis	RS-02.1	Do you provide tenants with ongoing visibility and reporting into your operational Service Level Agreement (SLA) performance?		
Resiliency		RS-02.2	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?		
Resiliency		RS-02.3	Do you provide customers with ongoing visibility and reporting into your SLA performance?		

Resiliency	Business Continuity Planning	RS-03.1	Do you provide tenants with geographically resilient hosting options?		
Resiliency		RS-03.2	Do you provide tenants with infrastructure service failover capability to other providers?		
Resiliency	Business Continuity Testing	RS-04.1	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?		
Resiliency	Environmental Risks	RS-05.1	Is physical protection against damage from natural causes and disasters as well as deliberate attacks anticipated, designed and countermeasures applied?		
Resiliency	Equipment Location	RS-06.1	Are any of your datacenters located in places which have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?		
Resiliency	Equipment Power Failures	RS-07.1	Are Security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?		
Resiliency	Power / Telecommunications	RS-08.1	Do you provide tenants with documentation showing the transport route of their data between your systems?		
Resiliency		RS-08.2	Can Tenants define how their data is transported and through which legal jurisdiction?		
Security Architecture					
Security Architecture	Customer Access Requirements	SA-01.1	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?		
Security Architecture	User ID Credentials	SA-02.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?		
Security Architecture		SA-02.2	Do you use open standards to delegate authentication capabilities to your tenants?		
Security Architecture		SA-02.3	Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?		

Security Architecture		SA-02.4	Do you have a Policy Enforcement Point capability (ex. XACML) to enforce regional legal and policy constraints on user access?		
Security Architecture		SA-02.5	Do you have an identity management system in place which enables both role-based and context-based entitlement to data (enables classification of data for a tenant)?		
Security Architecture		SA-02.6	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometric, etc.) for user access?		
Security Architecture		SA-02.7	Do you allow tenants to use third party identity assurance services?		
Security Architecture	Data Security / Integrity	SA-03.1	Is your Data Security Architecture designed using an industry standard? (ex. CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP CAESARS)		
Security Architecture	Application Security	SA-04.1	Do you utilize industry standards (Build Security in Maturity Model [BSIMM] Benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build-in security for your Systems/Software Development Lifecycle (SDLC)?		
Security Architecture		SA-04.2	Do you utilize an automated source-code analysis tool to detect code security defects prior to production?		
Security Architecture		SA-04.3	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?		
Security Architecture	Data Integrity	SA-05.1	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?		
Security Architecture	Production / Nonproduction Environments	SA-06.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?		
Security Architecture		SA-06.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?		

Security Architecture	Remote User Multifactor Authentication	SA-07.1	Is multi-factor authentication required for all remote user access?		
Security Architecture	Network Security	SA-08.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?		
Security Architecture	Segmentation	SA-09.1	Are system and network environments logically separated to ensure Business and customer security requirements?		
Security Architecture		SA-09.2	Are system and network environments logically separated to ensure compliance with legislative, regulatory, and contractual requirements?		
Security Architecture		SA-09.3	Are system and network environments logically separated to ensure separation of production and non-production environments?		
Security Architecture		SA-09.4	Are system and network environments logically separated to ensure protection and isolation of sensitive data?		
Security Architecture	Wireless Security	SA-10.1	Are policies and procedures established and mechanisms implemented to protect network environment perimeter and configured to restrict unauthorized traffic?		
Security Architecture		SA-10.2	Are policies and procedures established and mechanisms implemented to ensure proper security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings, etc.)		
Security Architecture		SA-10.3	Are policies and procedures established and mechanisms implemented to protect network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?		

Security Architecture	Shared Networks	SA-11.1	Is access to systems with shared network infrastructure restricted to authorized personnel in accordance with security policies, procedures and standards? Networks shared with external entities will have a documented plan detailing the compensating controls used to separate network traffic between organizations?		
Security Architecture	Clock Synchronization	SA-12.1	Do you utilize a synchronized time-service protocol (ex. NTP) to ensure all systems have a common time reference?		
Security Architecture	Equipment Identification	SA-13.1	Is automated equipment identification used as a method of connection authentication to validate connection authentication integrity based on known equipment location?		
Security Architecture	Audit Logging / Intrusion Detection	SA-14.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?		
Security Architecture		SA-14.2	Is Physical and logical user access to audit logs restricted to authorized personnel?		
Security Architecture		SA-14.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?		
Security Architecture	Mobile Code	SA-15.1	Is mobile code authorized before its installation and use and the code configuration checked to ensure that the authorized mobile code operates according to a clearly defined security policy?		
Security Architecture		SA-15.2	Is all unauthorized mobile code prevented from executing?		

Attachment 2

Coke Florida Hosting Security Guidelines

1. Security Measures. Supplier will take, and cause its contractors, vendors, and suppliers to take, appropriate measures to protect the Application(s) against "hackers" and others who may seek to modify the Application(s) or the data therein without the consent of Supplier or Coke Florida, and to correct the Application(s) to its original form in the event that it is modified without Supplier's consent. Supplier will test code for potential areas where security could be breached. Supplier must report to Coke Florida immediately any breaches of security, unauthorized changes, or access to the Application(s). In addition to the foregoing, if Supplier provides the Application(s) to Coke Florida from a location that is shared with a third party or third parties, then Supplier must develop a process, subject to Coke Florida's approval, to restrict access in any such shared environment to that portion dedicated to the Application(s) only to Supplier's personnel engaged in performing services related to the Application(s).

