Procurement Terms and Conditions

1. **OFFER AND ACCEPTANCE.** These Procurement Terms and Conditions, including its cover pages with commercial terms and administrative details and all attachments, (collectively, the "**Purchase Order**") constitute an offer by NortonLifeLock Inc. and its affiliates ("**NLL**") to purchase the goods, services, software licenses or other entitlements described in this Purchase Order (individually and collectively referred to as the "**Products**") and solely under the terms contained in this Purchase Order. The party to which this Purchase Order is issued is the seller, supplier or provider of such Products ("**Supplier**") and accepts this offer (pursuant solely to the terms herein) either by shipping the Products, promising to ship the Products or otherwise accepting or performing in accordance with this PurchaseOrder.

   ACCEPTANCE OF THIS OFFER IS EXPRESSLY LIMITED TO THE TERMS CONTAINED IN THIS PURCHASE ORDER. NLL OBJECTS TO AND HEREBY FULLY REJECTS ANY AND ALL TERMS PROPOSED BY SUPPLIER, INCLUDING WITHOUT LIMIT THOSE IN ANY QUOTE, INVOICE, ACCEPTANCE OR CONFIRMATION OF THIS OFFER WHICH ARE ADDITIONAL TO OR DIFFERENT FROM THE TERMS CONTAINED IN THIS PURCHASE ORDER. SUPPLIER AGREES THAT ANY SUCH ADDITIONAL OR DIFFERENT TERMS, WHETHER RECEIVED PRIOR TO OR AFTER THE DATE OF THIS PURCHASE ORDER, ARE HEREBY REJECTED BY NLL AND BY SUPPLIER AND WILL BE DISREGARDED AND DEEMED TO BE NULL AND VOID AND UNENFORCEABLE UNLESS SUCH TERMS ARE SPECIFICALLY AGREED TO IN A SEPARATE AGREEMENET BETWEEN THE PARTIES SIGNED BY A REPRESENTATIVE OF NLL AUTHORIZED TO ENTER INTO SUCH AGREEMENT.

   NO ASSIGNMENT. Neither party may assign this Purchase Order or their respective rights and obligations, in whole or in part and whether by operation of law, change of control or otherwise, without the other party's prior written consent, except to their successors by way of merger, acquisition or sale of assets, or to any entity controlling, controlled by or under common control with the assigning entity; provided, however, that Supplier may not assign or transfer to any competitors of NLL.

   COMPLIANCE. Any questions or inquiries concerning NLL's compliance with this Purchase Order, including without limit compliance with use restrictions and usage quantities will be discussed by the parties in good faith. If Supplier believes that NLL's responses are not accurate or complete, Supplier may engage a reputable and neutral third-party auditor to review NLL's usage records in compliance with industry standards and under the terms of a separate non-disclosure agreement. Such third party may not be compensated based on any findings or results.

2. **PAYMENT AND INVOICING.**
   - **A. PRICES.** The prices shown on this Purchase Order are the maximum amounts owed by NLL for the Products and are inclusive of all expenses, shipping, packing, handling and in-transit insurance charges.
   - **B. PAYMENT. Unless otherwise specified in this Purchase Order, undisputed payments for amounts due under or in connection with this Purchase Order will made within 60 days** of the later of NLL's receipt of invoice or receipt of Products.
   - **C. EXPENSES.** Expenses will be reimbursed at-cost (without mark-up) and only in compliance with NLL's Supplier Travel and Expense Policy, not to exceed the expense amounts specified on this Purchase Order.
   - **D. TAXES.** The prices shown on this Purchase Order do not include all applicable federal, state, and local taxes. All applicable taxes shall be stated separately on Supplier's invoice. If any withholding taxes are due in connection with this purchase, NLL will deduct the amount of such taxes from amounts otherwise due hereunder (with such net payment constituting payment in full) and, upon Supplier's request, provide documentation evidencing the amount of such taxes sufficient for Supplier to request a credit for the same.
   - **E. INVOICING.** (i) All invoices must include the respective Purchase Order line item number(s) against each line on the invoice, reflecting the qty, unit price, and unit of measure (and, when applicable, the point of shipment, complete routing and amount of freight prepaid), and non-compliant invoices will be rejected, (ii) all invoices are due and must be received by the last day of the month immediately following the month in which goods, services, software licenses and other entitlements were delivered or made available, including reimbursable expenses incurred (for example, fees and expenses incurred in October must be invoiced no later than November 30th), and (iii) only amounts specified in this Purchase Order are agreed and authorized for payment when due. **Except as expressly provided in this paragraph, no amounts may be incurred or invoiced or will be paid or are payable, and your organization and its representatives hereby waive all rights to collect any such amounts. This paragraph supersedes and will control in the event of a conflict or inconsistency with any other applicable terms and no attempt to supersede this paragraph will be valid or enforceable.**

3. **PHYSICAL DELIVERIES.** Unless otherwise expressly stated:
   - A. **Title and risk of loss or damage for all Products will pass to NLL upon its actual receipt of such Products at NLL's specified place of delivery. Supplier will bear the risk of loss or damage for Products rejected by NLL, except to the extent caused by NLL's employees' misconduct or negligence.**
   - B. NLL may at any time may reschedule delivery of all or part of the Products at no additional charge. The new delivery date designated by NLL will become the scheduled delivery date.
   - C. All Products will be packed in a manner that is: (i) in keeping with good commercial practices, (ii) acceptable to common carriers for shipment at the lowest rate for the particular Products, (iii) in accordance with I.C.C. regulations and (iv) adequate to ensure safe arrival of the Products at the specified destination.
   - D. All containers will be marked with the applicable lifting, handling and shipping information that includes Purchase Order numbers, Supplier's part number, the number of cartons and any other unique markings required by the NLL.

E. All shipments must be identified as either partial or complete and must include an itemized packing list with NLL's name, a named individual to act as recipient; complete "ship to" address (including building number); this Purchase Order number; quantity; description of shipment; dimensions of the shipping containers; net and gross weight.
F. At NLL's option, over-shipments will be returned at Supplier's risk and freight collect.
G. For Products delivered ahead of the scheduled delivery date, NLL may (1) return such Products at Supplier's risk and freight collect, or (ii) accept such Products with payment based on the scheduled delivery date and not the date of receipt by NLL.
H. Regardless of any prior inspection or payments, all Products will be subject to final inspection and acceptance (or rejection) at NLL's facility within a reasonable time after delivery.
I. Supplier must be the exporter and importer of record for all returns shipped. Supplier must comply with all applicable other nation rules and regulations pertaining to the export and/or import of rejected goods returned.

4. **WARRANTY AND REMEDIES.** Supplier hereby represents and warrants to NLL that Supplier and its Personnel:

A. will have all authority, licenses, permits, consents and legal documentation necessary to enter and perform under this Purchase Order, and will fully comply with all applicable laws, codes, and regulations (including without limit those regarding data privacy, export and import, the environment and hazardous materials);
B. do not know of any actual or potential conflicts of interest concerning this Purchase Order, and performance hereunder will not result in breach of any agreement with a third party;
C. will not use or provide NLL with any third party confidential or proprietary information or materials unless Supplier has obtained written authorization from such party for the use of such information and materials;
D. will perform under this Purchase Order with all necessary care, skill and diligence and in a professional manner pursuant to reasonable industry standards;
E. the Products will be new unless otherwise expressly purchased as used or refurbished;
F. the Products and will meet the specifications set forth in this Purchase Order or as otherwise expressly agreed by the parties in writing;
G. no claim is pending or threatened against the Supplier (or its suppliers) alleging that any Product infringes the IPR of any third party;
H. the media, if any, on which any Product is delivered to NLL will be free of defects in materials andworkmanship, and
I. all software and technology Products will be free of any viruses and illicit code, and Supplier will not deliver any software without first having used at least commercially reasonable means and practices to detect, completely remove and destroy any viruses and illicit code and confirm such removal and destruction.

For breach of warranty under subsections 4.E 4.F and/or 4.H, Supplier will promptly at its sole cost and expense, and at NLL's option,: (i) re-deliver the Products to NLL's reasonable satisfaction; (ii) refund the relevant fees paid for the deficient Products and any other Products whose use or value to NLL is materially degraded as a result of Supplier's failure to deliver conforming Products (in which case Supplier acknowledges and agrees NLL may, without further notice, cancel this Purchase Order in whole for default in accordance with the Section titled Cancellation).

