INFORMATION PROTECTION REQUIREMENTS ("Requirements")

1. SCOPE. These Requirements apply to all third parties who are providing goods and/or services ("**Company**") to Motorola Mobility LLC and its Affiliates (defined below) (collectively, "**Motorola**") and Company's performance of its obligations under all agreements with Motorola ("**Agreements**") with respect to Motorola's Confidential Information, Confidential Restricted Information, Personal Information, and Proprietary Information (each defined below). In the event of an inconsistency or conflict between these Requirements and the terms in the applicable Agreement, these Requirements will control, but only to the extent of such inconsistency or conflict.

2. DEFINITIONS.

2.1 "**Affiliate**" means any person or entity that directly or indirectly controls or is controlled by a party, or with which a party shares common control. A party "controls" another entity when the party, through ownership of the voting stock or other ownership interest of that entity, or by contract or otherwise, has the ability to direct its management.

2.2 "**Confidential Information**" is confidential or proprietary data, materials or information Motorola provides to Company: (i) in written or any other visually perceptible or tangible form, which is clearly designated as "confidential" or "proprietary" at the time of disclosure and (ii) in oral form, if it is identified as confidential at the time of disclosure. Confidential Information includes the existence and terms of any Agreements.

2.2.1 **"Confidential Restricted Information"** is Confidential Information disclosed under heightened security restrictions, without regard to designation or written confirmation as "confidential," "proprietary" or similar designation. Confidential Restricted Information includes, but is not limited to marketing and sales plans, customer lists, unpublished Motorola financial information, and trade secrets.

2.2.1.1 **"Personal Information"** is Confidential Restricted Information consisting of any information collected from or about one or more individuals who may include, but are not limited to, Motorola employees, their family members, job applicants, customers, consumers, contacts, suppliers, and partners or potential partners. Personal Information is either "General Personal Information" or "Sensitive Personal Information":

"General Personal Information" includes, without limitation, names, partial dates of birth, home and business addresses, home and business email addresses, home, mobile and business telephone numbers, employee ID numbers, photographs, and mobile device user data that is linked to an unique identifier such as the IMEI or MEID of an individual's mobile device.

"Sensitive Personal Information" includes, without limitation, racial or ethnic origin, religious or philosophical beliefs, political affiliations/opinions, trade union membership, medical or health-related records, sexual orientation, gender identity, disabilities, background checks, U.S. Social Security Numbers (SSNs) and similar government/national identification numbers (including tax identification numbers), Credit/Debit Card numbers and similar bank/financial account information, passwords and other authentication and authorization credentials, biometric identifiers, geolocation information, an individual's web browsing history, the history of applications installed and used on an individually identifiable mobile device, and complete dates of birth (year+month+day).

2.2.1.2 **"Proprietary Information"** is Confidential Restricted Information disclosed under the highest security restrictions, without regard to designation or written confirmation as

"confidential," "proprietary" or similar designation and includes prototype products and their associated documentation. Proprietary Information includes but is not limited to prototypes of unreleased products and their associated documentation and specifications.

2.3 "**Covered Information**" is Confidential Information, Confidential Restricted Information, Personal Information, and Proprietary Information collectively.

3. ACCESS COVERED INFORMATION. Company may collect, store, access, record, adapt, alter, use, process, maintain, disclose and dispose of (collectively, "**Access**") Covered Information only to fulfill Company's obligations under an Agreement, as otherwise expressly permitted under an Agreement, or pursuant to Motorola's written instructions and for no other purpose (the "**Purpose**").

4. SAFEGUARDS. Company will maintain a comprehensive and documented program consisting of administrative, physical, and technical safeguards (collectively, "**Safeguards**") that: (i) are designed to address any reasonably foreseeable threats to the confidentiality and security of Covered Information; (ii) protect such information from any unauthorized Access, data errors, loss of Access, or service disruption; (iii) limit the Access to such information in accordance with Section 5 below; and (iv) are appropriate to Company's role, operations and exposure to Covered Information.

