NuCompass MOBILITY

Data Protection Policy

Technical and Organizational Security Measures

NuCompass Mobility undertakes appropriate and commercially reasonable technical and organizational measures to protect against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. The measures take into account available technology, the cost of implementing the specific measures, and the level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected. NuCompass Mobility implements and maintains a commercially reasonable effective information security program to protect Client Data and Personal Information. The program includes appropriate administrative, technical, and physical safeguards.

I. AN INFORMATION/DATA SECURITY PROGRAM

A. NuCompass Mobility maintains a commercially reasonable comprehensive data security program which includes reasonable and appropriate technical, organizational, administrative, physical, and other security measures against the destruction, loss, unauthorized access, to or alteration of Personal Information, Client Data, and Client Confidential Information in the possession of NuCompass Mobility.

B. NuCompass Mobility takes responsibility for ensuring that any Material Subcontractors that NuCompass Mobility supplies Personal Information in order to perform Mobility Services authorized under the Agreement, maintain data security programs for the protection of such Personal Information which are at least as stringent as NuCompass Mobility's own program and in accord with generally accepted industry standards and practices.

II. AN INFORMATION/DATA SECURITY POLICY

A. NuCompass Mobility provides training to its employees regarding NuCompass Mobility's Polices. NuCompass Mobility's Policies include control architecture, encryption and data separation procedures, access control and verification, the presence or absence of audit trails, system testing and monitoring, disaster recovery and back-up, program responsibility, and data breach incident response procedures.

B. Subject to NuCompass agreements with Client. Clients have the right to review such documentation and/or inspect NuCompass Mobility's compliance with such program.

III, MATERIAL SUBCONTRACTORS AND PERSONAL INFORMATION

A. NuCompass Mobility maintains a risk management program focused on the identification, evaluation, and validation of a Material Subcontractor's privacy, security, and business continuity controls. The program is based on NuCompass Mobility's standards for Personal Information and focused on ensuring that the Material Subcontractor utilizes appropriate controls as applicable to the services delivered.

B. NuCompass Mobility excludes from its risk management program Material Subcontractors who are subject to Federal information security and data breach notification laws including, but not limited to, the Gramm-Leach-Bliley Act.

IV. ASSET MANAGEMENT

A. **Acceptable Use**. NuCompass Mobility maintains rules for the acceptable use of information and assets which are no less restrictive than generally accepted business practice.

B. **Portable Media and Devices.** NuCompass Mobility's Policies prohibit employees from storing Personal Information on portable devices and media unless required to perform the Mobility Services. When necessary for Mobility Services, NuCompass Mobility's employees may store Personal Information on laptops, USB drives, floppy disks, and CDs, as long as Personal Information is encrypted using a cryptographic algorithm. In addition, laptops shall full-disk encryption.

C. **Inventory Management**. NuCompass Mobility maintains an inventory program and performs monitoring to control the installation, ownership and movement of hardware, software and

communications equipment. All assets that contain or that have previously contained Personal Information or Client Confidential Information are triple wiped before they are retired and sent offsite.

D. **Personally-owned Equipment**. NuCompass Mobility's Policies restricts employee's storage of Client Confidential Information on personally-owned equipment.

V. SECURITY AWARENESS PROGRAM/TRAINING

A. NuCompass Mobility maintains an employee awareness program with respect to NuCompass Mobility's Policies. New and existing personnel receive mandatory training at least annually regarding the appropriate protection of Client Data, including Personal Information.

VI. PHYSICAL AND ENVIRONMENTAL SECURITY

A. **Secure Areas**. NuCompass Mobility provides appropriate security controls for all entry points, holding areas, telecommunications areas, and cabling areas that contain information processing systems or media containing Client Confidential Information and Personal Information including the following:

i) Access is controlled and restricted by use of a defined security perimeter, appropriate security barriers, entry controls and authentication controls. Access logs are maintained for up to one (1) year.

ii) All personnel (i.e. employees, contractors, visitors, et cetera) who will have access to NuCompass Mobility's offices, facilities or data center(s) are required to wear some form of visible identification to identify them as employees, contractors, visitors, et cetera.

iii) NuCompass Mobility maintains an industry standard clean desk policy.

iv) Visitors are escorted at all times.