EXCEPT AS PROVIDED UNDER THIS PURCHASE ORDER, SUPPLIER MAKES NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONCERNING MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

5. **TERMINATION.**

Supplier may terminate this Purchase Order if NLL commits a material breach hereunder and fails to cure such breach (or provide a reasonable plan to cure such breach) within 30 days of receiving written notice from Supplier detailing the breach. NLL may at any time terminate this Purchase Order in whole or in part, with or without cause, by providing Provider with written notice. Termination is effective immediately unless otherwise specified in the termination notice.

Upon any such termination, the sole compensation Supplier shall be entitled to invoice and/or receive from NLL shall be the price for any Products actually received and accepted by NLL prior to cancellation and Supplier hereby waives its rights to receive or collect additional amounts. If this Purchase Order is cancelled due to Supplier's default, NLL may procure, at Supplier's cost and in the manner NLL deems appropriate, Products similar or substantially similar to those cancelled.

6. **INDEMNITY.** Supplier shall indemnify, defend and hold harmless NLL and its officers, directors and employees from any losses, liabilities, damages, demands, suits, causes of action, judgments, costs or expenses (including court costs and reasonable legal fees) arising from:

A. any property damage, personal injury or death arising from the acts or omissions of Supplier or third parties engaged by Supplier;
B. any claims that the Products prepared or provided by or on behalf of Supplier hereunder infringe or misappropriate the intellectual property rights of any third party;
C. any claims or determinations that a relationship other than that of independent contractor was established between NLL and Supplier or any Supplier Personnel under: (a) in relation to the United Kingdom, the Transfer of Undertakings (Protection of Employment) Regulations 2006; (b) in relation to any other European Union member states, any national legislation implementing the Acquired Rights Directive; and (c) in relation to any state which is not a member of the European Union, any national or local legislation, which is broadly similar to the provisions of the Acquired Rights Directive, and
D. third party claims arising from breaches of confidentiality and personal data obligations, including without limit unauthorized use, access or disclosure of NLL's confidential information.

NLL shall have the right to approve any counsel retained to defend any demand, suit or cause of action in which NLL is a defendant, with

such approval not to be unreasonably withheld. Supplier agrees that NLL shall have the right to participate in the defense of any such demand, suit or cause of action concerning matters that relate to NLL. Supplier may not enter into any settlement without NLL's express written consent (which shall not be unreasonably be withheld), unless such settlement (i) releases NLL in full for all claims, (ii) does not impose any obligation on NLL, other than ceasing use of the infringing items (if any), and (iii) includes no admission of any kind by or on behalf of NLL. If, in NLL's reasonable judgment, a conflict exists in the interests of NLL and Supplier, NLL may retain its own counsel.

7. **LIMITATION OF LIABILITY.** EXCECPT FOR DEATH OR PERSONAL INJURY, BREACHES OF CONFIDENTIALITY OR PERSONAL DATA OBLIGATIONS, VIOLATIONS OF APPLICBALE LAW OR REGULATION, OR FRAUD OR INTENTIONAL MISCONDUCT, NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY, OR TO ANY THIRD PARTY, IN CONNECTION WITH THIS PURCHASE ORDER OR THE PRODUCTS AND SERVICES HEREUNDER FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, INCLUDING ANY DAMAGES FOR LOST PROFITS OR LOST REVENUE INCURRED BY EITHER PARTY OR ANY THIRD PARTY, WHETHER IN ACTION, CONTRACT OR TORT, EVEN IF THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

8. **INSURANCE.**

A. Unless otherwise expressly stated in a separate written agreement signed by both parties (which agreement is intended to govern the purchase or sale of the Products specified in this Purchase Order**), Supplier will maintain the following insurance coverage (or non-US dollar equivalents for Suppliers outside of the US) for the Products and its performance under this Purchase Order provided to NLL Corporation and its affiliates located in North America, South America, Europe, the Middle East and Africa**:

(i) Commercial general liability insurance (including contractual liability coverage) on an occurrence basis for bodily injury, death, "broad form" property damage, and personal injury, with coverage limits of not less than One Million Dollars ($1,000,000) per occurrence and Two Million dollars ($2,000,000) general aggregate for bodily injury and property damage;
(ii) Auto liability insurance covering all owned, non-owned and hired vehicles, with coverage limits of not less than One Million Dollars ($1,000,000) per occurrence for bodily injury and property damage;
(iii) Worker's compensation insurance as required by law in the state where the services will be performed, including employer's liability coverage for injury, disease and death, with coverage limits of not less than One Million Dollars ($1,000,000) per accident and employee;
(iv) Umbrella liability insurance on an occurrence form, for limits of not less than Three Million Dollars ($3,000,000) per occurrence and in the aggregate; and
(v) Professional liability (Errors & Omissions) on an occurrence or claims-made form, for limits of not less than Two Million Dollars ($2,000,000) annual aggregate.

Insurance carriers shall be rated A-1 or better by A.M. Best Company. The NLL entity issuing this Purchase Order is to be added as an additional insured on the Commercial General Liability policy. Licensor's Commercial General Liability policy shall be considered primary without right of contribution of any insurance carried by NLL insurance policies. Policies shall contain a Severability of Interests clause. Policies shall provide thirty (30) days written notice prior to cancellation, except in the event of non-payment, which shall require at least ten (10) days' notice.

In no event shall the foregoing coverage limits affect or limit in any manner Supplier's contractual liability for indemnification. Supplier shall be solely responsible for ensuring that its subcontractors maintain insurance coverage at levels no less than those required of Supplier under this Section. All of Supplier's activities under this Purchase Order shall be at Supplier's own risk, and Supplier's employees and agents shall not be entitled to any benefits under the policies of insurance maintained by NLL.

B. For Products and its performance under this Purchase Order to NLL affiliates in Australia, Supplier shall obtain and maintain in force with reputable insurers during the term of any services such insurance as is required by law in Australia, including Auto Liability and coverage for work place injury, and any coverages which are usual, customary and appropriate for its business according to the services or products provided. This shall include but is not limited to the following coverage (with non-US dollar equivalent amounts if policy limits are not provided in US dollars):

(i) Public and Products Liability – in limits not less than $10,000,000 AUD. The policy shall include an Indemnity to Principal endorsement in favor of NLL.

(ii) Professional Indemnity or IT Liability for damages arising from negligent acts, errors & omissions caused by the Supplier or any subcontractors conducting work on their behalf, with limits of not less than $1,000,000 AUD.

Supplier's coverage shall be considered primary without right of contribution of NLL's insurance policies. In no event shall the foregoing coverage limits affect or limit in any manner Supplier's contractual liability for Indemnification. Supplier shall be solely responsible for ensuring that its subcontractors maintain insurance coverage at levels no less than those required of Supplier under this Section. All of Supplier's activities under this Agreement shall be at Supplier's own risk, and Supplier's employees and agents shall not be entitled to any benefits under the policies of insurance maintained by NLL.

C. **For Products and its performance under this Purchase Order to NLL affiliates in India,** Supplier shall obtain and maintain in force with reputable insurers during the term of this Agreement such insurance as is required by law in India, such as Auto Liability, and any coverages which are usual, customary and appropriate for its business according to the services or products provided. This shall include but is not limited to the following coverages (with non-US dollar equivalent amounts if policy limits are not provided in US dollars):

1) Public Liability insurance in limits not less than the local currency equivalent of $1,000,000 USD, including coverage for Contractual Liability and Personal and Advertising injury.
2) Errors and Omissions insurance for damages arising from negligent acts, errors & omissions caused by the Supplier or any subcontractors conducting work on their behalf, with limits not less than the local currency equivalent of $1,000,000 USD.

The NLL entity issuing this Purchase Order shall be added as an additional insured to provider's policies.

Supplier's coverage shall be considered primary without right of contribution of NLL's insurance policies. In no event shall the foregoing coverage limits affect or limit in any manner Supplier's contractual liability for Indemnification. Supplier shall be solely responsible for ensuring that its subcontractors maintain insurance coverage at levels no less than those required of Supplier under this Section. All of Supplier's activities under this Agreement shall be at Supplier's own risk, and Supplier's employees and agents shall not be entitled to any benefits under the policies of insurance maintained by NLL.

9. RELATIONSHIP OF THE PARTIES / PERSONNEL

A. Supplier will ensure each of its employees, contractors, subcontractors, agents and any other third party engaged by Supplier or acting on Supplier's behalf (individually and collectively, ("**Personnel**") is bound by written agreement with Supplier to comply with the terms of this Purchase Order (including without limit those of confidentiality and data protection), and all requirements of any relevant statement of work as such statement of work applies to such Personnel. In addition, (i) Supplier shall be fully responsible and liable to NLL for all acts, omissions and breaches by its Personnel as if the same were undertaken directly by Supplier.

