

This Data Protection Policy ("Policy") is incorporated into the Agreement. Capitalized terms used in this document without definition herein have the meanings ascribed to them in the Agreement between LGEUS and Vendor, as defined in the Terms and Conditions or in the Master Services Agreement.

1.0 Definitions

- 1.1 "Authorized Employees" means Vendor Personnel who need to access Sensitive Information to enable Vendor to perform its obligations under this Agreement.
- 1.2 "LGE Data" means all information and data that is, in relation to the Agreement: (i) provided by or on behalf of LGEUS, its affiliates, employees, customers, or its users to Vendor; (ii) obtained, developed, produced or processed by Vendor (including its sub-processors) by or for the benefit of LGEUS or its affiliates; (iii) derived based on the information described in (i) or (ii). Notwithstanding the foregoing, LGE Data excludes any data or information expressly defined as owned by Vendor in the Agreement and which is not subject to any restrictions on use or disclosure.
- 1.3 "Safeguards" has the meaning assigned in Section 3.3.
- 1.4 "Security Incident" means a confirmed or reasonably suspected intentional or unintentional unauthorized Event that affects or is likely to affect the security of LGEUS's systems or networks or the confidentiality, integrity or availability of LGE Data.
- 1.5 "Sensitive Information" means LGE Data that includes (i) any Personal Information (as defined in the LGEUS Data Processing Addendum and (ii) Confidential Information (as defined in the Agreement).
- 1.6 "Vendor Personnel" means wage-earning or contracted staff engaged or employed by Vendor or a Vendor sub-processor or subcontractor, including officers, partners, principals, employees, agents, or independent contractors.

2.0 Use of LGE Data

- 2.1 As between LGEUS and Vendor, LGE Data is and will remain the exclusive property of LGEUS. Vendor may only access, use, collect, maintain, disclose, or share LGE Data in manners explicitly permitted by the terms of this Agreement and only to the extent strictly necessary to perform its obligations under this Agreement or as otherwise required by law.
- 2.2 Vendor may not modify, aggregate, analyze, commercially exploit, disclose, or otherwise use LGE Data other than as expressly specified in this Agreement or as LGEUS specifically directs in writing.
- 2.3 LGEUS makes no representation or warranty as to the accuracy or completeness of LGE Data. Vendor agrees that LGEUS, its employees, contractors, and agents will have no liability to Vendor resulting from any use of LGE Data.
- 2.4 Vendor agrees to return, or at the election of LGEUS, destroy (and certify in writing the destruction) all LGE Data within thirty (30) days of termination or expiration of this Agreement, or earlier if requested to do so in writing by LGEUS.
- 2.5 Vendor agrees that its collection, access, use, storage, and disclosure of Sensitive Information will comply with (i) the LG Data Processing Addendum, (ii) applicable federal, state and local, foreign, and international law, (iii) the FCC's Customer Proprietary Network Information ("CPNI") rules and regulations implementing 47 U.S.C. § 222, (iv) Vendor privacy policies, (v) rules of any applicable self-regulatory organizations in which the

Vendor is or has been a member or that the Vendor has been contractually obligated to comply with (e.g., Payment Card Industry Data Security Standard); or (vi) industry standard practices. For purposes of its obligations under this Policy, the acts or omissions of Vendor Personnel, agents, representatives, contractors, subcontractors, or Vendor affiliates will also be considered the acts or omissions of Vendor.