B. **Environmental Security**. NuCompass Mobility protects equipment from power failures and other disruptions caused by failures in supporting utilities, according to generally accepted security practices.

VII. COMMUNICATIONS AND OPERATIONS MANAGEMENT

A. **Protections Against Malicious Code.** NuCompass Mobility maintains detection, prevention, and recovery controls to protect against malicious software, which is no less rigorous than generally accepted security practices. NuCompass Mobility trains appropriate employees regarding prevention and detection of malicious software.

B. **Back-ups.** NuCompass Mobility performs appropriate back-ups of its information processing systems to perform the Mobility Services under the Grandfather/Father/Son schema allowing for recovery from daily/weekly/monthly and yearly back-ups.

C. **Exchange of Information.** To protect confidentiality and integrity of Personal Information in transit, NuCompass Mobility maintains a policy designed to transmit Personal Information in a secure manner over the Internet or in another electronic form. NuCompass Mobility educates employees regarding this policy and available encryption tools.

D. **Monitoring.** To protect against unauthorized access or misuse of NuCompass Mobility's information processing systems, NuCompass Mobility does the following:

i) Employs generally accepted security practices, security controls and tools to monitor information processing systems and log user activities, exceptions, unauthorized information processing activities and suspicious activities. NuCompass Mobility facilities/data centers are protected against unauthorized access as prescribed by NuCompass Mobility's security policies. User logs are kept for at least one (1) year.

ii) Performs frequent reviews of logs and take necessary actions to protect against unauthorized access or misuse.

iii) NuCompass Mobility will, at a Client's reasonable request, make applicable portions of logs available to the authorities to assist in investigations; provided however, that Client shall not be granted access to any information in such logs that includes data about other NuCompass Mobility clients or other NuCompass Mobility Confidential Information.

iv) Maintains the clocks of all relevant information processing systems synchronized using a national or international time source.

E. **Signature Upon Receipt**. NuCompass Mobility ensures that hardcopy documents or portable media containing Personal Information are transmitted via a secure delivery method that requires signature upon receipt.

VIII. ACCESS CONTROL

A. **Unauthorized Access.** To protect against unauthorized access or misuse of NuCompass Mobility information processing systems, NuCompass Mobility does the following:

i) Employs a formal procedure for granting and revoking access and access rights to all NuCompass Mobility information processing systems.

ii) Follows a "separation of duties" standard and maintains a formal approval process and audit trail for all access requests.

iii) Employs a formal password management process.

iv) Reviews users' access rights to confirm that they are appropriate for the users' role.

v) Maintains security practices regarding selection and use of strong passwords.

vi) Employs idle-lock for unattended equipment to prohibit access and use by unauthorized individuals.

vii) Controls access to operating systems through a secure log-on procedure.

viii) Provides information processing system users with a unique identifier (user ID).

ix) Tightly restricts and controls the use of utility programs that are capable of overriding system and application controls.

x) Closes inactive application sessions, when technically possible, after a defined period of inactivity.

B. **Network Access Control**. Access to internal, external, and public network services that allow access to NuCompass Mobility information processing systems include:

i) Generally accepted security practice standard authentication mechanisms for network users and equipment are in place and updated as necessary.

ii) Electronic perimeter controls that protect NuCompass Mobility information processing systems from unauthorized access.

iii) Authentication methods to control access by remote users.

iv) Physical and logical access control for diagnostic and configuration ports.

C. **Mobile Computing and Remote Working**. To protect NuCompass Mobility information processing systems from the risks inherent in mobile computing and remote working, NuCompass Mobility maintains commercially reasonable policies, operational plans and procedures for managing mobile computing and remote working and provide those upon reasonable request to Client.

D. **User ID**. NuCompass Mobility assigns a unique identifier (User ID) to all users accessing its information processing systems. Employees are prohibited from using "generic" User ID's to access NuCompass Mobility systems.

E. **Password Controls**. NuCompass Mobility employs a variety of password controls including minimum length, two-factor authentication, alpha/numeric characters, lockouts, expirations, stored encrypted, or password reuse. Password controls are included in all NuCompass Mobility information systems that contain Personal Information.