General:

1. All applications are responsible for complying with applicable laws and regulations.
2. All applications that are accessible from the Internet or process 'restricted' data must be approved prior to launch or implementation by Coke Florida.
3. All consumer facing web pages and mobile applications must contain a link to a privacy statement. Web pages that would appear to a consumer as being provided by Coke Florida must have a Coke Florida-otherwise approved privacy statement. Websites and other applications that post the Coke Florida privacy statement must be approved prior to launch by Coke Florida. Questions about this requirement or the content of the Coke Florida privacy statement should be directed to Coke Florida's Senior Vice President, Technology and Enterprise Transformation.
4. All questions related to the following controls should be directed to Coke Florida's Senior Vice President, Technology and Enterprise Transformation.

2. Physical Security

1. The equipment hosting the applications for Coke Florida must be located in a physically secure facility, which requires badge access at a minimum.
2. Physical access to infrastructure housing Coke Florida Confidential Information must be restricted and access allowed based on a need-to-know basis.
3. The hosting provider must have a background check procedure for all data center personnel.
4. Electronic media (online or offline) and confidential hard copy material must be appropriately protected from theft or loss.

3. Authentication

1. All access to systems will be controlled by an authentication method involving a minimum of a unique user ID/password combination.
2. Privileged users and administrators must use strong authentication.
3. Passwords must be changed on a periodic basis.
4. Passwords may never be stored in clear text.
5. Passwords must be complex and not easy to guess or crack. Effectiveness of authentication must be tested on a regular basis to ensure that unauthorized authentication is not easily permitted.
6. Remote network access must be secured by two-factor authentication.
7. All activity performed under a user ID is the responsibility of the individual assigned to that user ID. Users will not share their user ID/password with others or allow other employees to use their User ID/password to perform actions.
8. Use of generic user account will not be permitted.
9. Coke Florida connections must not be allowed to retain access to a disrupted session, a session that has ended abnormally, or when a security-related parameter has been exceeded or violated. An abnormal ending of a session must result in denied access and require the user to begin the login process.

4. Authorization

1. Logical or network access to infrastructure housing Coke Florida Confidential Information must be restricted and access allowed based on a need-to-know basis.
2. Access requests must be documented and approved based on a business need.
3. Access rights must be reviewed on periodic basis.
4. Upon termination or resignation of hosting provider personnel, access must be revoked within a timely manner.
5. Upon request, a list of users with access to Coke Florida Confidential Information must be provided.

5. System Security

1. The Application(s) must be securely configured according to a security baseline. This baseline must include removing unnecessary services and changing default, vendor-supplied or otherwise weak user accounts and passwords.
2. System components must maintain current security patch levels.
3. Web servers must be hardened according to a secure baseline.
4. Web servers must only allow the HTTP methods GET, HEAD, POST on a production web server. All other methods must be disabled, including TRACE and TRACK which are used in Cross-Site Tracing attacks.
5. Web servers must be configured to accept requests for only authorized and published directories. Default sites, executable or directory listings must be disabled.
6. An inventory of technology used to store or process Coke Florida data must be maintained.

6. Antivirus/Malware

1. Technologies must be used to monitor and remediate malware within the environment.
2. Malware prevention technologies should include, but are not limited to, desktop and gateway antivirus.

7. Change Management

1. Change requests will be documented via a change request form. The change request form will contain, at a minimum, the following information:
2. Business justification for the change
3. Nature of defect (if applicable)/enhancement
4. Testing required
5. Back-out procedures
6. Systems affected
7. User contact
8. The process to review and approve change requests must be documented. The process must include management approval.
9. Upon request, a list of change requests for systems housing Coke Florida Confidential Information must be provided.

8. Network Security

1. Industry standard firewalls must be implemented to protect the application environment and associated data from the Internet and untrusted networks.
2. Inbound and outbound connections must be denied unless expressly allowed.
3. Firewall events must be monitored in order to detect potential security events.
4. Network Intrusion Detection or Prevention Systems ("**NIDS/NIPS**") must be implemented to monitor traffic for applications handling confidential information.
5. Effectiveness of controls must be tested on a periodic basis.

9. Logging and Monitoring

1. Security relevant events, including, but not limited to, login failures, use of privileged accounts, changes to access models or file permissions, modification to installed software, or the operating system, changes to user permissions, or privileges or use of any privileged system function, will be logged on all systems.
2. Security logs will be retained for a minimum of one (1) year and with ninety (90) days maintained online. Access to security logs will be restricted to authorized persons.
3. The Application(s) clocks will be synchronized to an agreed standard to ensure the accuracy of audit logs.

10. Disaster Recovery/Availability

1. The Application(s) and application software backup will be performed before regularly scheduled system upgrades and/or maintenance occurs.
2. The Application(s) must be tested on a regular basis to ensure that contractual SLAs can be met.

11. Confidentiality

1. No unauthorized access to Coke Florida Confidential Information will be permitted. Controls may include, but are not limited to, access control lists and encryption to protect Coke Florida Confidential Information.
2. Any unauthorized disclosure of Coke Florida Confidential Information must be reported to Coke Florida personnel immediately upon discovery of release.

12. Security Incidents

1. Any security incident must be reported to Coke Florida in a timely manner.
2. Supplier must have personnel trained to identify and respond to security attacks.