4.1 To the extent that Company will Access Personal Information in order to fulfill its obligations under an Agreement, Company's Safeguards will also be designed to ensure that Company's Access to Personal Information complies with: (i) all applicable laws, rules, regulations, orders and ordinances; (ii) any relevant industry standards that are applicable to Company in its performance of its obligations under a Agreement; and (iii) an appropriate privacy policy maintained by Company and covering its performance of its obligations under the appropriate Agreement that will be adequate to comply with the foregoing legal obligations and industry standards.

In addition, Company may not otherwise use or modify the Personal Information, merge it with other data, commercially exploit it, use it for unauthorized marketing or advertising purposes, disclose it, transfer it across international borders or do any other thing that may in any manner adversely affect the integrity, security or confidentiality of such Personal Information, other than as expressly specified herein or as directed by Lenovo in writing.

4.2 Motorola will take reasonable steps to ensure that Company will only receive Personal Information if Company needs to Access Personal Information to perform its obligations under a Agreement. If Company inadvertently receives Personal Information then Section 4.1 above will not apply. Instead, Company's Safeguards will also include a process for notifying Motorola of the inadvertent disclosure of Personal Information and for promptly returning or destroying all copies of Personal Information that Company received from Motorola.

4.3 To the extent that Company will process, control or otherwise have access to any credit/debit card numbers and similar bank/financial account information of Motorola customers, consumers, employees, contacts or others, Company meets the requirements of the most current version of the Payment Card Industry's Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.

4.4 Company will not transfer any Motorola Personal Information across the borders of one country to another country without express approval from Motorola.

5. COMPANY'S MINIMUM SAFEGUARDS. Company's Safeguards will include, at minimum, the

following specific controls:

5.1 **Periodic Risk Assessment.** Company will implement and maintain, throughout the term of the applicable Agreement, a risk assessment program, which will include: (i) periodic assessment of Covered Information to identify risks of unauthorized Access; (ii) adoption of reasonable controls, procedures and training to address reasonably foreseeable risks; and (iii) evaluation and possible adjustment of Company's risk assessment program in the event of (A) an Incident (defined in Section 8.2 below), (B) changes in circumstances that reasonably implicate the security or confidentiality of such information, or (C) notification by Motorola of a reasonably foreseeable risk that Motorola believes needs to be addressed.

5.1.1 **Risk Assessment of Personal Information**. To the extent that Company Accesses Personal Information, Company will also periodically assess the adequacy of the Safeguards it has implemented under Section 4.1 above in addition to the other requirements of Section 5.

5.2 **Supervision and Training.** Company will provide the required level of training of, and supervision over, relevant employees, individuals in its Supply Chain (defined below), Permitted Recipients (defined below) and individuals in a Controlled Group (defined below), to ensure appropriate implementation of and compliance with Safeguards applicable to Covered Information.

5.3 **Access Control.** Company will limit Access to Covered Information to Company's employees, individuals in its Supply Chain, Permitted Recipients, and individuals in a Controlled Group, as set forth herein and who: (i) have a need to Access such information in order to perform Company's obligations under an applicable Agreement; (ii) have been properly background checked/screened; (iii) have completed Company's training and any other training prepared by Motorola on the required Safeguards; and (iv) if Company will Access Confidential Restricted Information, have agreed in writing to be bound by an Agreement that requires compliance with Company's Safeguards. Notwithstanding the foregoing, Company will only grant Access to Confidential Restricted Information to its employees who need to access such information in order to complete a specific Motorola-approved product requirement ("**Permitted Recipients**") at a specific Company site location as approved by Motorola in writing ("**Site**").

5.3.1 Company will only grant Access to Proprietary Information to Company employees who have been approved by Motorola as individuals permitted to Access Proprietary Information (the "**Controlled Group**") so Company can fulfill the Purpose. The Controlled Group will include only those individuals who need to Access Proprietary Information and will not include their managers or other employees of Company who do not need to Access Proprietary Information. These requirements take the place of the requirement to identify Permitted Recipients.

5.3.2 **Access Control Lists.** Company will maintain a written list, by Covered Information Accessed, of: (i) all employees and Company's suppliers, service providers, and subcontractors (collectively, its "**Supply Chain**") to whom Company has granted Access to Personal Information; (ii) all Permitted Recipients to whom Company has granted Access to Confidential Restricted Information; and (iii) all individuals in the Controlled Group to whom Company has granted Access to Proprietary Information, at any time during the term of the applicable Agreement. Company will update and maintain the accuracy of such lists, in a format approved by Motorola, at all times during such term, and after expiration or termination of an Agreement if Company has continuing access to or possession, custody or control of Confidential Restricted Information, and will provide copies of said lists to Motorola promptly upon request.