F. **Remote Access**. Remote access includes: two-factor authentication and network intrusion detection on the remote access network segment.

G. **Confidentiality Agreements.** New employees sign a confidentiality agreement within the first 30 days of hire and prior to handling Personal Information.

H. **Background Checks**. NuCompass Mobility conducts background checks for NuCompass Mobility employees prior to hire.

I. **Removal of Access Rights**. The access rights of NuCompass Mobility employees and Subcontractors to NuCompass Mobility and/or Client information processing systems are removed within twenty-four hours upon termination of their employment, contract or agreement, or adjusted upon change in duties.

J. **No Personal Information Storage**. NuCompass Mobility's Policies strictly regulates employees' storage of Personal Information on laptops or desktops.

K. NuCompass Mobility restricts access to Client Data and Personal Information to those employees that require such information to perform Mobility Services.

L. NuCompass Mobility grants employees minimum access rights and privileges needed to perform a particular function or transaction. This includes limiting administrative rights to laptops and desktops to technology support personnel. User access reviews are conducted at least semi-annually and access is updated as necessary.

IX. INFORMATION SYSTEMS MAINTENANCE

A. NuCompass Mobility maintains change control procedures to ensure that modifications to the production environment (e.g. application, operating system, and hardware level changes) protect the integrity, confidentiality, availability and security of NuCompass Mobility information systems. Documented procedures are maintained for granting emergency access or introducing unscheduled changes to the production environment. These procedures also include activity monitoring and subsequent removal of access. Logs that document this access are maintained. A separation of duties exists to ensure that changes are recorded and properly authorized (e.g. developers can not directly update programs, job control parameters, or other components of the production environment).

X. INCIDENT MANAGEMENT

A. NuCompass Mobility will promptly notify Clients upon learning of unauthorized access or disclosure of Personal Information in which NuCompass Mobility has a commercially reasonable belief that the confidentiality or security of Personal Information has been compromised ("Security Incident"). Thereafter NuCompass Mobility will:

i) Promptly furnish to Client details of the Security Incident and reasonably investigate such Security Incident;

ii) Reasonably cooperate with Client in litigation related to a Security Incident; and

iii) Promptly take reasonable appropriate measures to prevent a recurrence of the Security Incident.

B. **Security Assessments Following Information Security Events and Security Breaches**. Following the occurrence of a Security Incident, NuCompass Mobility will permit Clients to perform a logical security assessment of NuCompass Mobility's systems, data processing and business facilities to assess the impact of the event or breach.

XI. DATA BREACH LAWS

A. NuCompass Mobility will notify Clients within twenty-four hours of any breach of the security of Personal Information, in which NuCompass Mobility has actual knowledge that the Personal Information has been compromised or in which NuCompass Mobility has a reasonable belief that the confidentiality of Personal Information has been compromised, and will reasonably cooperate with Clients in any post-breach investigation as well as provide reasonable information regarding its remediation efforts. In addition, NuCompass Mobility will reasonably assist Clients to comply with state data breach notification laws following a breach of security affecting Personal Information. At all times, NuCompass Mobility shall cooperate with Clients to effect the breach response process required by applicable law. Clients shall solely direct and control the breach response process required by applicable law.

B. For purposes of the following paragraph, "Personal Information" shall have the same meaning as "personal information" under California Civil Code § 1798.29. Data breach shall mean the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information. To the extent any unauthorized disclosure of or access to Personal Information is attributable to a data breach by NuCompass Mobility (or any Material Subcontractor) of any provision or obligation under this Data Protection Policy Schedule, NuCompass Mobility shall bear the costs of providing notice to affected individuals, providing affected individuals with credit monitoring (subject to mutual agreement between NuCompass Mobility and Client), and such other remedies required by applicable law.

XII. SECURITY ASSESSMENTS/TESTS

A. **Initial and Recurring Security Assessments**. NuCompass Mobility will permit approved Client representatives (at Client's expense) to perform an on-site physical and logical security assessment of NuCompass Mobility's data processing and business facilities prior to commencing Mobility Services and each year thereafter, with NuCompass Mobility assessing no charge/service fee to Client for doing so. Security assessments will be performed at a date and time agreed to by both parties; scope of all online assessment activities will be defined and agreed to by both parties prior to the start of the assessment.