13. Application Security

1. Supplier will use a source code control system that authenticates and logs the team member associated with all changes to the software baseline and related configuration and build files.
2. Supplier will disclose if requested all third party software used in the software development and testing, including all binaries, frameworks, components and other products, whether commercial, free, open source or closed-source.
3. Supplier will review the security of the application including testing for common vulnerabilities such as those identified by OWASP and the Security Requirements.
4. All critical and high Severity issues that are identified will be addressed within an appropriate timeframe acceptable to both Supplier and Coke Florida.
5. Supplier will use all commercially reasonable efforts consistent with sound software development practices.
6. Supplier has developed secure coding guidelines that address the following:
   a. Input Validation and Encoding
   b. Authentication and Session Management
   c. Access Control
   d. Error Handling
   e. Logging
   f. Connections to External Systems
   g. Encryption
7. Confidential Information must be encrypted with strong encryption when transmitted over public networks. Confidential Information should be encrypted with strong encryption over internal networks.
8. Confidential Information should be encrypted when stored. Payment card information and social security numbers must be encrypted in storage at all times and must not reside on a DMZ. Additional types of data may require encryption based upon the results of a security review or changes in risk posture. Certain types of information, such as payment card "card-in-hand" numbers (CVV2, CIM, etc.) must not be stored.
9. Passwords, PINs and non-fixed password token data must always be encrypted when held in storage or when transmitted over networks.
10. Web pages sending or receiving confidential information, including authentication credentials, must use SSL 3.0 128-bit encryption with digital certificates signed by a trusted certificate authority. The use of self-signed certificates on Internet facing production web applications is not permitted.
11. For web applications, all confidential information must be sent using HTTP POST requests. The GET method must not be used to send confidential information via URL parameters.
12. For web applications, if a user is directed from a secure page to a non-secure page or non-Coke Florida site, appropriate notice of such redirection should be provided. Links to non-Coke Florida sites should not contain or transfer confidential information within the content or coding of the hyperlink.
13. Cookies should be marked with descriptive identifiers so that the nature of the data is evident to the user. (ISMP 10.6.6.a)
14. Cookies must not be used to store confidential information other than a session-id.
15. Cookies must not contain clear-text authentication information.
16. Confidential information should only be provided during a single session.
17. For web applications, page expiration should be enabled after a pre-defined period of time to prevent the continual display of confidential information after session activity has ceased. (ISMP 10.6.7.b)
18. Users will be provided with the ability to end a session with the application. Any active personal information should be expunged upon session completion and/or Coke Florida/browser termination.
19. For web applications, session-id values used for authentication and session management must be sufficiently randomized to prevent them from being guessed. The session-id value must not be based on authentication credentials and must not be persistent across different sessions.
20. For web applications, SSL must be used when username and password credentials are transmitted. SSL should be used upon subsequent page views in order to protect the session cookie.
21. For web applications, session or authentication information must not be passed through the URL. The POST method should be used to collect authentication information and cookies should be used to maintain session-ids.
22. Consumer message boards that discuss confidential information should use aliases and passwords to control access and use aliases for posting.

23. Forms displaying confidential fields, such as payment cards or social security numbers, must mask some or all of such data fields for fields larger than four characters. Fields of less than four characters should be completely masked.
24. For web applications, unless the site complies with COPPA regulations, web pages collecting age or date of birth information must not allow values entered for users under the age of 13.
25. Points of input, regardless of accessibility within the user interface, must be validated to ensure it is appropriate. Input should be checked for SQL or command injection, cross-site-scripting, buffer overflows or other similar attacks resulting from unvalidated input. (ISMP 10.9.1)
26. Handling mechanisms must use a "fail-closed" or "fail-safe" methodology. If an error occurs, then an appropriate decision must be made to continue or stop access. If the application does not know what to do, then it must "fail-closed" and stop access.
27. In production environments, error messages must not contain unnecessary information such as line numbers, code snippets, SQL statements, XML data, or application/platform name and version information. In cases where users will report error conditions, create error codes that are meaningful for the developers, but not meaningful to the user.
28. Applications should be developed to be resistant to Denial of Service ("**DoS**") conditions that can cause an application to become unavailable.
29. Applications should be regularly tested for network or application security attacks.

Attachment 3

Data Classification Guide

NOT CLASSIFIED: All nonpublic Coke Florida information does not require classification. Some information will not impact Coke Florida if it is disclosed to unauthorized individuals or if its integrity is impaired. However, all nonpublic Coke Florida information is subject to Coke Florida review or disclosure procedures to mitigate potential risks of inappropriate disclosure.

CONFIDENTIAL: Information, that if disclosed to unauthorized individuals outside Coke Florida, altered, misused or destroyed, may have a substantial adverse impact to Coke Florida. A negligible adverse impact will occur if the information is disclosed to unauthorized individuals, within Coke Florida. Access to this information will 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 an Officer of Coke Florida.
Classified Systems must comply with Coke Florida technical security standards (or equivalent).

HIGHLY RESTRICTED: Information that, if disclosed to unauthorized individuals (outside Coke Florida or within Coke Florida), altered, misused or destroyed, will directly cause damage to Coke Florida'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 will be granted to an individual on a need to know basis. Access to this information requires prior approval of the Senior Vice President, Technology and Enterprise Transformation of Coke Florida.
Classified systems must comply with Coke Florida 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 will 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 will be granted to an individual on a need to know basis. Access to this information requires prior approval of the Senior Vice President, Technology and Enterprise Transformation of Coke Florida. Refer to Coke Florida's Privacy Policy for additional information.