3.0 Vendor Personnel

- 3.1 Vendor shall maintain a “zero trust” environment where only Authorized Employees will have access to Sensitive Information and only to the extent necessary to perform their responsibilities under the Agreement.
- 3.2 Vendor shall ensure that all Authorized Employees pass a background check and are bound in writing to obligations of confidentiality sufficient to protect Sensitive Information in accordance with the terms of this Data Protection Policy.
- 3.3 Vendor shall ensure that all Authorized Employees receive appropriate training on matters relating to data security and limitations upon the use and disclosure of Sensitive Information upon hire and at least once per year thereafter. Upon request, Vendor shall provide a copy of all training materials presented over the past twelve (12) month period and documentation of attendance.
- 3.4 Upon written request of LGEUS, Vendor will promptly identify all Authorized Employees in writing. During the term of each Authorized Employee’s employment by Vendor, Vendor will at all times cause the Authorized Employee to strictly abide by its obligations under this Policy and, after the termination of employment, Vendor will use the same efforts to enforce the confidentiality obligations of the Authorized Employee as Vendor uses to enforce obligations with respect to its own similarly confidential information, provided that Vendor will not use less than reasonable efforts in its enforcement.
- 3.5 Vendor shall maintain a disciplinary process to address any unauthorized access, use, or disclosure of LGE Data by any Vendor Personnel.
- 3.6 Vendor shall eliminate access to Sensitive Information once Authorized Employees no longer have a need to know the Sensitive Information (e.g., terminate passwords).
- 3.7 Vendor shall not assign individual Authorized Employees for whom accepting work with LGEUS would constitute an obligation inconsistent or incompatible with the individual personnel’s obligations, or the scope of services to be rendered for Vendor, under this Agreement.
- 3.8 Upon request, Vendor shall require Authorized Employees to execute individual non-disclosure agreements with LGEUS, upon LGEUS request.

4.0 Safeguards

- 4.1 Vendor shall establish and maintain organizational, technical, physical, environmental, and other safeguards sufficient to prevent unauthorized access or damage to LGE systems and ensure the confidentiality, integrity, and availability of LGE Data in possession of Vendor and during the access, transmission, and storage.
- 4.2 Vendor shall follow a security framework no less rigorous than (i) specified in Vendor’s data security policies; (ii) set forth in this Data Protection Policy, including its Attachment 1 (Security Measures); (iv) industry standard practices; and (v) practices required by law, whichever requires the strictest controls (collectively, “Safeguards”). At a minimum, and not in lieu of the foregoing obligations, Vendor shall take the following measures:
 - (a) implement and maintain a comprehensive information security program that, at a

minimum, designates one or more employees to maintain such comprehensive information security program and includes written policies;

- (b) identify and assess internal and external risks to security, confidentiality, or integrity of Vendor systems and data in the possession or control of Vendor, including LGE Data;
- (c) develop policies for the storage, access, and transportation of records containing LGE Data outside of Vendor premises;
- (d) impose disciplinary measures for violations of Vendor's security program; and
- (e) monitor and assess Vendor's security measures at least annually and document vulnerabilities identified, and responsive actions taken.

4.3 Vendor shall implement—and require its subcontractors and sub-processors to implement—industry-standard user access management tools, including, at a minimum, multi-factor authentication and single sign-on with respect to any system(s) that contain or transmit LGE Data.

4.4 Vendor shall only store account passwords and answers to account security questions using secure, industry-standard cryptographic means (e.g., hashing), and in no event store account passwords and answers to account security questions in human-readable plaintext.

5.0 Secure Coding

5.1 All software, hardware, hosted computing services, tools, or processes provided by Vendor to LGEUS (collectively "Work Products") will be free of hidden features and security defects. No component of any Work Product will include any viruses, worms, time bombs, trojan horses or other harmful or malicious code, files, scripts, agents or programs ("Malicious Code"). Vendor shall not transmit to LGEUS, or cause any LGEUS system to be exposed to, Malicious Code. Vendor shall notify LGEUS in writing and in reasonable detail immediately upon becoming aware of the existence of any malicious code contained in a deliverable. If any Work Product contains Malicious Code, or if Vendor transmits any Malicious Code to an LGEUS system or causes any LGEUS system to be exposed to Malicious Code, Vendor shall cooperate with LGEUS, at Vendor's expense, to promptly remove the Malicious Code and repair any corrupted files or data.

6.0 Security Incident Response

6.1 If Vendor becomes aware of a Security Incident, Vendor shall notify LGEUS without undue delay, but no later than twenty-four (24) hours of becoming aware of the Security Incident.