B. Supplier is and shall at all times be deemed to be an independent contractor to NLL and nothing in this Purchase Order is intended to or shall be construed to establish between the parties any relationship of partnership, joint venture, joint employment, employment, franchise, or agency between the parties. Neither party has authority, and shall not represent that it has authority, to assume or create any obligation, express or implied, on behalf of the other party. As an independent contractor, Supplier shall be solely responsible for determining the means and methods for providing the Products. Furthermore, Supplier (and not NLL) shall be responsible for (a) making all applicable payments, reports and collections (including without limit federal, state and local taxes, social security, unemployment compensation and other contributions and withholdings) to and for its Personnel in compliance with all federal, state and local laws, regulations and the like, and (b) paying all applicable wages, benefits and other compensation to and for its Personnel (including without limit medical, dental, workers' compensation, disability insurance, pension or retirement plans and the like).

C. The terms of this section apply only to Supplier Personnel who may (i) perform Services on NLL designated premises, (ii) have access to Personal Data, (iii) have access to confidential information of NLL's customers, or (iv) have access to any network, systems or data repository owned or used by NLL, (individually and collectively 'Designated Services"), if any. NLL's work rules, policies and procedures must be adhered to and Supplier Personnel will not remove any materials, data or property from NLL's premises without first obtaining NLL's express consent. Upon NLL's request, Supplier will immediately remove any individual assigned to perform the Designated Services and replace with an equal or greater skilled individual. NLL will not be invoiced or obligated to pay for any time or expenses incurred to train and familiarize such replacement with the applicable Services engagement. Before Supplier Personnel may perform Designated Services, Supplier warrants that: (a) to the extent permitted by local law, it will perform (and will obtain appropriate consent to perform) those background investigations as required under a SOW, exhibit hereto or as otherwise expressly agreed by the parties in writing or, if none are expressly identified, then the background investigation will include a local, county and federal background investigation for each such individual including but not limited to identity and education verifications, eligibility to work confirmation and a detailed examination of criminal convictions involving a dishonest act (including but not limited to fraud, theft and embezzlement) and injury or threatened injury to another person, and (b) no information was discovered in such background investigation(s) that could negatively impact the performance or the integrity of the Services, and (c) Supplier will provide background investigation results and/or attestation to confirm compliance with this section, as NLL may request from time to time. NLL reserves the right to refuse access to its premises and network(s) at any time and for any lawful reason. Supplier's breach of this section will be a material breach of the Agreement.

10. WORK PRODUCT AND OWNERSHIP. All tangible and non-tangible items, hardware, equipment, documents, writings, data, content, graphic designs, photographs, reports, workflows, software (including modifications and documentation), feedback or other materials that are prepared for or provided to NLL under this Purchase Order, including without limit any data and information as input, processed and generated or output by any software Products (whether the software is on-premise at NLL or hosted by Supplier or its cloud or host providers, and whether provided as a subscription, SAAS or other service) ("**Results of Service**") shall be the sole and exclusive property of NLL. Supplier agrees that, to the maximum extent permitted by applicable law, and rights, title and interests in and to all Results of Service shall vest with and be owned solely by NLL including without limit all copyright, patent, trade secret, trademark and any other intellectual property rights (individually and collectively, "**IPR**") therein. In the event that all rights, title and interests in and to any Results of Service do not vest with or are owned solely by NLL, Supplier hereby irrevocably assigns to NLL for no additional consideration all rights, title and interests in and to the Results of Service and all IPR therein including without limit any applications, extensions and renewals therefor. Upon NLL's request, Supplier agrees to execute written assignments of such rights to NLL (and any other documents

necessary for NLL to establish, preserve, perfect or enforce its IPR in the Results of Service). Supplier hereby waives and agrees not to assert any "moral rights" that Supplier may have in the Results of Service, and Supplier hereby assigns to NLL all moral rights therein. In the event that any Results of Service are not assignable to NLL, Supplier hereby grants NLL a non-exclusive, worldwide, perpetual, fully-paid up, irrevocable license in and to those Results of Service and all IPR therein, including without limit the right to use, copy, sell, distribute (directly and through multiple tiers), and create and own derivative works of those Results of Service for itself and others and without accounting to Supplier.

In the event that any Pre-Existing Work owned or licensed by Supplier is provided to NLL under this Purchase Order or is otherwise integrated into Results of Service, Supplier hereby grants to NLL a non-exclusive, worldwide, perpetual, fully-paid up, irrevocable license in and to those Pre-Existing Works and all IPR therein to the extent necessary for NLL to exercise all of its rights in and to the Results of Service. "**Pre-Existing Works**" means all products, information and materials developed or otherwise created by or on behalf of Supplier prior to or independently from its performance under this Purchase Order, including without limit designs, inventions, object code, source code, documents, methods, specifications, notes and tools.

11. CONFIDENTIAL INFORMATION

"**Confidential Information**" means all (i) Personal Data and (ii) non-public information provided or revealed by one party ("**Discloser**") to the other party ("**Recipient**") or otherwise learned by a party during the course of performance under this Agreement, including without limit software, programs, prices, processes, requirements, documentation, bank account, credit card, financial, marketing and other business plans and information, and any other material or information identified at the time of disclosure as confidential or proprietary, or which otherwise one would reasonably expect to be confidential or proprietary. "**Personal Data**" means any information related to any identified or identifiable natural person (the "**Data Subject**"), an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The Data Subjects herein may be NLL (or its agents' or distributors') employees, contractors, end users, customers, customers' end users or employees, and/or other third parties. For clarity, all Results of Service and all information, data, content uploaded to a Product by or on behalf of NLL are NLL's Confidential Information. Except for Personal Data, Recipient's obligations of confidentiality hereunder do not apply to information that: (a) is or becomes public through no fault or breach by Recipient, (b) is or becomes known to Recipient (either directly or rightfully through a third party) without an obligation of confidentiality, (c) is independently developed by Recipient without use of or access or reference to Discloser's Confidential Information or (d) is disclosed with the prior written approval of Discloser on a case-by-case basis. All Confidential Information is and shall remain the sole property of Discloser, and Recipient shall not acquire any rights or licenses therein except as expressly set forth in this Agreement.

Recipient will not disseminate or disclose Confidential Information except to its Personnel with a bona fide need to know and who are under binding written obligations of confidentiality with Recipient to protect Discloser's Confidential Information substantially in accordance with the terms of this Agreement. In addition, Recipient may disclose Discloser's Confidential Information as required by law or court order but only if Recipient: (a) promptly notifies Discloser in writing of the requirement for disclosure, (b) discloses only as much of the Confidential Information as is required by such law or court order, and (3) provides a copy of disclosed information to Discloser.

Recipient must protect Discloser's Confidential Information with the same degree of care it uses to protect its own confidential information of a similar nature, and never using less than a reasonable degree of care. Recipient must use Discloser's Confidential Information only to the extent necessary in relation to its rights and obligations under this Agreement and must not use (and shall have no right to use) Confidential Information for any other purpose. In addition, Recipient must have and implement reasonable and appropriate technical, physical and organizational measures to protect Confidential Information against accidental or unauthorized access, use, alteration, disclosure, tampering or loss, and must provide at least a reasonable level of security appropriate to the risk represented by the possession, processing and nature of the Confidential Information to be protected. Such measures must comply with the laws, rules, regulations and orders of any governmental authority having relevant jurisdiction, including without limit the provisions of any data protection laws.

Supplier will notify NLL without undue delay (and, in all cases, not later than 24 hours) from the occurrence of any known or reasonably suspected accidental, unauthorized, or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Confidential Information transmitted, stored or otherwise processed hereunder. The notice will include sufficient detail for NLL to comply with its obligations related to the subject Confidential Information and take steps to prevent or minimize hardships from such disclosures. Supplier shall provide full and prompt cooperation and support as requested by NLL, including but not limited to making available key Personnel with sufficient knowledge to resolve or mitigate any the incident (including data privacy or security issues involving Personal Data), determine the scope of the incident, investigate the incident and root cause, prepare a written summary and assist in taking corrective action including any notification and/or announcement to regulators, affected parties and the public.

Unless otherwise directed by Discloser, Recipient will (at no cost) return to Discloser (or, at Discloser's express direction, destroy) any and all Confidential Information and any other information and materials that contain such Confidential Information immediately upon Discloser's request, or upon the earlier of the completion of Services or termination of this Agreement. Within 10 days following NLL's request, Supplier will provide NLL with a written certification, as signed by an officer or executive level employee of Supplier, certifying

to Supplier's compliance with this Section.

Recipient agrees that any breach of confidentiality and Personal Data obligations may result in irreparable harm to Discloser for which monetary damages may not be sufficient and that Discloser will be entitled to seek equitable relief without prejudice and in addition to any other rights or remedies the Discloser may have.