	ELECTRONIC MESSAGING SERVICES (1)	ELECTRONIC DOCUMENTS/ FILES	DATABASES/ STORAGE SYSTEMS/ APPLICATIONS	REMOVABLE MEDIA (2)	MOBILE DEVICES (3)	HARD COPY	VOICEMAIL / PHONE	DISPOSAL
NOT CLASSIFIED	No restrictions	No restrictions	No restrictions	No restrictions	No restrictions	No restrictions	No restrictions	No restrictions
CONFI-DENTIAL	Marked 'Confidential' in the Message Sensitivity setting, where available, or Subject line Encryption recommended	Marked 'Confidential' on every page, view, or document meta-data Encryption recommended	Marked 'Confidential' in meta-data, online screen displays and reports Encryption recommended Accessed via Company approved Secure Access Zone (SAZ) or authorized Third Party Provider	Marked 'Confidential' on exterior / adhesive label, where feasible Encryption recommended Secured in locked container, cabinet or drawer when not in use Do not leave unattended	Encryption recommended Do not leave unattended	Marked 'Confidential' on every page Secured in locked container, cabinet or drawer when not in use Facsimile transmission permitted when sender and receiver present Sent in protected envelope using normal post Do not leave unattended	Recipient can be identified and spoken to Voicemail identifies classification; messages deleted when no longer required Information not discussed in public place where it may be overheard Discussions via mobile phone conducted with discretion	Data on removable media, mobile devices, and hard drives irretrievably deleted prior to reuse or destruction Cross cut shredding or Company approved secure waste disposal service mandatory for hard copy documents
HIGHLY RE-STRICTED	Marked 'Highly Restricted' in the Message Sensitivity setting, where available, or Subject line Encryption mandatory	Marked 'Highly Restricted' on every page, view, or document meta-data Encryption mandatory	Marked 'Highly Restricted' in meta-data, online screen displays and reports Encryption recommended for enterprise database systems within a Company approved secure data center; otherwise encryption mandatory Accessed via Company approved Secure Access Zone (SAZ) or authorized Third Party Provider	Marked 'Highly Restricted' on exterior / adhesive label, where feasible Encryption mandatory Secured in locked container, cabinet, drawer, or safe when not in use Do not leave unattended	Encryption mandatory Do not leave unattended	Marked 'Highly Restricted' on every page Secured in locked container, cabinet, drawer, or safe when not in use Facsimile transmission not permitted Sent in protected envelope or tamper evident packaging by bonded courier; delivery tracking and recipient confirmation required Do not leave unattended	Voicemail not permitted Information not discussed in public place where it may be overheard Discussions conducted via mobile phone with discretion	Data on removable media, mobile devices, and hard drives irretrievably deleted prior to reuse or destruction Cross cut shredding or Company approved secure waste disposal service mandatory for hard copy documents
PERSONAL INFOR-MATION	Marked 'Personal Information' in the Message Sensitivity setting, where available, or Subject line Encryption mandatory for Sensitive Personal Information	Marked 'Personal Information' on every page, view, or document meta-data Encryption mandatory for Sensitive Personal Information stored on removable media	Marked 'Personal Information' in meta-data, online screen displays and reports Encryption recommended Accessed via Company approved Secure Access Zone (SAZ) or authorized Third Party Provider	Marked 'Personal Information' on exterior / adhesive label, where feasible Encryption mandatory for Sensitive Personal Information Secured in locked container, cabinet or drawer when not in use Do not leave unattended	Encryption mandatory for Sensitive Personal Information Do not leave unattended	Marked 'Personal Information' on every page Secured in locked container, cabinet or drawer when not in use Facsimile transmission permitted when sender and receiver present Sensitive Personal Information sent in protected envelope by bonded courier; delivery tracking and recipient confirmation required Do not leave unattended	Recipient can be identified and spoken to Voicemail identifies classification; messages deleted upon receipt Information not discussed in public place where it may be overheard Discussions via mobile phone conducted with discretion	Data on removable media, mobile devices, and hard drives irretrievably deleted prior to reuse or destruction Cross cut shredding or Company approved secure waste disposal service mandatory for hard copy documents

Attachment 4

Data Privacy Security Requirements

(a) **Roles.** During the course of providing Services and the Application(s), Supplier and Supplier's contractors, vendors, and suppliers may be provided access to or otherwise obtain Personal Information (as defined below) from, or on behalf of, Coke Florida. Supplier agrees to protect, and cause all its contractors, vendors, and suppliers to protect, all Personal Information as detailed in this Attachment. In relation to the Personal Information (i) Coke Florida will at all times act as and maintain the role of the owner and/or controller of such information; and (ii) Supplier will at all times act as and maintain the role of the processors, and, subject to Section K, will only process or transfer such Personal Information as instructed and permitted by Coke Florida, and only to perform obligations under this Attachment and as specifically permitted by the Agreement or as otherwise instructed in writing from time to time by Coke Florida. Supplier may not use Personal Information for any other purpose, including, without limitation, for its own commercial benefit, unless agreed to in writing by Coke Florida.

(b) **Definitions.** For the purposes of this Attachment, the following definitions will apply:

a. "**Personal Information**" means any information that identifies or can be used to identify an individual, including, without limitation: (a) name; (b) mailing address; (c) telephone or fax number; (d) email address; (e) and identification number.

b. "**Privacy Laws**" means all national, state or local laws, regulations, ordinances, or other government standard relating to the privacy, confidentiality or security of Personal Information that apply to Supplier's and Supplier's contractors', vendors', and suppliers' handling of Personal Information, including any of the foregoing imposing minimum security requirements; requiring the secure disposal of Personal Information; requiring notice to individuals of incidents involving unauthorized access, acquisition or use of information about them; or any governing general data protection, electronic commerce or data retention.

c. "**Security Incident**" means a situation where Supplier reasonably believes that there has been any unauthorized access, acquisition, use, disclosure or destruction of or damage to Personal Information, or any other breach of applicable law, this Attachment or the Agreement in relation to the processing of Personal Information by any current or former employee, contractor, vendor, supplier, or agent of Supplier or by any other person or third party.

(c) **Instructions.** The Agreement (including the exhibits and attachments hereto) constitutes the written instructions by Coke Florida as of the effective date for Supplier's processing of Personal Information. Such instructions may be modified and/or supplemented from time to time (i) by written agreement of Coke Florida and Supplier or (ii) by written notice from Coke Florida to Supplier, so long as the modification or supplement does not impact Supplier's cost of providing or ability to provide the Application(s).

(d) **Access Limitations.** Supplier agrees that it will maintain, and cause its contractors, vendors, and suppliers to maintain, appropriate access controls, including, but not limited to, limiting access to Personal Information to the minimum number of personnel who require such access in order to provide the Application(s) to Coke Florida.