6.2 When providing notice of the Security Incident, the notice will summarize in reasonable detail the nature and scope of the Security Incident (including the nature of the data and whether data subjects are impacted) and the corrective action already taken or to be taken by Vendor. The notice will be timely, supplemented in reasonable detail, and inclusive of relevant forensic reports. Unless prohibited by an applicable statute or court order, Vendor shall also notify LGE of any third-party legal process relating to any Security Incident, including, but not limited to, any legal process initiated by any governmental entity.

6.3 Vendor shall not notify any third party that a Security Incident involves or may impact LGEUS without prior consent from LGEUS.

6.4 Vendor shall undertake all action necessary, at its own expense, to contain, mitigate and remediate the Security Incident, minimize any adverse impact on LGEUS, and cure any failure to comply with the obligations of this Policy. Vendor shall, at Vendor's cost, provide

sufficient support for LGEUS to investigate the Security Incident, contain, mitigate, and perform remediation activities, if necessary.

- 6.5 Vendor shall provide LGEUS with assurance satisfactory to LGEUS that such Security Incident will not recur and provide regular updates of security concerns of which Vendor becomes aware that may have an adverse effect on LGEUS (including any LGEUS affiliates). Vendor will thereafter provide LGEUS with a written action plan satisfactory to LGEUS that addresses such security concerns.
- 6.6 Without limiting any other rights or remedies of LGEUS, if in connection with any Security Incident or any act or omission of Vendor or any Vendor Personnel, notice to any individuals, legal authorities, or other third parties of any actual or suspected unauthorized access to or use of Sensitive Information, or of any other event or circumstance requiring such notice, is required under any law applicable to LGEUS or Vendor, or LGEUS otherwise determines in its sole discretion that notice of such event or circumstance is reasonably necessary (each, a "Notification Event"), Vendor will (i) assist LGEUS in notifying such third parties of the Notification Event, and communicating with and assisting such third parties regarding the Notification Event; and (ii) if requested by LGEUS, provide notice of the Notification Event to all persons and entities as may be requested by LGEUS. The content of any statements, communications, notices, filings or reports by or for Vendor related to any Notification Event, including those required by law, must be provided to LGEUS within a reasonable time before any publication or release. All disclosures, filings, public statements, press releases, and notifications by or for Vendor that relate to any Notification Event that either (i) Vendor intends to be available to LGEUS users, customers, or employees, or (ii) reference LGEUS in any manner, must be approved by LGEUS prior to release. Vendor will be responsible for any costs of LGEUS in connection with any notification to third parties or any other activities relating to any Data Incident or Notification Event, including costs of notifying consumers or other third parties, providing call center services, providing credit monitoring services, and taking other steps to mitigate or remediate the effects of any Security Incident or Notification Event.

7.0 Location of Vendor Operations

- 7.1 Vendor shall ensure that all Sensitive Information resides in the United States without the express permission of LGEUS. If, in the sole and reasonable determination of LGEUS, LGEUS is required by law to limit access to or use or disclosure of other LGE Data within the United States, the parties will cooperate in good faith to comply with such requirements and to ensure that LGEUS is not in violation of any laws or requirements. If the parties cannot come to a mutually agreed-upon resolution, LGEUS may terminate any or all open SOWs without liability.

8.0 Remedies for Breach/Indemnity

- 8.1 Vendor agrees that a breach of any obligation set forth in this Exhibit by Vendor may result in irreparable harm for which monetary damages may not provide a sufficient remedy. As a result, LGEUS will be entitled to both monetary damages and equitable relief. Vendor further agrees that, without limiting any of its other rights or remedies under the Agreement or at law, LGEUS will have the right to immediately terminate all open SOWs without liability upon written notice if Vendor breaches any of its obligations under this Exhibit.
- 8.2 Vendor agrees to indemnify and defend LGEUS, including its parent, subsidiaries, and LGEUS Affiliates, and each of their respective officers, shareholders, directors, and

employees, from and against any Damages arising out of or relating to Vendor's performance of its obligations under this Exhibit. Vendor's indemnification obligations under this Exhibit will not be limited by any provisions limiting Vendor's liability under this Agreement (including any disclaimer of liability for consequential, incidental, exemplary, punitive, or special damages). Vendor agrees that, without limiting any of its other rights or remedies under the Agreement or at law, LGEUS will have the right to terminate all open SOWs without liability upon written notice if of breach by Vendor of any of its obligations under this Policy.