12. INFORMAITON SECURITY AND DATA PROTECTION

Information Security. Supplier represents that it has and will maintain, at a minimum, the technical and organizational measures and controls specified in **Exhibit A** attached hereto (NLL's Supplier Security Requirements), and Supplier will update those with equivalent or more protective measures and controls as needed to remain compliant at all times with then-current industry standard practices.

Personal Data and Tracking. Encompassed with and subject to Supplier's obligations under Section 17 (Confidential Information), and to the extent that Supplier processes Personal Data for, or on behalf of, NLL pursuant to this Agreement, the terms of the Data Processing Addendum attached hereto as **Exhibit B** applies. "Process" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. If Supplier uses or provides tracking technologies (including without limit pixels, tags or web beacons) in the performance of Services, Supplier must: (i) notify NLL about the type of tracking technology used and the information collected, (ii) collect information and use information gained exclusively to perform the Services; and (iii) enable appropriate mechanisms to allow data subjects to opt-in and opt-out of such tracking technologies including but not limited to the provision of accurate and complete disclosures prior to the collection of information in accordance with applicable laws.

13. PUBLICITY. Supplier shall have no right to use NLL's name, logos or trademarks or otherwise make any direct, indirect or implied reference to NLL, its relationship with Supplier or any benefits NLL has or may derive from the Products or its relationship with Supplier, without obtaining prior express written consent from NLL's Public Relations department on a case by case basis (and not as part of any other document issued by or on behalf of Supplier under this Purchase Order).

14. GOVERNMENT CONTRACT. If this Purchase Order is related directly or indirectly with the performance of a prime contract with the U.S. Government or a subcontract thereunder, the terms of the Federal Acquisition Regulations or other appropriate regulations thereunder will be inserted in contracts or subcontracts that apply to this Purchase Order.

15. EXPORT. Supplier shall comply with all applicable international, national, federal, state and local laws, regulations and rules governing the Product and Results of Service, including compliance with any export licenses in performing its duties hereunder. Supplier shall not export or re-export any software, personal computer system, part, technical data or sub- elements under this Purchase Order ("Technical Data"), directly or indirectly in violation of export control laws or regulations of the United States or other countries including the United States Department of Commence Denial and Probation Orders and sanctions administered by the Office of Foreign Assets Control, and, furthermore, shall not distribute Technical Data to any country, firm or person listed on such Orders or sanctions. Software and Technical Data is prohibited for export or re-export to any destinations prohibited by applicable export and import laws, rules and regulations, without first obtaining a license (including, but not limited to Cuba, North Korea, Iran, Syria and Sudan or to any country subject to relevant trade sanctions). Supplier is responsible for maintaining internal procedures to comply with relevant export laws and agrees that such compliance shall be at its own expense and legal direction. Supplier shall obtain and maintain in effect all licenses, permits and authorizations required for the performance of its obligations hereunder and shall provide NLL with all applicable information to enable NLL's compliance with relevant laws and regulations, including, but not limited to, applicable U.S. Export Control Classification Numbers and other information as NLL may reasonably request. A breach of this section by either party is deemed a material breach and grounds for termination of this Purchase Order for cause.

16. COMPLIANCE WITH ANTI-CORRUPTION LAWS. Supplier shall comply (and shall ensure its officers, directors, employees and contractors, subcontractors, agents and any person or entity acting on its behalf or under its control comply) with all applicable U.S. and international anti-corruption laws and regulations, including but not limited to the U.S. Foreign Corrupt Practices Act and the UK Bribery Act. No payments or transfers of value shall be made which have the purpose or effect of public or commercial bribery, acceptance or acquiescence in extortion, kickbacks or other unlawful or improper means of obtaining or retaining business or directing business to any person or entity. Supplier shall cooperate fully in NLL's efforts to enforce the terms of this provision, including but not limited to providing, upon request from NLL (i) certification of compliance with this provision as signed by an authorized representative of Supplier and (ii) reasonable and prompt cooperation at Supplier's expense with respect to any investigation relating to this provision.

17. GENERAL

A. **Governing Law; Venue**. The provisions of the United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Purchase Order.

- **Purchase Orders entered into by NLL Corporation or its affiliates located in North America and South America** will be valid, governed and construed exclusively in accordance with the laws of California without regard to principles of conflicts of law. Any legal action or

proceeding arising under this Purchase Order will be brought exclusively in Santa Clara County, California, and the parties hereby consent to personal jurisdiction and venue therein. The provisions of the United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Purchase Order.

- **Purchase Orders entered into by NLL Corporation affiliates located in Europe, the Middle East and Africa** will be valid, governed and construed exclusively in accordance with the laws of England and Wales without regard to principles of conflicts of law. Any legal action or proceeding arising in connection with this Purchase Order will be brought exclusively under the jurisdiction of the English courts, and the parties hereby consent to personal jurisdiction and venue therein.

- **Purchase Orders entered into by NLL Corporation Affiliates in Asia Pacific including India and excluding Japan and China** will be valid, governed and construed exclusively in accordance with the laws of Singapore without regard to principles of conflicts of law. Any legal action or proceeding arising in connection with this Purchase Order will be brought exclusively in the courts of Singapore, and the parties hereby consent to personal jurisdiction and venue therein.

B. Severability. If any provision of this Purchase Order is found partly or wholly illegal or unenforceable, such provision shall be enforced to the maximum extent permissible, and the legality and enforceability of the other provisions of this Purchase Order shall remain in full force and effect.

C. No Waiver. The failure by either party to enforce any provision of this Purchase Order will not constitute a waiver of future enforcement of that or any other provision. All of the remedies provided for in this Purchase Order are non- exclusive and without prejudice to any other rights NLL may have at law or in equity.

D. Equal Opportunity Employer. Supplier represents that (i) it is an equal opportunity employer and does not discriminate on the basis of race, sex, age, national origin, disability, marital status, veteran status or any other basis forbidden by law and (ii) all Products will be provided/performed in conformance with the above stated nondiscrimination policy and all applicable equal opportunity laws and policies and (iii) Supplier will not directly or indirectly violate the letter or spirit of such laws and policies.

E. Survival. Except as expressly set forth herein, the rights and obligations which by their nature are on-going shall survive even following the parties' completion of performance under the Purchase Order (and shall survive any cancellation or termination of this Purchase Order), including without limit those related to payment, ownership, confidential information, data protection, relationship of the parties, indemnity, limit of liability, publicity, export and compliance with laws.

F. Conduct.

(i). *Code of Conduct*. Supplier will at all times comply with NLL's Global Supplier Code of Conduct, a copy of which can be found at: https://www.nortonlifelock.com/theme/procurement-code-conduct

(ii). *U.N. Global Compact*. NLL is a participant in the United Nations Global Compact ("Global Compact"). As a participant, NLL encourages Supplier to conduct its business pursuant to the Global Compact's Ten Principles (www.unglobalcompact.org). The Global Compact is an international initiative working to advance ten universal principles in the areas of human rights, local labor laws, environmental and anti-corruption.

G. Response to Subpoena. In the event that Supplier receives a subpoena from any party or a request for information from a government agency ("Subpoena") for NLL's Confidential Information, or is otherwise legally compelled to produce NLL's Confidential Information, Supplier will (a) promptly notify NLL of the existence of such Subpoena; (b) promptly request that such Subpoena be reissued directly to NLL; and, (c) where the requesting party refuses to reissue the Subpoena directly to NLL, reasonably cooperate with NLL in responding to such requests for information or documents and provide NLL with a copy of any and all of Supplier's responses to the Subpoena if permitted to do so.

In the event that NLL receives a Subpoena for NLL's Confidential Information, Supplier will reasonably cooperate with NLL to produce NLL's Confidential Information in a timely manner. Such cooperation may include, but is not limited to, gathering and providing NLL's Confidential Information to NLL at no additional charge to NLL. Where the burden on Supplier associated with such cooperation exceeds that which is reasonable, the parties will engage in good faith negotiation regarding an appropriate allocation of cost.

(END OF TERMS
EXHIBIT A (MASTER PROVIDER SECURITY REQUIREMENTS) AND EXHIBIT B (DATA PROCESSING ADDENDUM AND ITS ATTACHMENTS) FOLLOW ON THE NEXT PAGES)

EXHIBIT A
NortonLifeLock Inc. and its Affiliates ("NLL")
Master Provider Security Requirements

1. NLL SECURITY REQUIREMENTS

The service provider (or "Provider") shall operate in compliance with: i) the requirements set forth in this Master Provider Security Requirements document, (ii) industry best practices and standards; and iii) any applicable legal and regulatory requirements.