(e) **Security Incidents.** Supplier will notify Coke Florida in writing immediately (and in any event within thirty-six (36) hours) whenever Supplier reasonably believes that there has been a Security Incident. After providing notice, Supplier will investigate the Security Incident, take all necessary steps to eliminate or contain the exposure of Personal Information, and keep Coke Florida advised of the status of the Security Incident and all related matters. Supplier further agrees to provide, at Supplier's sole cost, reasonable assistance and cooperation requested by Coke Florida and/or Coke Florida's designated representatives, in the furtherance of any correction, remediation, or investigation of any Security Incident and/or the mitigation of any damage, including any notification that Coke Florida may determine appropriate to send to affected individuals, regulators or third parties, the provision of any information or actions required by applicable law, including, without limitation, the Florida Information Protection Act and the Health Insurance Portability and Accountability Act, and/or the provision of any credit reporting service that Coke Florida deems appropriate to provide to affected individuals. Unless required by law, Supplier will not notify any individual or any third party other than law enforcement of any potential Security Incident involving Personal Information without first consulting with, and obtaining the permission of, Coke Florida. In addition, within thirty (30) days of identifying or being informed of a Security Incident, Supplier will develop and execute a plan, subject to Coke Florida's approval, that reduces the likelihood of a recurrence of a Security Incident. For the avoidance of doubt, any additional data breach and security incident related requirements stated on pages 1 and 2 of these Security Requirements, including, without limitation, in Section 6 (Additional Data Breach Security Requirements) and Section 7 (Remediation Requirements) shall similarly apply in the event of a Security Incident.

(f) **Information Return or Disposal.** Supplier will, as appropriate and as directed by Coke Florida, regularly dispose of Personal Information that is maintained by Supplier and/or Supplier's contractors, vendors, and/or suppliers, but that is no longer necessary to provide the Services. Upon termination or expiration of the Agreement for any reason or upon Coke Florida's request, Supplier will immediately cease handling, and cause its contractors, vendor, and suppliers to cease handling, Personal Information and will return in a manner and format reasonably requested by Coke Florida, or, if specifically directed by Coke Florida, will destroy, and cause its contractors, vendors, and suppliers to destroy, any or all Personal Information in Supplier's and Supplier's contractors', vendors', and suppliers' possession, power or control. If Supplier and/or Supplier's contractors, vendors, and/or suppliers disposes of any paper, electronic or other record containing Personal Information, Supplier and Supplier's contractors, vendors, and suppliers will do so by taking all reasonable steps (based on the sensitivity of the information) to destroy the Personal Information by: (a) shredding; (b) permanently erasing and deleting; (c) degaussing; or (d) otherwise modifying the Personal Information in such records to make it unreadable, unreconstructable and indecipherable. Upon request, Supplier will provide a written certification that Personal Information has been returned or securely destroyed in accordance with this Section.

(g) **Privacy.** The parties acknowledge that the Application will collect Personal Information of individuals. Such data will be collected and used in accordance with a privacy policy to be prepared by Coke Florida and agreed upon by Supplier, and Supplier's contractors, vendors, and suppliers, and predominantly displayed in the Application in accordance with legal requirements. The parties agree to adhere to the terms of the privacy policy, and not to use or

distribute Personal Information collected from individuals in any manner that is inconsistent with such privacy policy.

(h) **Subcontracting.** Supplier will ensure that Personal Information is not disclosed to, transferred to or allowed to be accessed by any third party (including affiliates and subcontractors) without the prior written permission of Coke Florida, except (i) as specifically stated in this Attachment or the Agreement, or (ii) where such disclosure or transfer is required by any applicable law, regulation, or public authority. If Coke Florida approves Supplier's disclosure of and/or transfer granting access to Personal Information to a third party, the third party will, prior to any disclosure, have entered into an agreement at least as restrictive as the Agreement and this Attachment. The agreement will be provided to Coke Florida promptly upon request. Supplier will remain accountable and responsible for all actions by such third parties with respect to the disclosed or transferred Personal Information.

(i) **Data Integrity.** If applicable, ensure that all Personal Information created by Supplier on behalf of Coke Florida is accurate and, where appropriate, kept up-to-date. Ensure that any Personal Information that is inaccurate or incomplete is erased or rectified in accordance with Coke Florida's instructions or applicable provisions in this Attachment.

(j) **Access Requests.** Supplier will promptly notify Coke Florida in writing (and in any event within five (5) days of receipt), unless specifically prohibited by applicable law, if Supplier receives: (i) any requests from an individual with respect to Personal Information processed, including, but not limited to, opt-out requests, requests for access and/or rectification, and all similar requests, and will not respond to any such requests unless expressly authorized to do so by Coke Florida; or (ii) any complaint relating to the processing of Personal Information, including, but not limited to, allegations that the processing infringes an individual's rights under applicable law.

(k) **Production Requests.** If Supplier receives any order, demand, warrant, or any other document requesting or purporting to compel the production of Personal Information under applicable law (including, for example, by oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil investigative demands or other similar processes), Supplier will immediately notify Coke Florida (except to the extent otherwise required by applicable law) and will not disclose the Personal Information to the third party without providing Coke Florida at least forty-eight (48) hours, following such notice, so that Coke Florida may, at its own expense, exercise such rights as it may have under law to prevent or limit such disclosure. Notwithstanding the foregoing, Supplier will exercise commercially reasonable efforts to prevent and limit any such disclosure and to otherwise preserve the confidentiality of the Personal Information and will cooperate with Coke Florida with respect to any action taken with respect to such request, complaint, order or other document, including to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to the Personal Information.

(l) **Investigations.** Upon notice to Supplier, Supplier will assist and support Coke Florida in the event of an investigation by any regulator, including a data protection regulator, or similar authority, if and to the extent that such investigation relates to Personal Information handled by Supplier, and/or Supplier's contractors, vendors, and/or suppliers, on behalf of Coke Florida. Such assistance will be at Coke Florida's sole expense, except where such investigation was required due to Supplier's and/or Supplier's contractors', vendors', and/or suppliers' acts or omissions, in which case such assistance will be at Supplier's sole expense.