5.4 **Transmission Across Networks**. Company will only transmit Covered Information to Company's employees, individuals in its Supply Chain, Permitted Recipients, and individuals in a Controlled Group as applicable using secured, access controlled business networks. Company will not use personal email addresses, public email systems, public or free file exchanges, or public or free web sites to exchange Covered Information.

5.5 **Encryption.**

5.5.1 **Portable Devices.** Company will encrypt all Covered Information stored, transmitted, or received on portable devices or media, including but not limited to laptop computers, servers, mobile devices, hard drives, disks, backup tapes or other such electronic storage media, (collectively "**Portable Devices**") using, at a minimum, an industry standard and community-vetted encryption implementation. Company will encrypt all Confidential Restricted Information stored, transmitted, or received on Portable Devices using only the latest available encryption methods, with certificates, or other encryption methods specifically prescribed by Motorola. Such Portable Devices will be password protected and have active and operational antivirus protection where available. Notwithstanding the foregoing, Confidential Restricted Information in the form of source code will be located on a single, dedicated, designated secure server that will be used for all development activities relating to such source code. Company will ensure that such source code is available only to the applicable Permitted Recipients or applicable individuals in a Controlled Group, through such specially secured system servers used solely for such source code access. Company will not be required to encrypt Covered Information on such Portable Devices where encryption is not technically feasible as agreed by the parties. In that event, Company will take reasonable and appropriate steps to secure Covered Information stored on its Portable Devices including but not limited to restricting the amount of Covered Information stored; setting timeout values; using secure passwords passphrases or PINs, automatically erasing a Portable Device after a specified number of invalid login attempts, and configuring its Portable Devices with remote wipe capabilities. If Company will be storing Confidential Restricted Information on Portable Devices where encryption is not technically feasible, Company will obtain Motorola's express written approval for prior to storing said information on unencrypted Portable Devices.

5.5.2 **Transport.** Except as otherwise provided in Section 5.5.1 above, Company will encrypt all Covered Information stored on any physical or logical media, before that media is stored or transported outside of Motorola's or Company's physically secured facilities, using an industry standard and community-vetted encryption implementation. Except as otherwise provided in Section 5.5.1 above, Company will encrypt all Confidential Restricted Information stored on any physical or logical media, before that media is stored or transported outside of Motorola's or Company's physically secured facilities, using only the latest available encryption methods, with certificates, or other encryption methods specifically prescribed by Motorola.

5.5.3 **Transmission**. Company will encrypt all transmissions of Confidential Restricted Information across all networks not operated or used exclusively by Company using an industry-standard and community-vetted encryption implementation

5.5.4 **Exclusions**. Notwithstanding the other provisions in this Section 5.5, Company will not be required to encrypt hard copy documents containing Covered Information, or to encrypt such information where prohibited by an applicable law, but will take appropriate steps to secure such documents from unauthorized Access as set forth herein.

5.6 **Exit Procedures.**

5.6.1 Company will develop and maintain reasonable exit procedures to ensure that no departing employee or individual in its Supply Chain has Access to Covered Information after termination of employment or engagement by Company.

5.6.2 To the extent that such parties have access to Motorola corporate accounts, systems, offices or resources, after termination of employment or engagement by Company, Company will inform Motorola in writing within a reasonable time prior to or immediately upon termination of such individual.

5.7 **Physical Facilities and Systems.**

5.7.1 To the extent that Company Accesses Covered Information in physical facilities or using services, systems, computers, devices or media that are owned or managed by Motorola or Motorola's designated outsourcing suppliers, Company will require that its employees and its Supply Chain personnel conduct themselves in a manner compliant with all internal Motorola policies provided to Company that are relevant to the use of those facilities, services, systems, computers, devices or media and will require that all relevant employees and individuals in its Supply Chain are aware of and comply with such policies.