Nothing herein is intended or shall be construed to limit Provider's obligations to NLL under any agreement, statement of work or other terms or conditions (collectively "Agreement") between NLL and Provider. In the event of any conflict between such provisions and this Provider Security Requirements document, the stricter, higher or more protective standard shall govern unless otherwise expressly agreed to in writing and signed by both parties.

2. **DEFINITIONS**

TERM	DEFINITION
NLL Data	Any NLL data, content and information that Provider is provided, or has access to, pursuant to the applicable Agreement with NLL.
NLL Restricted Data	Highly sensitive NLL Data limited to very few individuals and shared only on a need-to-know basis. Applies to NLL Data that must be protected due to legal or regulatory requirements; may give NLL a competitive advantage. Any NLL Data containing Nonpublic Personal Information (NPI), Personally Identifable Information (PII), or Protected Health Information (PHI) is considered NLL Restricted. Unauthorised disclosure impact will be severe. Unauthorized access, use, or disclosure is expected to have a major reputational, regulatory, or financial impact. The business impact of loss or modification will be severe and is expected to have a major adverse effect on operations, assets, or individuals.
NLL Confidential Data	Sensitive NLL Data limited to small groups (e.g., project teams) and shared only on a need-to-know basis. Applies to company secrets, proprietary code, and other data that would give NLL a competitive advantage. Any NLL Data that is not expressly classified under this Section 2 as either NLL Restricted Data, NLL Confidential Data or Internal Use Only is NLL Confidential. Unauthorised disclosure impact will be severe to moderate. Unauthorized access, use, or disclosure may have a major reputational or financial impact but is not expected to have a regulatory impact. The business impact of loss or modification will be severe to moderate and may have a major adverse effect on operations, assets, or individuals.
NLL Internal Use Only	Non-sensitive NLL Data used for conducting company business. Applies to data commonly available within NLL and used for daily operations. Unauthorised disclosure impact will be minimal. Unauthorized access, use, or disclosure is not expected to have a reputational, regulatory, or financial impact. The business impact of loss or modification will be minimal and may have a limited adverse effect on operations, assets, or individuals.
Handle (or "handle")	Any processing operation(s) performed upon NLL Data, whether by automatic means or not, such as collecting, recording, using, accessing, copying, reproducing, retaining, storing, disclosing, modifying, altering, transferring, transmitting, deleting, destroying or otherwise disposing of, selling, assigning, licensing, or marketing.
Personnel	Provider's employees, contractors, subcontractors, and/or third parties engaged by or on behalf of Provider that provide services to NLL and/or handle NLL information.
NLL Information Assets	NLL assets including end user computing devices, networks, infrastructure, data respositories.

3. INFORMATION SECURITY POLICIES

3.1. Management Direction for Information Security

3.1.1. Provider shall maintain an Information Security Policy (ISP) that is reviewed and approved at least annually at the executive level. Provider shall ensure that all Personnel have access and comply with the ISP.

4. ORGANIZATION OF INFORMATION SECURITY

4.1. Internal Organization

4.1.1. Provider shall adopt physical, technical and organizational security measures in accordance with industry best practices and standards, and be in compliance with all applicable legal and regulatory requirements as they apply to the Provider's services being provided to NLL.

5. HUMAN RESOURCE SECURITY

5.1. Prior to employment

5.1.1. Without limiting obligations under an Agreement, Provider shall, when and to the extent legally permissible, perform background verification checks in compliance with the NLL policies for all Personnel who may have access to NLL Restricted Data or NLL Confidential Data and/or the NLL network. Such background checks shall be carried out in accordance with and as permitted under applicable regulation and law, and shall include the following regional equivalent items: SSN Trace, Global Blacklist Search, Criminal County Search (5-Year Address History), Criminal Federal Search (5-Year Address History), and Financial Sanctions Search.

5.2. During employment

5.2.1. Provider shall provide security awareness training based on industry best practices and standards to all Personnel at least annually.

5.2.2. Additional Training

5.2.3. Provider shall complete and implement additional training as may be required by NLL from time to time.

5.3. Termination and change of employment

5.3.1. Provider shall implement effective user termination / transfer controls that include access removal / disablement immediately upon termination or transfer of Personnel or when such Personnel no longer require handling of Symnatec Data as part of their job duties for Provider.

6. ASSET MANAGEMENT

6.1. Responsibility for assets

6.1.1. Providers that use NLL Information Assets shall strictly adhere to NLL's Acceptable Use Standard.

6.1.2. NLL Information Assets may not be modified in any way or used to provide services to any other parties other than by prior express written agreement with NLL.

6.2. Media handling

6.2.1. Destruction Requirements and Compliance Evidence

6.2.1.1. Any and all NLL Data is and shall remain the sole property of NLL, and Provider shall not acquire any rights or licenses therein except as expressly set forth in the relevant Agreement. Provider shall return to NLL (or at NLL's option, destroy) any and all NLL Data and any other information and materials that contain such NLL Data (including all copies in any form) immediately upon NLL's request, or upon the earlier of the completion of services or termination of the relevant Agreement.

6.2.1.2. Provider shall ensure secure disposal of systems and media to render all NLL Data contained therein as undecipherable or unrecoverable prior to final disposal or release from Provider's possession, This shall be undertaken in accordance with NIST approved standards and within ten (10) days following NLL's request, Provider shall provide NLL with a written certificate of destruction.

6.2.2. Removable Media

6.2.2.1. Use of removable media is prohibited, All ports for USB and external drives must be disabled on all workstations that handle NLL Data.

7. ACCESS CONTROL

7.1. Business requirements of access control

7.1.1. Provider shall implement strong access control and restrict access to operating system configurations to authorized, privileged personnel for systems handling NLL Restricted Data or NLL Confidential Data.

7.1.2. Mobile devices and teleworking

7.1.2.1. Provider shall require that all Personnel who are able to access to NLL Data must use a Provider issued device, excluding mobile phones.

7.1.2.2. Provider shall not allow (and shall restrict), Personnel to access NLL Data via a mobile phone.

7.1.3. User access management

7.1.3.1. Provider shall ensure that the system (Network, Hosting and Application) is designed in compliance with the least privilege principle.

7.1.3.2. Provider shall enforce the use of strong passwords for all systems (Network, Hosting, and Application) as follows:

- Passwords are at least ten (10) characters long
- Contain at least three of the following: Upper-case letters, lower-case letters, numbers, non-alphabetic characters
- Expire after 90 days for all systems
- Are never hard-coded, stored in files, or stored or transmitted in clear text

7.1.3.3. All vendor default passwords within software and hardware products must be changed before or during installation

7.1.4. User responsibilities

7.1.4.1. For administrative accounts, Provider shall use multi-factor authentication or other positive controls such as increased password length, shorter password life or restrictive white lists of users to restrict access to administrative accounts.

7.1.5. System and application access control

7.1.5.1. Provider shall maintain documentation on the applicable application, architecture, process flows and/or data flow diagram, and security features for applications handling NLL Restricted Data or NLL Confidential Data.

8. CRYPTOGRAPHY

8.1. Cryptographic controls

8.1.1. Provider shall use NIST or PCI approved encryption and hashing standards (e.g. SSH, SSL, TLS) for transmission and storage of NLL Restricted Data and NLL Confidential Data.

8.1.1.1. Where necessary to be stored on a laptop, the laptop shall be protected by full disk encryption.

8.1.2. NLL Restricted Data or NLL Confidential Data stored on archive or backup systems shall be subject to at least the same protection measures used in the live environment.

9. PHYSICAL AND ENVIRONMENT SECURITY

9.1. Secure areas

9.1.1. Provider shall ensure the physical and environmental security of all areas containing NLL Restricted Data or NLL Confidential Data, including but not limited to data centers and server room facilities, are designed to:

9.1.1.1. Protect information assets from unauthorised physical and logical access based on role, duties, grade level, geographical location for all Personnel.

9.1.1.2. Manage, monitor and log movement of Personnel into and out of such facilities and all other applicable areas including but not limited to badge access control, locked cages, secure perimeter, cameras, monitored alamars, and enforced use provisioning controls.

9.1.1.3. Guard against environmental hazards such as heat, fire and water damage.

9.1.1.4. Security Personnel deployed to supervise the access to premises, and strict policies to ensure NLL Data is not removed from the premises.

9.1.2. In regards to the data centers, contact centers and server facilities, Provider shall logicaly or physically segregate NLL Data from other customer or tenant's data.