(m) **Transfer, Disclosure and Access.** Supplier will hold, and will cause its contractors, vendors, and suppliers to hold, Personal Information in strict confidence and ensure that all Personal Information received from or on behalf of Coke Florida is maintained in a secure manner. Supplier will ensure that Personal Information is not physically transferred to, allowed access by or otherwise processed by its employees or personnel or its contractors, vendors, or suppliers in any country other than the United States unless agreed to in writing by Coke Florida. Upon Coke Florida's request, Supplier will enter into appropriate data transfer agreements with Coke Florida as needed to satisfy cross-border transfer obligations relating to Personal Information.

(n) **Compliance.** Supplier will take any other steps reasonably requested by Coke Florida to assist Coke Florida in complying with any notification, registration or other obligations applicable to Coke Florida under applicable laws, rules and regulations with respect to such party's processing of Personal Information under this Attachment. In the event that this Attachment, or any actions to be taken or contemplated to be taken in performance of this Attachment, do not or would not satisfy either party's obligations under such laws, the parties will negotiate in good faith upon an appropriate amendment to this Attachment.

(o) **Third-Party Beneficiaries.** The parties agree that Coke Florida's affiliated entities are intended third-party beneficiaries of this Attachment and that this Attachment is intended to inure to the benefit of such affiliates. Without limiting the foregoing, Coke Florida affiliates will be entitled to enforce this Attachment as if each was a signatory to this Attachment.

(p) **Survival.** The obligations of Supplier under this Attachment will continue for so long as Supplier continues to have access to, is in possession of or acquires Personal Information, even if all agreements between Supplier and Coke Florida have expired or been terminated.

(q) **Changes.** The requirements by either Coke Florida or Supplier relating to any changes of the written processing instructions or the actions will be subject to the Change Control Procedures agreed between the parties, unless the change does not impact Supplier's cost of providing or ability to provide the Services. If such a change requirement is generated by a modification in the Privacy Laws and is required for ongoing compliance with such Privacy Laws, then Coke Florida will have the right to require the implementation of the requested change even if the Change Control Procedures have not yet been followed through to completion. In such event, Coke Florida agrees to pay the reasonable fee charged by Supplier in consideration for the implemented change.

Attachment 5

Computer Incidence Response Team Process

Priority	Description of Event	Select Examples	Action Necessary
Priority Critical	Serious event that is adversely impacting to the image and reputation of Coke Florida and its trademarks Prevents Coke Florida from making a sale, or from meeting legal or contractual obligations	ERP servers attacked WWW site defaced and in media Information inadvertently displayed to the public (e.g., personal information disclosed, Coke Florida business information) Successful DDoS attack that impacts Coke Florida applications Virus or worm is rapidly spreading throughout the infrastructure and affecting communications	E-mail to Coke Florida Cyber Incident e-mail box (cyberincident@cocacolaflorida.com) immediately upon recognition of event.
Priority High	Event with a definite occurrence that adversely impacts Coke Florida if not addressed Affects non-critical applications	Network probes are discovered that have affected the productivity of multiple users Virus is rapidly spreading throughout the WAN but containment procedures are underway and the virus is not impacting Coke Florida applications	

Attachment 6

Disaster Recovery Plan

(To be provided by Supplier)

Attachment 7

Secure Coding Guidelines

1. INTRODUCTION

Coke Florida and Supplier agree to maximize the security of the software according to the following terms.

2. LIFECYCLE ACTIVITIES

(a) Implementation

Supplier agrees to provide and follow a set of secure coding guidelines and to use a set of common security control programming interfaces (such as the OWASP Enterprise Security API ("**ESAPI**")). Guidelines will indicate how code should be formatted, structured, and commented. Common security control programming interfaces will define how security controls must be called and how security controls will function. All security-relevant code will be thoroughly commented. Specific guidance on avoiding common security vulnerabilities will be included. Also, all code will be reviewed by at least one other supplier against the Security Requirements and coding guideline before it is considered ready for unit test.

(b) Security Analysis and Testing

Supplier will perform either Static or Dynamic application security analysis on all software builds prior to being provided to customer. All Critical and High vulnerabilities must be properly remediated prior to the build being provided to customer.

(c) Secure Deployment

Supplier agrees to provide secure configuration guidelines that fully describe all security relevant configuration options and their implications for the overall security of the software. The guideline will include a full description of dependencies on the supporting platform, including operating system, web server, and application server, and how they should be configured for security. The default configuration of the software will be secure.

3. SECURE CODING GUIDELINES

The Secure Coding Guidelines used by developer need to address the following.

(a) Input Validation and Encoding
(b) Authentication and Session Management
(c) Access Control
(d) Error Handling
(e) Logging
(f) Connections to External Systems
(g) Encryption
(h) Availability
(i) Secure Configuration
(j) Specific Vulnerabilities

4. PERSONNEL AND ORGANIZATION

(a) Security Architect

Supplier will assign responsibility for security to a single senior technical resource, to be known as the project Security Architect. The Security Architect will certify the security of each deliverable.

(b) Security Training

Supplier will be responsible for verifying that all members of the developer team have been trained in secure programming techniques.

(c) Trustworthy SUPPLIER

Supplier agrees to perform appropriate background investigation of all development team members.

5. DEVELOPMENT ENVIRONMENT

(a) Secure Coding

Supplier will disclose if requested what tools are used in the software development environment to encourage secure coding.

(b) Configuration Management

Supplier will use a source code control system that authenticates and logs the team member associated with all changes to the software baseline and all related configuration and build files.

(c) Distribution

Supplier will use a build process that reliably builds a complete distribution from source. This process will include a method for verifying the integrity of the software delivered to Coke Florida.