5.7.2 To the extent that Company Accesses Covered Information in physical facilities or using services, systems, computers, devices or media that are not owned or managed by Motorola, Company's Safeguards will include the following controls:

5.7.2.1 **Appropriate Physical Security Requirements.** Company will implement and maintain appropriate controls to prevent unauthorized physical Access to Covered Information, and the systems, computers, devices or media containing this information. Prototypes require additional security measures. All prototypes will be stored in an approved security enclosure and follow Motorola approved security procedures. All exterior doors and windows will be protected with industry standard security locks and monitored 24x7 by an industry standard alarm system. All exterior doors will be monitored 24x7 by video cameras. All computer rooms and closets will be protected by industry standard security locks and will be monitored 24x7 by video cameras. All computer rooms or closets will be monitored for unauthorized entry and have restricted access.

5.7.2.2 **Appropriate Systems Security Requirements.** Company will implement and maintain reasonable controls to prevent unauthorized Access to any system, computer, device or media used by Company to Access Covered Information. The controls will meet or exceed industry standards, including the following: (i) reasonable account and system access controls, including strong passwords (e.g., following password generation guidelines established by NIST or CERT) to secure any accounts with Access to Covered Information; (ii) reasonable malware controls, including the installation, regular update and routine use of both antivirus and antispyware software products on all systems, computers, devices or media with Access to Covered Information; and (iii) reasonably up-to-date software, including appropriate maintenance of Company's operating system(s) and other applicable software, and successful installation of reasonably up-to-date security patches on all systems, computers, devices with Access to Covered Information.

5.7.2.3 **Transported Asset Protection Association ("TAPA") Standards.** Upon request from Motorola, Company will obtain a TAPA Level A certification on all facilities in which it Accesses Covered Information, and will provide to Motorola a copy of such certification annually.

5.7.2.4 **Assessment and Reporting.** To the extent that Covered Information consists of Motorola owned goods, inventory, tools, or components, Company will conduct regular blind cycle counts of such Covered Information. Deviation of on-hand verses on-book inventory constitutes an Incident subject to the requirements of Section 8 below.

5.8 **Vulnerability Management.**

5.8.1 **Vulnerability Assessments**. Company will perform regular vulnerability assessments (including scans for network access), at least annually, of all infrastructure, applications and other dependencies used in connection with Company's performance of its obligations under an Agreement.

5.8.2 **Incident Response Program.** Company will maintain a specialized incident response process to respond to any cyber attacks and/or incidents involving Covered Information, including information security breaches.

5.8.3 **Logs.** Company will create and retain for a reasonable period logs and audit records reasonably sufficient to reconstruct all access, authentication and authorization events pertaining to Covered Information Accessed by Company and its Supply Chain.

5.9 **Internal Firewall**. If any Company projects exist that are competitive to the Motorola specific project for which Confidential Restricted Information, Company will maintain an internal firewall prohibiting Access to such information by any Company employees, or individuals in its Supply Chain, that work on such competitive projects, and that also sets a restricted Access period.

5.10 **Added Proprietary Information Requirements.**

5.10.1 **Clean Room.** Before Accessing Proprietary Information, Company will designate a secure "clean room" for the handling and storage of Proprietary Information (the "**Clean Room**"), and provide a description of the Clean Room's security features that will include, at a minimum, all applicable Safeguards set out herein. Company will not allow Access to Proprietary Information outside the Clean Room without Motorola's express prior written approval.

5.10.2 **Clean Room Acknowledgment Forms**. Company will acknowledge receipt of Proprietary Information by executing a separate acknowledgement form provided from Motorola that describes the specific Proprietary Information that is disclosed to Company. Each individual in a Controlled Group will execute a separate third-party acknowledgement form, provided by Motorola, prior to Accessing Proprietary Information. Company will deliver signed acknowledgement forms to Motorola prior to allowing Access to individuals in the Controlled Group.

5.10.3 **Clean Room Manager.** Before Accessing Proprietary Information, Company will designate a Clean Room Manager acceptable to Motorola that will have sole responsibility for managing the Clean Room and will accept all Proprietary Information from Motorola ("**Clean Room Manager**").

5.10.4 **Access to Proprietary Information.** Company will: (1) track and log Access to Proprietary Information by members of the Controlled Group; (2) preserve Access logs for the duration of the Controlled Group's Access to Proprietary Information; and (3) prohibit the Controlled Group from storing Proprietary Information on Portable Devices.

