Security and Compliance Standard for Outsourced Third Party Service Providers

The purpose of this standard is to provide technical, organizational, operational, and security measures relevant to the protection and handling of Personal Data and Customer Confidential Information in the possession of outsourced Service Providers.

Date Created: February 9, 2015		Created by: Security Dept
Version No: 1.0	Reviewed: 3-14-15	Last Reviewed by: Vendor Mgmt Team

Table of Contents

NGA will, and will require its third party service providers to, comply with the standards set forth in this document (collectively, the "Standard").

1. Information Risk Management

1.1. Maintain appropriate organizational, technical, and physical measures and controls to protect and ensure the security and confidentiality of Personal Data and Customer Confidential Information

1.2. Maintain formal written policies and procedures for the administration of information security throughout the organization consistent with the requirements of this standard.

2. User Awareness

2.1. Check and verify the identity and right to work of all personnel before allowing access to Personal Data and Customer Confidential Information systems in accordance with local laws applicable to the countries in which they operate.

2.2. Personnel with access to Personal Data and Customer Confidential Information must participate in appropriate information security awareness training provided by the Service Provider and thereafter on at least an annual basis.

2.3. Personnel must comply with all information security controls and processes documented in this Standard.

2.4. Personnel must bring all situations of security exposures, misuse or non-compliance to management's or Security's attention.

3. Incident and Change Management

3.1. Maintain an incident management plan designed to promptly identify, prevent, investigate, and mitigate any Security Incidents and perform any required recovery actions to remedy the impact.

3.2. Security Incidents must be logged, reviewed on a periodic basis, and maintained for a minimum of twelve (12) months.

3.3. Maintain documented change management procedures that provide a consistent approach for controlling, implementing and documenting changes (including emergency changes).

3.4. Production changes must be approved by the appropriate system owner.

3.5. Apply procedures and measures to regularly update and patch computer programs to eliminate vulnerabilities and remove flaws that could otherwise facilitate security breaches.

4. User Access

4.1. Ensure each account is attributable to a single individual with a unique ID (not shared) and each account must require authentication (e.g., password).

4.2. Ensure user access to systems that contain or process Personal Data and Customer Confidential Information are reviewed and approved at least quarterly (Every 3 months).

4.3. Undertake reasonable measures to terminate access, whether physical or logical, no later than the date of personnel separation or personnel transfer to a role for which access is no longer required.

4.4. Use strong passwords consistent with technology industry practices, including minimum password length, lockout, expiration period, complexity, encryption, changing of default passwords, and usage of temporary passwords.

4.5. Service Provider must process and access Personal Data and Customer Confidential Information only on a need-to-know basis and only to the extent necessary to perform services.

5. Data Protection

5.1. Encrypt or protect by other technical means Personal Data and Customer Confidential Information so that it cannot be read, copied, changed or deleted by unauthorized persons when saved on mobile devices (e.g., laptops) or removable media.

5.2. Encrypt and protect Personal Data and Customer Confidential Information so that it cannot be read, copied, changed or deleted by unauthorized persons during transmission or transit outside of Service Provider's internal network.

5.3. Personal Data and Customer Confidential Information shall not be processed on personal accounts (e.g., individual email or cloud services accounts (e.g., Gmail, Yahoo, Dropbox, Google Drive)) or on personally-owned computers, devices or media.

5.4. Maintain hardening and configuration requirements consistent with industry practices.

5.5. Use industry best practices to implement and maintain appropriate security measures and procedures designed to provide antivirus and spyware software protection to systems that handle or hold Personal Data and Customer Confidential Information.

5.6. Maintain inventories that list all critical Service Provider Information Systems

5.7. Workstations must not be left authenticated when unattended and must be password or PIN protected when not in use. An inactivity lock must be implemented on workstations.

5.8. Comply with all applicable data privacy regulations.

6. Physical Security

6.1. Physically secure perimeters and external entry points against unauthorized access.

6.2. Visitors must be required to sign a visitors register (maintained for at least one year) and be escorted or observed at all times.

6.3. A clear desk policy must be enforced throughout the facility. Documents that contain Personal Data and Customer Confidential Information must be kept secured (e.g. locked office or file cabinet) when not in use.

6.4. Servers and/or network equipment used to store or access Personal Data and Customer Confidential Information must be kept in a secure room containing additional access control mechanisms.

6.5. Servers and/or network equipment used to provide services must incorporate controls to mitigate the risk of power failure and environmental conditions.

6.6. Physical access must be monitored, recorded and controlled with physical access rights reviewed at minimum annually.

7. Compliance Standards and Assurance

7.1. Service Provider will conduct its own SOC1 (SSAE16/ISAE3402) and/or SOC2 Audit (as applicable) and provide NGA an annual copy thereof.

- In the event a SOC1 or SOC2 is not in place, Service Provider will operate against a generally accepted standard of operational and general IT security controls and evidence of their regular execution will be retained and provided upon reasonable request.

7.2. Any locally applicable external auditing standards or certifications will be presented to represent validation of Service Provider standards and controls.

7.3. Service Provider will have processes, policies and controls around Quality, Security and Business Continuity/Disaster Recovery which are substantially aligned with or have achieved recognized standards such as ISO 9001:2008 (Quality), ISO 27001:2005 (Security) and ISO 22301 (Business Continuity and Disaster Recovery Plan) in accordance with its industry's best practices and legislative requirements and will provide evidence of such processes, policies and controls or compliance with the standards, as applicable, upon request.

7.4. Service Provider will submit to periodic monitoring against NGA's standard control framework and rotational audits as required.

7.5. Service Provider must maintain a list of all sub-contractors handling Personal Data and Customer Confidential Information and ensure they are in compliance with this standard.