6. LIBRARIES, FRAMEWORKS, AND PRODUCTS

(a) Disclosure

Supplier will disclose if requested all third party software used in the software, including all libraries, frameworks, components, and other products, whether commercial, free, open-source, or closed-source.

(b) Evaluation

Supplier will make reasonable efforts to ensure that third party software meets all the terms of the Agreement and this Attachment and is as secure as custom developed code developed under the Agreement.

7. SECURITY REVIEWS

(a) Right to Review

Coke Florida has the right to have the software reviewed for security flaws at their expense at any time within sixty (60) days of delivery. Supplier agrees to provide reasonable support to the review team by providing source code and access to test environments.

(b) Review Coverage

Security reviews will cover all aspects of the software delivered, including custom code, components, products, and system configuration.

(c) Scope of Review

At a minimum, the review will cover all of the Security Requirements and should search for other common vulnerabilities. The review may include a combination of vulnerability scanning, penetration testing, static analysis of the source code, and expert code review.

(d) Issues Discovered

Security issues uncovered by Coke Florida will be reported to both Coke Florida and Supplier. All issues will be tracked and remediated as specified in the Security Issue Management section of this Attachment.

8. SECURITY ISSUE MANAGEMENT

(a) Identification

Supplier will track all security issues uncovered during the entire lifecycle, whether a requirements, design, implementation, testing, deployment, or operational issue. All critical and high vulnerabilities must be remediated before the application is provided to Coke Florida.

(b) Remediation

At a minimum all critical and high severity security issues that are identified before delivery will be fixed by Supplier. Security issues discovered after delivery will be handled in the same manner as other bugs and issues as specified in the Agreement.

9. ASSURANCE

(a) Assurance

Supplier will provide a "certification package" as requested consisting of the security documentation created throughout the development process. The package should establish that the Security Requirements, design, implementation, and test results were properly completed and all security issues were resolved appropriately.

(b) Self-Certification

The Security Architect will certify that the software meets the Security Requirements, all security activities have been performed, and all identified security issues have been documented and resolved. Any exceptions to the certification status will be fully documented with the delivery.

(c) No Malicious Code

Supplier warrants that the software will not contain any code that does not support a software requirement and weakens the security of the application, including computer viruses, worms, time bombs, back doors, Trojan horses, Easter eggs, and all other forms of malicious code.

10. SECURITY ACCEPTANCE AND MAINTENANCE

(a) Acceptance

The software will not be considered accepted until the certification package is complete and all security issues have been resolved.

(b) Investigating Security Issues

After acceptance, if security issues are discovered or reasonably suspected, Supplier will assist Coke Florida in performing an

investigation to determine the nature of the issue. The issue will be considered "novel" if it is not covered by the Security Requirements and is outside the reasonable scope of security testing.

(c) Other Security Issues

Supplier will use all commercially reasonable efforts consistent with sound software development practices, taking into account the severity of the risk, to resolve all security issues not considered novel as quickly as possible.

Attachment 8

Web Application Security Assessment

Coke Florida will use the proprietary Web Application Security Assessment ("**WASA**") methodology during the project. The WASA methodology includes the use of an automated security-scanning tool supported by manual hacking and enumeration procedures to detect and exploit vulnerabilities. WASA methodology consists of the three steps as follows:

Step I – Assess/Model Threats. Coke Florida starts its assessment by gathering information about the Web application and supporting infrastructure via discussions with application owners and custodians. The information gathered during this phase will be used to ensure that the following issues are addressed:

- All prerequisite information about the systems and networks is gathered to allow an Impact Analysis to be completed;
- Realistic threats which are relevant to the organization are defined and agreed upon with application owners or custodians;
- Appropriate tests targeting key mission critical applications, application modules or access methods are identified; and
- Limitations to the proposed security assessment are determined (e.g., DoS testing).

The threat agents, or "scenarios," PwC typically uses include the following categories:

- Uninformed outsider testing – Emulates attacks from individuals with no significant knowledge of the application; testing is performed without credentials to the application.
- Informed insider testing – Emulates attacks from employees or contractors with legitimate access to the application; testing is performed with credentials to the application.

Step II – Automated Testing. In this step, Coke Florida will utilize a variety of freeware and commercial security tools to scan each Web application for known vulnerabilities in a comprehensive and efficient manner. PwC will utilize top commercial Web application security scanning tools, as well as Coke Florida proprietary testing tools, through which Coke Florida will test the security of the Web applications from the vantage point of an unauthenticated user (anonymous Web user) and an authenticated user (user with valid credentials). Each scan will be performed twice, once without logging into the application followed by another scan as a valid user.

Step III – Advanced Manual Testing. Manual testing will be performed to identify security exposures and exploit findings discovered from automated vulnerability scanning. The Coke Florida testing team will leverage its years of manual Web application security testing experience and its understanding of weaknesses in common coding practices in an attempt to identify security weaknesses in the designated Web application. For each of the identified potential weaknesses, Coke Florida will manually attempt to exploit the vulnerability to verify that the application is susceptible to attack and to fully understand the impact of the weaknesses. Additionally, Coke Florida will attempt to understand whether multiple lower- or medium-risk vulnerabilities constitute a higher risk rated vulnerability when exploited together. This task accounts for approximately eighty percent (80%) of Coke Florida testing.