9.0 Audits

- 9.1 Vendor shall engage a third-party internationally recognized audit firm ("Auditor"), at Vendor's own cost, to perform periodic audits, scans, and tests as follows at least once per year and after any Security Incident that occurs during the term and at the request of LGEUS ("Audit Reports"):
- (a) ISO 27001, SSAE 18/SSAE 16/SOC-1, Type II audit and a SOC-2, Type II audit of Vendor's controls and practices relevant to security, availability, integrity, confidentiality and privacy of LGEUS Data;
 - (b) a network-level vulnerability assessment of all Vendor systems used to deliver the Services; and,
 - (c) a risk assessment, which may include but is not limited to a formal penetration test of all systems used to provide the Services.
- 9.2 In addition to Vendor's provision of Audit Reports to LGEUS, LGEUS, through its authorized representative, will have the right no more than once per year during the term during reasonable business hours and upon reasonable notice, to perform an operational audit of Vendor's compliance with its obligations under the Agreement.
- 9.3 If LGEUS has a good faith belief based on specific facts that Vendor's privacy practices and standards may not be in compliance with its obligations under this Policy, LGEUS will have the right to conduct an audit through its authorized representative regardless of whether LGEUS already conducted an audit during the year.
- 9.4 In addition to the audit rights set forth in the Agreement, and for purposes of audits performed pursuant to this Policy, Vendor will grant LGEUS representatives all relevant access to Vendor's books (to the extent the books contain LGE Data), facilities, procedures, and records as they may be reasonably required in order to ascertain facts directly relevant and necessary to verify that Vendor's privacy practices and standards comply with its obligations under this Policy. In no event will this access include Vendor's financial books (such as ledgers, income statements, balance sheets, or cash flow statements), records that show Vendor cost information, return rates, product performance information, product engineering information, or information owned by a third party, unless the documents contain LGE Data. If the documents include LGE Data, information relating to Vendor's cost, profit and loss, or any third-party information protected by a nondisclosure agreement with Vendor will be redacted. Unless the privacy audit relates to an issue where LGEUS has a good faith concern or obligation to urgently obtain information regarding Vendor's compliance with its obligations pursuant to this Exhibit, LGEUS will provide the specific scope of the scheduled audit with a list of specific information, if available, to be reviewed and a good faith summary of the types of information within the scope that may be requested during the course of the audit within ten (10) days of the scheduled audit.

Vendor will provide authorized representatives of LGEUS with this information and assistance as reasonably requested to perform the audits.

- 9.5 If the parties agree that any audit pursuant to this Exhibit reveals an inadequacy or insufficiency of the Vendor's privacy practice and standards, then Vendor shall promptly develop and provide to LGEUS a corrective action plan that must be reasonably satisfactory to LGEUS and promptly implement the plan at Vendor's sole cost and expense. In this event, LGEUS, through a third-party auditor as provided above, may perform one or more additional follow-up audits to verify performance under the corrective action plan (and to examine any areas potentially affected by the action plan) without regard to the time limitations set forth above.