B. **Security Assessment Findings**. Upon completion of a security assessment, the Client will provide NuCompass Mobility with a security assessment completion letter that summarizes Client's security assessment findings. These findings may identify one or more security deficiencies. The parties will mutually agree upon the set of issues that require remediation, corresponding solutions and target remediation dates. If mutual agreement cannot be reached, then these issues may be escalated using the dispute resolution provisions within the Client/NuCompass Mobility Agreement. NuCompass Mobility shall bear the full cost of any mitigation activity that addresses a finding of the security assessment.

XIII. DATA MASKING

A. **Masking**. Personal Information stored or used outside of production environments has been disguised so that it cannot be associated with an actual individual. The extract and transformation of Personal Information is done within a production environment before it is transmitted to a non-production environment.

B. **Applicability**. This section details the technology security requirements for masking Personal Information. NuCompass Mobility applies these procedures to:

i) All activities performed within NuCompass Mobility's non-production environments that use Personal Information.

ii) Temporary employees, contractors, consultants, NuCompass Mobility's external business alliances, or anyone using Personal Information.

iii) At Client's request, NuCompass Mobility will provide information affirming that its data masking efforts meet the requirements.

C. **When to Mask Data**. NuCompass Mobility masks Personal Information if the data is moved outside of the production environment (such as quality control, test and development environments). If a business need exists to use Personal Information for non-production activities then NuCompass Mobility will obtain written permission from the Client. If the Client believes data elements (other than those listed in subsection D below) need to be masked based on the nature of such data, the parties shall agree to any changes through the Change Order process. Masking may be accomplished as follows:

i) Appropriately masked data may be provided by the Client, or

ii) NuCompass Mobility may develop its own tools to mask Client Data as long as the masking meets or exceeds the specifications contained below.

D. **Masking Requirements**

i) Social Security Numbers, Social Insurance Numbers, and other identification numbers issued by governmental entities.

ii) Names (includes any name field).

(1) The first and last names must be changed to a name or character strings other than those that appear in the record.

(2) The names may not be switched with other Client member names.

(3) Blanking out the name is acceptable.

iii) Addresses (includes any address field, property location, garage location, et cetera).

(1) The street number must be changed to a number or character string other than the number that appears in the record.

(2) It is acceptable to have all addresses in a test data set changed to a single address, such as 100 Main Street.

(3) The addresses may not be switched with other Client member addresses.

(4) Blanking out the number or entire address is acceptable.

iv) Email address (includes any email address field).

(1) The email address must be changed to a character string other than the email address that appears in the record.

(2) The email address may not be switched with other Client member email addresses.

(3) It is acceptable to have all email addresses in a test data set changed to the same email address.

(4) Blanking out the email address is acceptable.

v) Phone number (includes any phone number field including home phone, personal phone, business phone, et cetera).

(1) The phone number must be changed to the correct area code followed by 555 and four random numbers (or other similar masking procedure).

(2) It is acceptable to have all phone numbers in a test data set changed to the same phone number.

(3) Blanking out the phone number is acceptable.

vi) Date of birth.

(1) Add or subtract a random number of days, months, years within the testing limits.

(2) It is acceptable to have all dates of birth in a test data set changed to the same date of birth.

(3) Blanking out the date of birth is acceptable.

E. **Exclusions to Data Masking Requirements to Solve Production Problems**. Data masking is not required for non-production activities, such as emergency testing, when such activities are necessary to solve a critical production problem (e.g. if production cycles or processes are stopped or significantly impaired).

F. **Disposing of Masked Data.** NuCompass Mobility will remove masked records and excluded production data from non-production environments as soon as the non-production activities are complete. Clients consider non-production activities to be complete when the production data is no longer required to resume activity or produce documentation.

XIV. TRANSFER AND STORAGE OF CLIENT DATA

A. **Prior** Written Approval. NuCompass Mobility will relocate Mobility Services offshore, in another country, only with prior written approval from Clients.