10. OPERATIONS SECURITY

10.1. Operational procedures and responsibilities

10.1.1. Provider shall implement operating system hardening for hosts and infrastructure handling NLL Restricted Data or NLL Confidential Data. Operating system hardening includes, but is not limited to, the following configurations and practices:

- Strong password authentication
- Inactivity time-out
- Disabling unused ports/services
- Log management
- Disabling or removal of unnecessary or expired accounts
- Changing default account passwords and where possible default account names
- Timely patching and updates to firmware, OS and system, application and database level software

10.2. Protection from malware

10.2.1. Provider shall employ and maintain comprehensive anti-malware solutions configured to download signatures at least daily and a firewall solution (or other threat protection technologies) for end user computing devices which connect to the NLL network or handle NLL Restricted Data or NLL Confidential Data.

10.2.2. Provider shall prohibit and disable the use of external devices for storing or carrying, or in use with machines handling NLL Restricted Data or NLL Confidential Data. External devices include without limit: flash drives, CDs, DVD, external hard drives and other mobile devices.

10.3. Logging and Monitoring

10.3.1. Provider shall ensure system audit or event logging and related monitoring procedures are implemented and maintained to proactively record user access and system activity for routine review. All log files shall be retained for at least twelve (12) months and access restricted to authorized personnel only.

10.3.2. Providers who have physical access to NLL Restricted Data or Confidential Data shall maintain logs for all entry points from CCTV, badge readers and sign-in sheets. All log files shall be retained for at least twelve (12) months and access restricted to authorized Personnel only.

10.4. Vulnerability Scanning

10.4.1. Providers who handle NLL Restricted Data or NLL Confidential Data, or host internet accessible sites on behalf of NLL (either directly or through third parties), shall;

10.4.1.1. Utilize industry standard scanning tools to identify network, host and application vulnerabilities.

10.4.1.2. Perform at least monthly internal vulnerability scans of network(s), host(s) and application(s).

10.4.1.3. Perform ad-hoc vulnerability scanning to identify network, host and application vulnerabilities prior to release to production and after significant changes.

10.4.1.4. Remediate all critical, high and medium vulnerabilities according to CVSS scoring, prior to release to production and therafter according to the following vulnerability remediation timeframes:

- Critical/High – 30 days
- Medium – 60 days
- Low – 90 days or prior to the next testing time period

10.4.1.5. For Critical Zero-day vulnerabilities, recommended remedial risk mitigation actions are implemented without undue delay in no event later than the timeframe specified for Critical vulnerabilities in this section. Provider shall promptly implement recommended remedial risk mitigation action, such as applying a software patch, software upgrades, application configuration modifications, or other compensating security preventative control methods, no later than twelve (12) business days after the recommended remedial action has been published, tested and determined safe for installation and use.

10.5. Penetration Testing

10.5.1. Providers who handle NLL Restricted Data or NLL Confidential Data, or have access to the NLL network shall;

10.5.1.1. Utilize an independant third-party to perform an at least annual penetration test of network(s), host(s) and application(s).

10.5.1.2. Utilize an independent third-party to perform ad-hoc penetration tests prior to release to production and no less than thirty (30) days after significant changes.

10.5.1.3. Remediate all critical, high and medium vulnerabilities discovered by the pen-tester , prior to release to production and therafter according to the following vulnerability remediation timeframes:

- Critical/High – 30 days
- Medium – 60 days
- Low – 90 days (or prior to the next testing time period

10.5.1.4. Provide to NLL the executive summary portion of the third party penetration test relating to the network(s), host(s) and application(s).

10.5.1.5. Review the penetration test reports for any appointed subcontractor or fourth-party to NLL, who handles NLL Restricted Data or NLL Confidential Data, or hosts internet accessible sites for Provider on behalf of NLL and notify NLL of their use.

10.5.1.6. NLL reserves the right to independently or utilize an authorized third-party to perform a network penetration test on the area(s) of the Provider's network that handles NLL Restricted Data or NLL Confidential Data, connects to the NLL network, or hosts internet accessible sites on behalf of NLL.

11. COMMUNICATIONS SECURITY

11.1. Network-Level Requirements

11.1.1. Provider shall use firewall(s) to protect networks that handles NLL Restricted Data or NLL Confidential Data or host internet accessible sites on behalf of NLL. The firewall(s) shall be able to effectively perform the following functions: stateful inspection, logging, support for all IPSec standards and certificates, support for strong encryption and hashing, ICMP and SNMP based monitoring and anti-spoofing. Provider shall have network-based security monitoring (i.e., syslog, security information and event management (SIEM) software or host-based intrusion detection systems) for the segment(s) which handles NLL Restricted Data or NLL Confidential Data.

11.1.2. Provider is not permitted to use a Dynamic DNS service for their external facing website IP address. If a static IP address cannot be provided, then a non-Internet-based method of interaction/communication shall be used.

11.2. Hosting-Level Requirements

11.2.1. The Provider shall not use or change a cloud environment in any capacity (i.e., IaaS, PaaS, SaaS, process, transmit, access and store data) without obtaining express prior written consent from NLL. If NLL provides such permission the Provider shall logically segregate all NLL Restricted Data and Confidential Data.

11.3. Information transfer

11.3.1. Provider shall not access, store, process and/or use any NLL Data in a location outside the United States. Additionally, Provider shall ensure that all Personnel who have access to NLL Data are located in the United States. If access or handling is performed outside of the United States additional terms or agreements may be appropriate and Provider agrees to promptly and in good faith enter into such additional terms or agreements as NLL may require from time to time.

12. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

12.1. Security in development and support processes

12.1.1. Providers that develop source code for NLL, handle NLL source code (including without limit any NLL product or service source code), or develop and maintain applications that handle NLL Restricted Data or NLL Confidential Data shall;

12.1.1.1. Deliver at least annual secure code training to all Personnel in-scope for delivering such services to NLL. Developers shall be proficient in the OWASP Top 10 and the CWE/SANS Top 25 vulnerabilities and their appropriate remediation techniques. Provider shall provide NLL with this initial evidence of compliance within thirty (30) days from the effective date of the relevant Agreement between NLL and Provider and annually thereafter.

12.1.1.2. Maintain and evidence an annual review of a documented Change Management process and Software Development LifeCycle (SDLC) , which includes:

- Independent secure code reviews
- Secure programming guidelines and protocols for developing applications
- Threat model methodology to identify the key risks to applications and/or source code
- Application security testing (Testing may include Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) and third-party penetration testing)

12.2. Test Data

12.2.1. Provider may never use NLL Data for any testing scenarios.

13. SUPPLIER RELATIONSHIPS

13.1. Information security in supplier relationships

13.1.1. Providers that either connect to any NLL network, handle NLL Restricted Data or NLL Confidential Data and/or develop or host internet assessable sites on behalf of NLL, shall ensure that they maintain an applicable SOC 2 Type 2 attestation and/or, ISO/IEC27001 certification. Provider shall provide NLL with a copy of the SOC 2 Type 2 report, and/or ISO27001 Statement of Applicability with certificate.

13.1.2. Providers who cannot provide an applicable attestation or certification as stated above, are required to undertake a NLL's Security Risk Assessment (SRA) and/or provide a SIG LITE. on an annual basis.

13.1.3. NLL is a PCI Level 1 merchant. Any Provider who handles credit card data on behalf of NLL, shall at all times remain in compliance with the most recent version of Payment Card Industry Data Security Standard (PCI DSS) to the extent PCI DSS is applicable to the services provided under the Agreement (e.g., if Provider accesses, collects, uses, retains, processes, discloses or transfers any cardholder data as defined under PCI DSS or any other data protected or subject to PCI DSS (collectively, "PCI Data"), or if any part of such services impacts the security of the PCI Data environment). Upon request by NLL, Provider shall promptly provide sufficient proof, as determined by NLL in its sole discretion, of compliance with PCI-DSS to NLL. If Provider has knowledge of a potential violation of PCI DSS, Provider shall notify NLL promptly, but no later than 48 hours, after obtaining such knowledge and come into compliance with PCI DSS within the time frame specified by NLL, but no later than 30 days, after Provider obtains knowledge of such violation. Provider shall ensure that all of its Personnelcomply with the same obligations that apply to Provider under the Agreement and remain liable to NLL for compliance with the Agreement by its Personnel. Provider shall provide NLL with this initial evidence of compliance (PCI AoC) within thirty (30) days from the effective date of the relevant Agreement between NLL and Provider and annually thereafter.

13.1.4. Where Provider or its Personnel have a reasonable belief that NLL Data may have been compromised, including without limit any unauthorized handling, NLL may conduct an SRA on three (3) days' notice at the Supplier's expense. Provider shall provide prompt, full and good faith cooperation in the performance of the SRA.