10.0 Miscellaneous

- 10.1 Vendor shall flow down (i.e., require such sub-processors and subcontractors) to perform all material obligations, representations, covenants, warranties, and requirements of, or applicable to Vendor as set forth in the Agreement and this Policy. Flow downs will include the requirement that sub-processors and subcontractors secure consent from each Authorized Employee to perform a background check. For the avoidance of doubt, Vendor shall be responsible for the sufficiency of the security, privacy, and confidentiality safeguards of all sub-processor and subcontractor personnel and liable for any failure by such personnel to meet the terms and conditions of this Policy.
- 10.2 LGEUS may, from time to time, provide Vendor with reasonable written guidelines, rules, and/or procedures for accessing, using, storing, and handling Sensitive Information or LGEUS equipment, systems, or facilities, and updates thereto ("Special Privacy and Data Protection Procedures"). Vendor will comply with all applicable Special Privacy and Data Protection Procedures when accessing Sensitive Information, equipment, systems, or facilities. Vendor will make Special Privacy and Data Protection Procedures available to all relevant Vendor Personnel and will provide an appropriate level of supervision and training to relevant Vendor Personnel on the procedures required by the Special Privacy and Data Protection Procedures.
- 10.3 If LGEUS reasonably determines that (a) Vendor is likely to fail to perform its privacy or security obligations under this Agreement or (b) Vendor's access to Sensitive Information creates a material risk to the security, privacy, or confidentiality of LGE Data, LGEUS may require Vendor to demonstrate compliance and provide a cure plan. Notwithstanding any other provision of the Agreement, LGEUS may, in its sole discretion, without penalty of any kind to LGEUS, and without limiting any other rights or remedies of LGEUS under the Agreement, (i) work with Vendor to implement alternative processes and controls that reasonably address or resolve the failure, (ii) suspend or terminate Vendor's access to LGE Data and systems until the matter is resolved, and/or (iii) immediately terminate the Agreement in part or in whole.
- 10.4 The obligations set forth in this Policy will survive the termination or expiration of this Agreement for any reason. The provisions in this Exhibit relating to Sensitive Information will govern all privacy, security, and confidentiality obligations with respect to Sensitive Information to the extent there is any conflict between it and other provisions of this Agreement. As may be requested by LGEUS from time to time, Vendor will provide assurances in writing that it has implemented all requirements set forth in this Policy.

ATTACHMENT 1**Security Measures****A. Workstation Configuration**

1. Vendor shall ensure that Vendor Personnel does not process or store LGE Data on any device or machine except secured workstations (including desktop and laptop PCs) (i) provided by Vendor or (ii) provided by LGEUS. Vendor shall not permit Vendor Personnel to store or use LGE Data on personal devices under any circumstances.
2. All Vendor-provided workstations used to process or store LGE Data must be protected with the following precautions: (i) workstations must meet the requirements laid out in either the Federal Desktop Core Configuration (FDCC) security configuration (<http://nvd.nist.gov/fdcc/index.cfm> or <http://csrc.nist.gov/publications/nistpubs/800-70-rev1/sp800-70r1.pdf>) or USGCB Version 1.2 or higher; (ii) workstations must be located in a physically secure location, e.g., a location secured by the use of a badge reader, key, or appropriate security guard; (iii) workstations must lock automatically after 15 minutes of inactivity (i.e., require login); (iv) application and operating system patches and service packs must be kept up to date, either automatically or via a centrally controlled process, and must not, under any circumstances, be more than 30 days out of date; (v) a real-time virus scanner must be installed and running; signature files must be kept up to date; the virus scanner must run daily scan of the workstation; (vi) a host firewall must be enabled ('built-in' OS firewalls are acceptable, for example Windows XP/Vista or Mac OS X firewalls) and configured to be as restrictive as the environment allows; (vii) workstations must be configured to prevent other computers from accessing LGE Data remotely (i.e., workstations must not act as servers); (viii) an anti-malware solution must be active; signature files must be kept up-to date; scans must be run at least weekly; (ix) documented controls must be in effect to prevent copying data to portable storage (e.g., CDs/DVDs, USB, disks, etc.);
3. LGEUS-Provided and Customer-Provided Workstations. Vendor shall ensure that Vendor Personnel does not tamper with, disable, modify, or otherwise yield inoperable any privacy, security, or access control on any LGEUS-provided laptops, workstations, or other equipment used to process or store LGE Data. Vendor shall maintain documented controls to prevent copying data to any portable storage device (e.g., portable hard drives, CDs/DVDs, USB, etc.). All LGEUS-provided laptops, workstations, and other equipment must remain in a physically secure location.