Coke Florida will assess each of the Web applications' susceptibility to a variety of attacks, including the Open Web Application Security Project ("**OWASP**") Top Ten security flaws:

- Invalidated Input
- Broken Access Control
- Broken Authentication and Session Management
- Cross Site Scripting (XSS) Flaws
- Buffer Overflows
- Injection Flaws
- Improper Error Handling
- Insecure Storage
- Denial of Service (pre-production applications)
- Insecure Configuration Management

Additionally, but not limited, Coke Florida will assess each application for the following:

- Access to sensitive data – Sensitive files such as the System backup files or configuration files containing passwords may be present on the Web server and accessible to unauthorized individuals (identified through manual methods);
- Administrative Access – Default or easily guessable passwords may be used to gain access to the administrative section of the System (identified through manual methods);
- Authentication – Obtain unauthorized access to data or functionality due to authentication weakness (identified through manual and automated methods);
- Backdoors – Identify malicious entry paths that provide administrative access into the application or system (identified through manual methods);
- Cookie poisoning – Change cookie data to access sensitive information or impersonate another user (identified through manual methods);
- Forceful browsing – Access a Web page or directory directly that should only be reached as an authenticated user (identified through manual and automated methods);
- Hidden field manipulation – Modify hidden field values to manipulate Web application functionality or access sensitive data (identified through manual methods);
- Informational – View unauthorized data, such as personally identifiable information of another user (identified through manual methods);
- Infrastructure/platform misconfigurations – Web servers may be inadvertently misconfigured to permit anonymous authoring through FrontPage Server Extensions, file transfers with WebDAV, directory indexing and browsing, etc. (identified through manual and automated methods);
- Input validation – Input unauthorized types or amounts of data to determine if the application responds erratically (identified through manual and automated methods);
- Known vulnerabilities – Identify known vulnerabilities present in the Web application (identified through manual and automated methods);
- Misconfigurations – Identify and exploit system configuration settings that provide excessive access to application configuration, data, or functionality (identified through manual methods);
- Parameter manipulation – Manipulate parameters by using special characters or "illegal" input such as SQL or JavaScript code to cause the Web application to behave in an unauthorized or inappropriate manner (identified through manual and automated methods);
- Session management – Compromise session management technology to hijack another session (identified through manual and automated methods);
- SQL injection – Insert SQL code into form fields to bypass authentication or execute SQL statements directly on the database (identified through manual and automated methods);
- Stealth commanding – Insert code in form fields to take control of an application or its host operating system (identified through manual and automated methods); and
- Third-party misconfigurations – Exploit configuration errors in third party applications such as database servers (identified through manual and automated methods).

Attachment 9

Terms and Conditions of Service for Single Sign-On Capability

The following Terms and Conditions of Service for Single Sign-On Capability govern Coke Florida's use of the Single Sign-On Capability function of the Services. These Terms and Conditions are in addition to those Terms and Conditions of Service contained in the Agreement.

Service Single Sign-on Capability ("**SSO Capability**") will permit Coke Florida's Users to sign on to Service from either Coke Florida's website, or the website of a third-party provider acceptable to Supplier ("**Third-Party Website Provider**"). In connection with using SSO Capability, Coke Florida agrees as follows:

(i) All SSO Capability will conform to the Supplier silent log-in requirements, which will be provided to Coke Florida in writing by Supplier, and which may be amended from time to time by Supplier. Supplier will provide Coke Florida with sufficient prior written notice of any amendments to the silent log-in requirements to enable Coke Florida to timely comply with any such amendments. Any computer or other access device used in connection with SSO Capability is hereby defined as an "**SSO Capability Device.**"

(ii) Coke Florida will be solely responsible for providing Supplier proper authentication protocols as set forth in the silent log-in requirements, including user IDs, passwords and other access codes (collectively, "**Authentication Protocols**") used as means to authenticate the identity of Participants on SSO Capability Devices and for transmitting such Authentication Protocols to Supplier to provide Participants SSO Capability. Coke Florida will be solely responsible for the security of the SSO Capability Devices, other computers, networks and systems of Coke Florida. Supplier will not be liable or responsible in any way to Coke Florida, Participants, or others for any losses, damages, claims, costs, expenses or other obligations incurred by Coke Florida, Participants or others as a result of being provided improper Authentication Protocols, the improper transmission of Authentication Protocols to Service, or the security of the SSO Capability Devices and computers, networks and systems of Coke Florida.

(iii) Any and all form of interaction by electronic means on Service via any SSO Capability Device ("**Instruction**") will be conclusive, final and binding, and Coke Florida will be responsible for all Instructions. Coke Florida represents and warrants that each Instruction is and will be: (a) in compliance with this Attachment, the Agreement and applicable law; and (b) conducted in accordance with Coke Florida's applicable internal, policies or procedures. Coke Florida agrees to notify Supplier immediately if Coke Florida becomes aware of any compromise of any SSO Capability Device or Authentication Protocols that could lead to non-authorized Instructions.

(iv) Supplier may from time to time (but is under no obligation to) distribute new versions or updates to SSO Capability. If any new versions and/or updates are made available, Coke Florida is responsible for using such new versions and/or updates and ensuring that Coke Florida is using the most current version available.

(v) Coke Florida will, or will cause Third-Party Website Provider to, operate and maintain their Participant directory and log-in process in accordance with industry best practices to ensure the integrity and security of the Participant directory and log-in process. Supplier will have no responsibility for Coke Florida's or the Third-Party Website Provider's operation and maintenance of the Participant directory and login process.

(vi) Coke Florida agrees that the SAML Assertion to be used by Coke Florida or the Third-Party Website Provider will be signed using a signing certificate that has been issued from a public key infrastructure ("**PKI**") mutually agreed upon by Coke Florida and Supplier. Coke Florida or the Third-Party Website Provider may use a PKI of a trusted third-party such as VeriSign or CyberTrust or, if Coke Florida provides appropriate documentation acceptable to Supplier, an internally-built PKI. The PKI will be protected in a hardware device known as an HSM. The HSM must be a FIPS 140-2 Level 3 device. Security Assertion Markup Language ("**SAML**") is an XML standard for exchanging authentication and authorization data between security domains as defined by the Organization for the Advancement of Structured Information Standards. SAML Assertion is the actual passing of a Participant's unique identifying information between Coke Florida or the Third-Party Website Provider and Supplier using SAML.