13.1.5. Provider and its Personnel shall fully cooperate with any NLL or NLL appointed third party auditors, including any regulatory investigation of NLL or its affiliates, and shall allow access to any (i) Personnel involved in performance of the services or handling of NLL Data, (ii) premises where the services are being performed; (iii) applications and systems used to perform the services; (iv) data and records kept or created with respect to the services or any agreement in place between Provider and NLL and/or Provider and its Personnel.

13.1.6. NLL Restricted Data or Symatec Confidential Data shall not be shared with any other third party without prior written agreement from NLL.

13.2. Right to Audit

13.2.1. In addition to NLL's inspection and audit rights as set forth in any relevant Agreement, NLL reserves the right to require the Provider to undertake a NLL Security Risk Assessment at least annually. If Provider fails to comply with such request within a reasonable timeframe, or if the security questionnaire raises NLL security concerns that are not addressed by Provider to NLL's satisfaction, NLL reserves the right (in addition to any other audit or other rights it may have) to conduct, or engage a reputable third party auditor to conduct an SRA.

14. INFORMATION SECURITY INCIDENT MANAGEMENT

14.1. Management of information security incidents and improvements

14.1.1. Provider shall notify NLL immediately, and in no event later than twenty-four (24) hours, if there is a reasonable basis to believe that NLL Restricted Data or Confidential Data may have been compromised, including without limit any unauthorized handling.

14.1.2. Provider shall inform NLL of the following;

14.1.2.1. A description of the nature of the incident including, where possible, the categories and approximate scale of the incident;

14.1.2.2. The name and contact details of the Provider contact from whom more information can be obtained; and

14.1.2.3. A description of the measures taken or proposed to be taken to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

14.1.3. Provider shall work with NLL promptly and in good faith as required to resolve the incident, and in conjunction with any associated investigations.

15. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

15.1. Information security continuity

15.1.1. Provider agrees to maintain a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) (the "Plans") with respect to the services being performed for NLL.

15.1.2. The Plans must be tested at least annually, a copy may be requested by NLL, and all findings shall be remediated.

15.1.3. At a minimum the Provider's Plans must include the following requirements:

15.1.3.1. Business Continuity Plan (BCP). The Provider must maintain a BCP for their essential business functions. A BCP must contain the information necessary to plan for the recovery of each essential business functions. BCPs must document the requirements necessary to execute the recovery strategy. BCPs must include strategies to achieve the essential business function recovery timelines determined in the associated Business Impact Analysis. The BCP must include the following information:

- Executive Summary:
  - Plan Overview, including the plan specific recovery objectives
  - Scope
  - Assumptions
  - Business Impact Assessment (BIA)
- Recovery Strategy Details and Recovery Procedures for each of the following effects:
  - Loss of Facility
  - Loss of Critical Personnel
  - Loss of Core Dependencies
- Notification, Escalation and Plan Activation Procedures
- Calls Lists
- Recovery Resource Requirements

15.1.3.2. Disaster Recovery Plan (DRP). Except to the extent superseded by more stringent standards included in the Agreement, the following shall apply;

- Provider shall provide NLL with a DRP relevant to any site, network, system, and/or application used to host NLL websites and data within thirty (30) days of the request.
- DRPs shall include procedures to achieve a Recovery Time Objective (RTO) of four (4) hours or less and Recovery Point Objective (RPO) of no more than one (1) hour.

15.1.3.3. Internet Service Providers. Provider shall maintain at least two Internet Service Providers ("ISPs") with multiple paths into the building and traffic shall automatically be rerouted to another carrier.

15.1.3.4. Fire. Provider's facilities shall contain an automated fire suppression system that will not affect any of the equipment or systems but will immediately extinguish a fire.

15.1.3.5. Bandwidth. Provider shall maintain two identical routers and an alternate firewall server. The back up router and firewall shall be pre configured and able to be brought online immediately.

15.1.3.6. Power. Provider's service facilities shall have multiple sources of power including heavy-duty utility feed, extensive Uninterrupted Power Supply (UPS) battery backup, surge protectors between power feed and UPS, and a back-up generator.

15.1.3.7. Server Failure. Provider's system shall be redundant to a reasonable degree necessary to meet up time and maintenance requirements.

15.1.4. Upon Provider's determination of a disaster as defined in the Plan, Provider shall immediately notify NLL and commence the activities for which it is responsible under the Plan. If Provider materially breaches its obligations to provide disaster recovery services in accordance with this Section, and, as a result thereof, fails to commence performance of services critical to the operation of NLL's business within the proscribed period, NLL shall have, in addition to any other rights of NLL hereunder, the right to retain a third party to provide such services for so long as the disaster continues, at Provider's expense. Upon cessation of a disaster, Provider shall as soon as reasonably practicable, provide NLL with an incident report detailing the reason for the disaster and all actions taken by Provider to resolve the disaster.

EXHIBIT C
DATA PROCESSING ADDENDUM

WHEREAS NortonLifeLock Inc. and/or its affiliates ("NLL") has procured from Provider certain products and/or services under the Agreement that involve the processing of Personal Data by Provider.

WHEREAS in this context, NLL acts as "Controller" and Provider acts as "Processor" with respect to the Personal Data or as the case may be, NLL acts as a "Processor" for its end customers including its affiliated companies (as ultimate Data Controllers) and Provider acts as a "Sub-Processor" acting on the instruction of the NLL vis-a-vis its end customers.

The parties agree as follows:

1. **Definitions**. Unless otherwise defined in the Agreement, all capitalized terms used in this Addendum will have the meanings given to them below. If any definitions set forth herein or in the Agreement conflict with statutory definitions provided in any applicable Data Protection Law, the definition in the Data Protection Law shall control.

   "**Applicable EU Legislation**" means the (i) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (ii) as of 25 May 2018, the then applicable General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR") and, (iii) any applicable EU Member State Legislation.
   "**Controller**" means the party which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
   "Data Protection Law(s)" means the Applicable EU Legislation and any other data protection laws which may be applicable to the Personal Data Processed under the Agreement.
   "**EEA**" means the European Economic Area.
   "**Personal Data**" and "Data Subjects" have the same meanings as set forth in the Agreement.
   "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
   "Process" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
   "**Processor**" has the same meaning as set forth in the Agreement.
   "**Services**" means the services as described in the Agreement.
   "**Standard Contractual Clauses"** means those clauses specified pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the Directive, a form of which is attached hereto as Annex 1.

2. **Compliance with Laws**. Each party will comply with the Data Protection Laws as applicable to it. In particular and without limiting the foregoing, NLL will comply with its obligations as Controller and Provider will comply with its obligations as Processor as set out in the Applicable EU Legislation. To the extent required by any Data Protection Law(s), the parties agree to negotiate in good faith and execute any such additional, supplemental or revised documents pertaining to the Processing of Personal Data as reasonably necessary for the provision of Services under the Agreement.

3. **Data Processing.** Provider shall not Process Personal Data other than on the relevant documented instructions from NLL or its Affiliates unless Processing is required by applicable Data Protection Laws to which the Provider is subject, in which case Provider or the relevant Provider Affiliate shall to the extent permitted by applicable Data Protection Laws inform NLL of that legal requirement before the relevant Processing of that Personal Data. Each of NLL and its relevant Affiliates instructs Provider and each Provider Affiliate (and authorizes Provider and each Provider Affiliate to instruct each of its Subprocessor) to: i) Process Personal Data as part of the Services; and ii) in particular, transfer Personal Data to any country or territory, as reasonably necessary for the provision of the Services but always in compliance with the express terms herein and in the Agreement. NLL warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in this Section 3 on behalf of itself and each of its relevant Affiliates.

   The parties will describe in each applicable Statement of Work, the nature, purpose, duration and subject matter of Personal Data processing including the categories of Personal Data and Data Subjects and, if relevant, the list of Sub-processors processing Personal Data as part of the Services, as well as the location of the processing activities by the Provider and, if applicable, by each subprocessor.

4. **Provider Employees/Agents.** Provider will restrict access to Personal Data solely to those employees and agents who require such access to perform the Agreement, and Provider covenants and agrees that those employees/agents to whom it grants access to such Personal Data are or shall be: i) directed to keep such Personal Data confidential; and, ii) subject to written confidentiality obligations consistent with this Addendum and applicable Data Protection Laws. Upon termination of any employee or agent, Provider shall prohibit access to Personal Data and/or any systems that process Personal Data by the terminated employee/agent.