B. Network Configuration

Vendor shall ensure that networks used to access LGE Data are configured as follows: (i) a firewall must be used to control access between the Internet and workstations used to process LGE Data; (ii) inbound Internet access must be protected from malicious code intrusion (e.g., scanning at email gateways, blocking links, stripping executables, intrusion detection/prevention system); (iii) outbound Internet access must have controls to prevent leakage and misdirection of LGE Data (e.g., proxy server, content filtering, or other network control); and (iv) if wireless networking is used at any point along the data path, the wireless network must be secured using the WPA2 standard.

C. Data Usage

Vendor shall ensure that user accounts, passwords, and keys provided by LGEUS remain confidential and are not shared between Vendor Personnel. LGE Data may only be stored on workstations allocated to the processing of LGE Data. LGE Data must not be printed except for temporary use to facilitate data processing. At the end of any processing, all printed LGE Data must be destroyed in a manner in which the data is not recoverable.

D. Data Transmission

Files containing LGE Data must be downloaded and uploaded using cryptographic means (e.g., SFTP).

E. Data Storage and Encryption

For LGE Data stored in a data center or local network drive, access must be controlled and limited to Authorized Employees specifically engaged for the applicable project. Backups of LGE Data must be encrypted. Backup tapes must be stored in an access-controlled area which is equipped with proper protocol to safeguard against natural disasters (fire suppression, flood protection, surge protection, etc.). Transport of backup tapes to secure offsite storage must be in locked containers and tracked by chain-of-custody documentation. Upon termination of this Agreement or upon request by LGEUS, after successful transfer of data as may be requested by LGEUS, backups must be disposed of in a secure manner. Vendor must encrypt, using an appropriate, industry-standard encryption algorithm, all LGE Data (A) during transfer across any network that is not owned and managed by Vendor solely as an internal network; (B) stored or transported outside of LGEUS' or Vendor's facilities; or (C) stored on portable devices or portable electronic media (to the extent otherwise permitted under the Agreement).

F. Data Disposal LGE Data must be securely deleted from all erasable media immediately after project completion for the Services under any SOW or upon written request from LGEUS. Vendor must provide LGE with evidence that said data has been purged by providing evidence in the form of a system log file or certificate of destruction. Tapes, printed output, optical disks, and other physical media must be physically destroyed by a secure method, such as shredding performed by a bonded vendor.

G. Monitoring

Vendor environments that LGEUS identifies as at risk for data loss/data leakage are subject to monitoring by LGEUS, including agent-based or hosted data loss prevention systems.

H. Testing and Scans

Vendor will perform regular vulnerability scans of all Vendor and Vendor Personnel infrastructure, applications, services, systems, and devices Vendor and Vendor Personnel use to access LGE Data using an industry-standard vulnerability scanner at reasonable intervals, but in no event less frequently than once per month. Vendor will have an accredited third party perform a security and privacy design review and penetration test of Vendor's and all Vendor Personnel's service(s), systems, and devices used to access LGE Data as circumstances reasonably require, but in no event less frequently than once per year. Vendor hereby grants LGEUS the limited right to perform logical assessments of the security of Vendor's workstation and network security via penetration, intrusion, and/or analysis services using intrusive or passive techniques and software tools ("Testing"). LGEUS may conduct the Testing using a combination of manual inspection (e.g., hidden fields examination, etc.) and commercial off-the-shelf tools. Vendor agrees to cooperate in good faith to identify mutually acceptable times for the Testing. During the Testing, Vendor will provide access to any devices and assistance to LGEUS as LGEUS may reasonably require.