5.11 **Prototypes**. Company will comply with all of the following special terms and conditions for Prototypes.

5.11.1 **Prototype Terminal Delivery and Return.** Pursuant to the terms of an Agreement, Motorola may deliver to Company certain prototypes ("**Prototypes**") of its products for the Purpose. Company will track and return each of the Prototypes within five days following completion of testing, or, immediately upon Motorola's request.

5.11.2 **Post Delivery Support.** Company and Motorola agree that no post delivery support by Motorola is required by an Agreement. Motorola will handle any request for post delivery support from Company on a case-by-case basis.

5.11.3 **Software Upgrades for Prototypes.** Motorola will upgrade the Prototypes with the latest software if requested by Company, but does not guarantee that the Prototypes will have the capability to be upgraded. Any software upgrades will be provided within a jointly agreed period of time.

5.11.4 **Type Approvals.** Company acknowledges that while Prototypes have been designed and manufactured to comply with all applicable laws and regulations, Motorola may not yet have obtained the necessary approvals and has not placed the Prototypes on the market. In such instances, Motorola will be in the process of obtaining type approval from the appropriate regulatory bodies, and testing the Prototypes to ensure compliance with all applicable product safety requirements.

5.11.5 **Labeling.** Depending on where the Prototypes will be shipped, Motorola will label the Prototypes with the following notice language:

If shipped to North America or Latin America:

"This device has not been authorized as required by the rules of the FCC. This device is not and may not be, offered for sale or lease, or sold or leased, until authorization is obtained" and "CONFIDENTIAL MOTOROLA RESTRICTED PROPERTY: NOT FOR SALE"

If shipped to Europe:

"This device does not currently comply with the RTTE directive and is intended for demonstrative purposes only. This apparatus may not be marketed or put into service until it has been made to comply with the RTTE directive" and "CONFIDENTIAL MOTOROLA RESTRICTED PROPERTY: NOT FOR SALE"

If shipped to Asia:

"CONFIDENTIAL MOTOROLA RESTRICTED PROPERTY: NOT FOR SALE"

The label will be placed in a conspicuous location on the Prototypes. The Prototypes will not be labeled with the CE mark. Company will not remove, cover or otherwise tamper with any labels or markings on the Prototypes. Company will not photograph the Prototypes, or allow them to be photographed.

5.11.6 **No Transfer of Prototypes.** Company represents and warrants that it will not transfer, sell or lease to any third party, for compensation or otherwise, possession of or the right to use, possess, or operate, the Prototypes.

5.11.7 **Restrictions on Use.** Company agrees (i) it will not reverse engineer, de-compile, or disassemble the Prototypes including but not limited to any software embedded on such Prototypes; (ii) it will place the Prototypes in a secure environment within Company's facility and will not remove the Prototypes from such facility unless so authorized by Motorola; (iii) it will place the Prototypes in a secure and locked location when not in use by Company; (iv) to restrict access to the Prototypes to Company's employees who need to know to accomplish the Purpose; and (v) it will not attempt to circumvent, disable, or otherwise interfere with the operation of security-related software ("**Security Software**") embedded on Prototypes.

5.11.8 **Export Control**. Company acknowledges, agrees, and consents to Security Software sending location information of such Prototype to Motorola, which may reveal the location of Company or Company's employees evaluating such Prototype(s). Such location information will be used by Motorola solely to track the location of the Prototypes and may only be activated in the event of a breach of the applicable Agreement.

5.11.9 **Indemnification.** Company agrees to defend, indemnify, and hold Motorola harmless against any claims brought by third parties alleging injuries, damages, liabilities, and expenses (including attorney's fees) caused by any unauthorized use of the Prototypes.

5.11.10 **No Warranty**. No warranty or indemnity of any kind, express, implied, or statutory, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose, is given by Motorola in connection with Company's use of Prototypes. Motorola and Company agree and acknowledge that all such warranties are hereby excluded and Prototypes are provided "as is."

5.11.11 **No Liability**. In no event will Motorola be liable for any damages, including, without limitation, incidental or consequential damages, losses, or expenses arising out of Company's use, possession, or operation of the Prototypes. Company hereby waives such damages, losses, and expenses.