5. **Data Subjects Rights and Controller Assistance.** Provider shall notify NLL of any request received from a Data Subject(s) or any other party in regard to NLL Personal Data. Provider will not respond to such requests except on the documented instructions of NLL or as required by applicable Data Protection Law, in which case Provider shall to the extent permitted by such law inform NLL of that legal requirement before the Provider responds to the request. Provider will reasonably assist NLL with any obligations it may have to comply with Data Protection Laws including, but not limited to, NLL's obligations to respond to Data Subject requests and in regard to transparency and fulfilment of Data Subject rights.

6. **Technical and Organizational Security Measures.** Provider shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in applicable Data Protection Laws (e.g. Article 32(1) of the GDPR). Without limiting the foregoing, Provider agrees to implement the security measures set out in **Exhibit B** of the Agreement.

7. **Audit of Technical and Organizational Security Measures.** Upon NLL's request, Provider agrees to make available all information necessary to demonstrate compliance with data protection policies and procedures implemented as part of the Services applicable under the Agreement including, but not limited to, Provider's then-current audit results, certifications and attestations (e.g ISO 27001, SOC2 TYPE2). In the event that NLL, a third-party data controller or processor under obligations of applicable Data Protection Laws, a data protection authority or regulator requires additional information or physical access to Provider's personnel, data, systems or facilities for audit purposes, such access shall be made available under an agreement of confidentiality, in accordance with the audit/access provisions set forth in Exhibit B.

8. **Data Breach Notification and Remediation.** Provider will notify NLL without undue delay (and, in all cases, not later than 24 hours) if there has been a Personal Data Breach. Provider will send all notification of known or suspected breach of Personal data to: security@nortonlifelock.com

   Provider shall provide NLL all reasonably required support and cooperation necessary to enable NLL to comply with its legal obligations in case of a Personal Data Breach (including, without limitation, articles 33 and 34 of the GDPR). In addition, Provider shall, as soon as reasonably possible, take all action reasonably necessary, at Provider's sole cost and expense, to determine the root cause of the Personal Data Breach and prevent any other or further unauthorized access, use or processing of Personal Data. Provider shall provide full and prompt cooperation and support as requested by NLL, including but not limited to making available applicable logs, systems, and key personnel with sufficient knowledge to resolve or mitigate any data privacy or security issues involving Personal Data, determine the scope of the incident, investigate the incident, prepare a written summary and assist in taking any additional corrective or responsive action, including but not limited to all assistance reasonably necessary to provide notification to regulators and/or announcement to affected Date Subjects and the public as required by Data Protection Laws and/or determined by NLL. Except and only to the extent expressly required by law or pursuant to third-party agreements, Provider agrees that it will not inform any third party that NLL Personal Data has been involved in a Personal Data Breach without NLL's prior written consent. If Provider is compelled by law or third party agreement(s) to provide public/third-party notification of a Personal Data Breach, Provider will not identity NLL (directly or indirectly), and will use commercially reasonable efforts to obtain NLL's prior approval regarding the content of such disclosure to minimize any adverse impact to NLL, and its respective customers and/or employees. NLL may suspend or terminate the access, processing, or storage of Personal Data by Provider, or take other appropriate action, pending resolution of any known or suspected Personal Data Breach.

   Provider will defend, indemnify and hold harmless NLL and its agents, assigns and successors-in-interest against any and all third-party claims, suits, actions, proceedings or demands and judgments, losses, payments, costs, expenses (including related to investigation, technical third parties or reasonable attorneys' fees), damages, settlements, liabilities, fines or penalties of NLL, arising from or relating to Personal Data Breach caused by Provider's breach of the terms herein. In addition to and without limiting the foregoing or any other rights or remedies available to NLL at law or equity, Provider will reimburse NLL in full for all actual costs, expenses, and liabilities incurred by NLL as a result of a Personal Data Breach caused by Provider, including, but not limited to, the costs or expenses incurred by NLL related to the investigation and remediation of such Personal Data Breach and the costs and expenses incurred in providing any notices and/or ongoing credit monitoring to Data Subjects whose information may have been subject to a Personal Data Breach.

9. **Sub-Processing.** Provider must obtain NLL's prior written consent before it engages third party providers as Sub-Processors of Personal Data to support or enable the provision of Services. Subject to and without limiting the foregoing, NLL, on behalf of itself and its relevant Affiliates, consents to the use of Sub-Processors identified specifically in **Annex 1** hereto. For any new Sub-Processors appointed during the term of the Agreement, Provider shall provide NLL notice at least forty-five (45) days prior to allowing Sub-Processor access to Personal Data hereunder. NLL may object to a new Sub-Processor within sixty (60) days of receipt of the notice. If NLL objects to a new Sub-Processor in accordance with the above, Provider will use commercially reasonable efforts to change the Services to ensure that NLL Personal Data is not processed by the new Sub-Processor in question. If Provider is unable to make such a change, NLL may terminate the applicable Services by providing written notice in accordance with the terms of the Agreement. In case of termination of Services pursuant to this section, Provider will issue a pro-rated refund for any unused prepaid fees.

   Provider will restrict the Processing activities performed by Sub-Processors to only what is strictly necessary to provide the Services.
   Provider will impose appropriate contractual obligations in writing upon the Sub-Processors that are no less protective than this Addendum and Provider will remain responsible for its compliance with the obligations under this Addendum.

10. **Transfers/EEA+ Data Processing.** Provider shall only process Personal Data at the locations set out in **Annex 1** hereto and shall not transfer Personal Data across country borders unless Provider has obtained prior written authorization from NLL. The Provider will advise NLL of any changes to those agreed transfers and must obtain NLL consent to any such changes. If applicable and with respect to Personal Data originating from the European Economic Area or Switzerland (EEA+) that Provider may process under this Agreement and transfer outside the EEA+, the parties will document the details of the processing in the Agreement, and hereby agree that the terms of the EU Standard Contractual Clauses shall govern such transfer(s) between each relevant NLL Affiliate and Provider, as attached in **Annex 2** hereto. In the event that such transfer mechanisms are no longer deemed adequate, the Provider agrees to execute any legitimate data transfer mechanism as NLL may deem appropriate to protect data being transferred outside the EEA+. Subject to Section 9 above and if required by the Applicable EU Legislation, should Provider transfer EEA+ Personal Data to a Sub-Processor located in any country that may have less protective data protection laws than the EEA+, Provider shall execute EU Standard Contractual Clauses in the form provided in Annex 2 as between such Sub-Processor and Provider acting on behalf of NLL, unless the transfer of such Personal Data occurs via an alternative means permitted by Applicable EU Legislation.

11. **Data Protection Impact Assessment and Prior Consultation.** Provider shall provide reasonable assistance to NLL in regard to data protection impact assessments, and prior consultations with regulators or supervising authorities or other competent data privacy authorities, which NLL reasonably considers to be required by any applicable Data Protection Laws, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, the Provider.

12. **Compliance.** Provider shall monitor compliance with these terms and ensure that its personnel, agents and Sub-Processors are suitably qualified, trained and accountable for their actions with regard to processing Personal Data. Provider shall ensure that, to the extent permitted by applicable law, adequate background checks and reviews are completed with respect to individuals having access to Personal Data prior to such access being given. Provider must inform and train its personnel, agents and Sub-Processors who are responsible for processing and protecting Personal Data about privacy laws and regulations and about the obligation to protect Personal Data in accordance with the requirements of this Agreement. Provider further agrees that upon termination of any personnel, agent or Sub-Processors, access to Personal Data and to any systems processing Personal Data will be terminated immediately.

13. **Return or Deletion of Personal Data.** Provider will, upon receiving NLL's written request, delete or return, as specified by NLL, Personal Data within a reasonable period of time. Upon NLL's request, Provider will provide a written certification of its compliance with these provisions, in accordance to Exhibit B (Master Provider Security Requirements).

14. **Order of Precedence.** If there is a conflict between the Agreement and this Addendum, the terms of this Addendum will control.

Attachments:

Annex 1 – Standard Contractual Clauses, with Appendices 1 and 2

Annex 1

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The data exporting organisation is NortonLifeLock Inc. or its relevant Affliate(s)Address: .....

Tel.: .....; fax: ; e-mail:

(the data **exporter**)

And

Name of the data importing organisation is the Provider or its relevant Affilaite as expressly identified in the Agreement (or any Statement of Work or Order

executed thereunder). Address:.....

Tel.:.....; fax: .....; e-mail: .....

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1 hereto.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses1. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

On behalf of the data importer:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties or alternatively the details of the Personal Data processing will be as set forth in the applicable statement of work or order form.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

……

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

……

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

……

Categories of data

The personal data transferred concern the following categories of data (please specify):

……

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

……

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

……

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER

Name:……

Authorised Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):
See Exhibit A of the Agreement.