I. Physical Security of Vendor Locations Prior to beginning the Services and from time to time upon the written request of LGEUS, Vendor shall provide LGEUS with Vendor's written policy detailing physical security controls for each Vendor location. Vendor agrees to comply with such policy throughout the duration of this Agreement and agrees that LGEUS has the right to audit such compliance pursuant to the terms of the Agreement.

J. Backups and Disaster Recovery

1. If the Services include providing a SaaS, PaaS, IaaS, or other Vendor hosted Service, Vendor is responsible for creating, maintaining, and testing backup copies of LGE Data. Vendor is responsible for an orderly and timely recovery of LGE Data in the event that the Services are interrupted. Vendor shall maintain no less than thirty (30) days of backups. Where fees are based on data usage, backups of LGE Data will not be considered in calculating storage used by LGEUS.
 2. Vendor shall have a minimum of one (1) disaster recovery site at a distance of at least one hundred (100) miles from the primary site. LGE Data must be replicated from the primary data center to the disaster recovery site in a time and manner sufficient to meet industry-standard recovery point and recovery time objectives applicable to the type of data hosted by Vendor, and the Services must be configured to failover from the primary data center to the disaster recovery site within the recovery time objective. LGEUS will not incur any costs in relation to additional recovery site(s).
 3. Vendor shall implement, maintain, and test disaster recovery plans to minimize downtime resulting from all hazards, including system failure. Vendor represents that these disaster recovery plans are documented, tested no less frequently than once every twelve (12) months, and updated as required. LGEUS has a right to review Vendor's disaster recovery plans, and Vendor must, upon LGEUS request, provide LGEUS with a copy of such plans.
- K. **Chain of Custody** Vendor shall ensure that LGE Data is available to LGEUS at all times (24/7/365) during the term of the Cloud Services and for a period of thirty (30) days after the term ends, including during any suspension of Cloud Services.
- L. LGE Data shall not be altered, moved, or deleted without LGEUS consent;
- M. If legal mandates for data retention apply specifically to LGE Data, Vendor shall comply with all such mandates communicated to Vendor in writing; and
- N. Vendor must document and maintain an appropriate chain of custody throughout the duration of this Agreement for the purposes of potential forensic or legal investigation. Vendor shall not remove metadata except as directed by LGEUS.
- O. **Encryption and Authentication**
1. Vendor shall encrypt all LGE Data, including backups, while at rest and in transit from end to end using encryption standards and methods that are approved and recommended by NIST and, if applicable, FIPS 140-1 and FIPS 140-2 or their successors.
 2. Proven algorithms such as AES-128, AES-256, ECDH, Blowfish, PGP, RSA, WAP2, or WPA3 for Wi-Fi encryption and SSH v 2 for remote login must be used as the basis for encryption technologies. At a minimum, the hash algorithm must be 256bit SHA-2, and the symmetric key encryption algorithm is AES-128. SSL/TLS implementations must use, at a minimum, version number 1.2 with a cipher suite implementing Cipher Block Chain (CBC) or Galois/Counter modes (GCM) as modes of operation for the cipher component and 256bit SHA-2 for the digest component. A minimum of 2048-bit RSA key modulus must be used for key establishment and digital signatures. A minimum of P-256 curve must be used for elliptical curve key establishment and digital signatures.
 3. Password complexity must include at least 8 characters and a combination of at least 2 of the following: uppercase/lowercase/digit/symbol. For password hashing, PBKDF2, Scrypt and Bcrypt or better must be used. Approved encryption algorithms must be of a minimum key length of 128 bits.
 4. Shared keys used for IPsec tunnels must be complex, randomly generated, and not be stored

for later reference. During the initial setup of an IPSec tunnel, the shared key must be transmitted out of band to the other party involved. Vendor must utilize cryptographic algorithms that are acceptable to LGEUS.

5. Random number generation shall be compliant with NIST SP 800-90A and FIPS 140-2. Furthermore, it shall meet the requirements of the draft NIST SP 800 90B and C. NIST resources are available at <https://csrc.nist.gov/>.
6. Digital Certificates that validate and secure communications used by the general public must be generated by trusted third-party providers.