5.11.12 **Title of Prototypes**. Title to the Prototypes will at all times remain with Motorola. Company will not acquire any property rights, including, but not limited to intellectual property rights, in the Prototypes by reason of provision of such Prototype or under any Agreement and will not allow any mortgage, lien, or other encumbrance to be placed thereon.

5.11.13 **Tracking of Prototypes**. Motorola reserves the right to track the location of all Prototypes Accessed by Company. Company agrees that it will not interfere with any tracking measures Motorola applies to its Prototypes.

5.12 **Disaster Recovery.** If Company will Access Covered Information using its own systems, Company will maintain a written disaster recovery program that documents business impact assessments, contingency plans, and recovery procedures. Company will review, update and test its program regularly in accordance with changing technologies, conditions, and operational requirements. Company and Motorola will determine and agree on prioritized recovery objectives and ensure that Motorola's and Company's programs are compatible. Any occurrence or omission that causes Company to activate its disaster recovery program will qualify as an Incident as described by Section 8 below.

6. COMPLIANCE WITH SECURITY STANDARDS

6.1 Company covenants that it has implemented all Safeguards and other measures described in these Requirements.

6.2 When requested by Motorola in writing, Company will provide reasonable assurances in writing that it has implemented and maintains Safeguards and other requirements set forth herein.

6.3 Company will ensure that all its employees and individuals in its Supply Chain (including Permitted Recipients and members of a Controlled Group) strictly comply to Motorola's Information Protection Requirements.

7. SECURITY ASSESSMENT

7.1 Company will cooperate with reasonable efforts by Motorola to assess the sufficiency, in Motorola's commercially reasonable judgment, of Company's Safeguards and compliance with the requirements herein by responding to Motorola's reasonable information requests. As part of such an assessment, Company will provide Motorola with accurate information as Motorola may reasonably request, respond to reasonable information inquiries, and make Company representatives reasonably available to answer reasonable questions.

7.2 With reasonable prior written notice, Motorola may initiate annually, a non-intrusive, general assessment conducted pursuant to the terms of this Section 7.

7.3 Motorola may initiate an assessment concerning specific Company Safeguards and other requirements herein to respond to or otherwise manage an Incident or a change in circumstance that presents reasonably foreseeable risks to the security or confidentiality of Covered Information. Company will cooperate with such an assessment on an expedited basis.

7.4 Motorola may, in its sole discretion, assign its own employees or independent third parties acting on its behalf to perform assessments described in this section. If Motorola chooses to employ a third party, Motorola will ensure that the third party has agreed to terms of confidentiality with

respect to any Company-provided information no less restrictive than as apply to Motorola.

7.5 Motorola agrees to treat information provided by or on behalf of Company or gathered by Motorola as part of an assessment of Company hereunder as confidential and with appropriate care as obligated under the confidentiality terms of the applicable Agreement.

8. INCIDENT RESPONSE

8.1 Company will maintain an incident response program designed to manage any Incident in compliance with the requirements set forth herein.

8.2 Company will notify Motorola when Company has reason to believe that there has been or is reasonably likely to be unauthorized Access or loss of Access to Covered Information, (an "**Incident**"). Company will notify Motorola without unreasonable delay, but in no event longer than 24 hours after discovery of an Incident.

8.3 Notification to Motorola under this Section 8 will be made by sending an email to security@motorola.com that (i) provides a description of the Incident, identifies Covered Information at issue, identifies the known or suspected unauthorized recipients of the information, and summarizes all efforts undertaken and planned to investigate and resolve the Incident and secure the information, systems and services at issue; and (ii) identifies a point of contact at Company who will be available to Motorola as a contact regarding the Incident.

8.4 In the event of an Incident, Company will promptly provide assistance to Motorola in investigating the Incident, remedying the cause of such Incident, and taking any other actions reasonably necessary to halt the Incident (if it is ongoing).

8.5 The content of any statements, communications, notices, filings or reports by Company or its Supply Chain related to any Incident, including those required by law, will be provided to Motorola within a reasonable time prior to any publication or communication. Except for any notices and content thereof that Company or its Supply Chain are required by law to provide, all public statements, press releases or customer notifications by Company or its Supply Chain relating to the Incident will be approved by Motorola prior to any publication or communication.

8.6 Company will provide Motorola with the name, address, phone number, and email of a point of contact that will be available 24 hours a day, seven days a week so Motorola can report Incidents or obtain information about Incidents that Company has reported.

9. CORRECTIVE ACTION. If Motorola determines that Company's Safeguards contain a material vulnerability, it will promptly notify the Company in writing. Company will promptly correct or mitigate any material vulnerabilities (either discovered by Company or Motorola) in its Safeguards, systems, processes, policies, procedures involving its Access to Covered Information, within a reasonable period of time, but in no event longer than 60 days after Company's discovery unless no commercially reasonable solution is available within such period of time. Upon discovery or notification of a material vulnerability that is not corrected or mitigated within five business days of Company's discovery or receipt of notification of the same, Company agrees promptly to provide Motorola with a corrective action plan documenting the risks identified, Company's response to the risks, and specific dates by which the risks will be eliminated, or reduced to a level acceptable to Motorola, by Company.

10. THIRD PARTY AGENTS / SUBCONTRACTORS / SERVICE PROVIDERS. If Motorola has agreed in writing to permit Company's use of its Supply Chain to provide services and/or products to Company on Motorola's behalf, then Company agrees to: (i) provide its Supply Chain with Access to Covered Information only where there is a legitimate need to do so in connection with Company's obligations under a Agreement; (ii) ensure that members of Company's Supply Chain who have Access

to Covered Information agree in writing to take appropriate steps to implement their own Safeguards consistent with the requirements herein and the confidentiality provisions in the applicable Agreement; (iii) take reasonable steps to ensure that Company's Supply Chain has implemented appropriate Safeguards consistent with the requirements herein and the confidentiality provisions of the applicable Agreement; (iv) assume responsibility for the sufficiency of the security Safeguards that its Supply Chain has implemented; and (v) and assume liability for any failure Safeguards implemented in its Supply Chain to meet the terms and conditions herein and the confidentiality provisions of the applicable Agreement.

11. TERMINATION AND RETENTION

11.1 Upon expiration or termination of an Agreement, Company will ensure that all persons or entities acting on Company's behalf no longer have Access to Covered Information. Company will ensure that all persons or entities acting on Company's behalf: (i) immediately cease Accessing Covered Information; (ii) return or destroy all Covered Information and materials related thereto at Motorola's election, within 90 days or sooner if reasonably requested by Motorola, except to the extent that Company's retention of such information is required by law or Professional Responsibilities (as defined below); and (iii) upon written request of Motorola, confirm to Motorola in writing that it has done so.

11.2 Company may retain only the portions of Confidential Information as required by law, rule, regulation or in accordance with applicable professional standards or rules promulgated by the American Institute of Certified Public Accountants (AICPA), Public Company Accounting Oversight Board (PCAOB), or state board of accountancy (collectively, such retention rights, "**Professional Responsibilities**") following expiration or termination of a Agreement. Company will store such Confidential Information using industry-standard practices of due care. The Confidential Information stored in this manner will be kept solely as an archival copy, and will be securely destroyed as soon as Company is not required by law or Professional Responsibilities to retain it. Prior to such destruction, Company will maintain all Safeguards to protect the security and confidentiality of the retained Confidential Information.

11.3 Covered Information destruction should follow an industry standard procedure for complete destruction such as NIST Special Publication 800-88.

12. LEGAL PROCESS. Other than as necessary to perform its obligations under a Agreement, Company will not release Covered Information unless compelled to do so by a court or other government authority of competent jurisdiction or in accordance with applicable professional standards or rules promulgated by or in response to written requests from the AICPA, PCAOB, or state board of accountancy, subject to the conditions that Company: (i) takes reasonable steps to preserve the confidentiality of Covered Information, including without limitation (A) releasing or providing Access to only the minimum amount of information requested, and (B) taking reasonable steps to ensure that the release or Access does not result in further disclosure of the requested information to improper or unauthorized third parties or the public; (ii) provide, except as prohibited by law, Motorola prompt notice of the legal process and give Motorola the opportunity to seek an appropriate protective order or to pursue such other legal action necessary to preserve the confidentiality of Covered Information; and (iii) provide reasonable assistance to and cooperate with Motorola in its efforts to preserve the confidentiality of Covered Information.