The Joint Commission Enterprise

VENDOR DATA PROTECTION EXHIBIT

This Data Protection Exhibit ("**Data Protection Exhibit**") forms part of the Master Services and Subscription Agreement ("**Agreement**") between CLIENT (as defined in the Agreement, herein "**Joint Commission Enterprise**"**)** and VENDOR (as defined in the Agreement, herein "**Service Provider**"). Joint Commission Enterprise and Service Provider expressly agree to be bound by the terms of this Data Protection Exhibit for any and all products or services provided by Service Provider to Joint Commission Enterprise under the Agreement.

1. Processing of Personal Data

a) Joint Commission Enterprise is and shall remain the controller of all information that identifies or can be used to directly or indirectly identify, contact, locate, or is otherwise related to an individual ("**Personal Data**") under applicable data privacy, data protection, and data security laws and regulations ("**Applicable Privacy Laws**"). The Joint Commission Enterprise maintains the rights and obligations to determine the purposes for which Personal Data is processed (which includes but is not limited to, collection, recording, storage, use, retention, access, disclosure, analysis, security, deletion, modification, sale, sharing, augmentation, transmission, and the means by which Personal Data may be transferred to a third country or international organization) ("**Process**" or "**Processing**"). Nothing in this Data Protection Exhibit shall restrict or limit in any way Joint Commission Enterprise's rights or obligations as controller of Personal Data for such purposes. To the extent that any data privacy or data protection obligations in the Agreement are less stringent than the obligations set forth in this Data Protection Exhibit, the terms of this Data Protection Exhibit shall control.

b) Service Provider shall only Process Personal Data in accordance with the instructions of and on behalf of the Joint Commission Enterprise, as necessary to carry out the purposes of the Agreement in accordance with Annex I or as otherwise authorized by the Joint Commission Enterprise in writing ("**Processing Services**"). For clarity, and without limiting the generality of the foregoing, in no event may Service Provider: (a) "sell" or "share" (as defined under Applicable Privacy Laws) Personal Data; (b) disclose Personal Data to any third party for the commercial benefit of Service Provider or any third party; (c) retain, use, disclose, or otherwise Process Personal Data outside of its direct business relationship with the Joint Commission Enterprise or for a commercial purpose other than the business purposes specified in the Agreement; or (d) combine Personal Data with personal data that Service Provider receives from, or on behalf of, other persons, or collects from its own interaction with an individual, except and solely to the extent expressly permitted under Applicable Privacy Laws. Service Provider certifies that it understands and will comply with the foregoing restrictions. Where applicable law requires Service Provider to Process Personal Data under terms other than those of this Data Protection Exhibit, or other written instructions of the Joint Commission Enterprise, Service Provider shall immediately notify the Joint Commission Enterprise of such legal requirement before Processing in accordance with the legal requirement, unless the applicable law prohibits disclosure on important grounds of public interest. In addition, Service Provider shall notify the Joint Commission Enterprise immediately if, in Service Provider's assessment, any of the Joint Commission Enterprise's instructions infringes applicable law.

c) Service Provider shall immediately notify the Joint Commission Enterprise in writing of any request, complaint, claim, or other communication received by Service Provider (including its affiliates), as well as authorized agents, subcontractors, or other third parties authorized by the Joint Commission Enterprise ("**Subprocessor(s)**") regarding Personal Data: (i) from an individual who

is (or claims to be) the subject of the Personal Data, or that individual's authorized agent; (ii) from any data protection authority, law enforcement agency, or other government authority; and/or (iii) from the Joint Commission Enterprise's employees or other third parties, other than those set forth in this Data Protection Exhibit. Unless otherwise required by applicable law, Service Provider shall obtain the Joint Commission Enterprise's express written consent before disclosing or sharing any Personal Data in response to such requests, and Service Provider shall respond to such requests only when authorized by the Joint Commission Enterprise to do so. Notwithstanding anything to the contrary, however, Service Provider shall also cooperate with and provide assistance to the Joint Commission Enterprise and its affiliates, agents, Subprocessors, and representatives in responding to requests, inquiries, claims, and complaints regarding the Processing of Personal Data.

d) Service Provider warrants that any persons authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that such persons who have access to Personal Data are bound to Process Personal Data in accordance with the Joint Commission Enterprise's instructions.

e) Upon request, Service Provider shall provide reasonable cooperation and assistance to the Joint Commission Enterprise in carrying out any data protection impact assessment or similar activity, through means, including but not limited to, providing a systemic description of the envisaged Processing operations, assistance with an assessment of the risks to the rights and freedoms of the individuals to whom the Personal Data relates, and/or an assessment of the necessity and proportionality of the Processing operations in relation to the underlying purpose. Service Provider shall also cooperate and provide any assistance or information needed for the Joint Commission Enterprise to engage in consultations with regulatory authorities or otherwise respond to requests for information from such authorities.

2. Technical and Organizational Security Measures

a) Service Provider shall implement and maintain a written information security program ("**Information Security Program**") that includes appropriate administrative, technical, organizational, and physical safeguards to protect Personal Data, including, as appropriate: (i) the pseudonymization and encryption of Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services, including protection against unauthorized access, use, disclosure, alteration, or destruction of Personal Data; (iii) the ability to timely restore the availability of and access to the Personal Data in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing, and evaluating the effectiveness of the administrative, technical, organizational, and physical measures to ensure the security of the Processing.

b) In addition to any specific and or supplemental security safeguards established in the Agreement between the parties, Service Provider's Information Security Program shall include, but not be limited to, the safeguards set forth in Annex II to this Data Protection Exhibit, which is incorporated herein by this reference. To the extent that any specific or supplemental security safeguards in the Agreement are less stringent than the safeguards set forth in Annex II to this Data Protection Exhibit, the terms of Annex II shall control. Upon the Joint Commission Enterprise's reasonable request, Service Provider shall provide a copy of its written Information Security Program to the Joint Commission Enterprise as well as any third party audits or certifications establishing that it has implemented the safeguards set out in the Information Security Program.

c) **Credit/Debit Card Processing:** To the extent Service Provider Processes or transmits credit or debit card information, Service Provider agrees to provide evidence of compliance with the current version of the Payment Card Industry Data Security Standard ("**PCI DSS**") published on the PCI Security Standards Council ("**PCI SCC**") website and based on the Service Provider's merchant level and/or Service Provider's status: (i) on the date hereof; (ii) annually thereafter during the term of the Agreement; and (iii) upon request from the Joint Commission Enterprise. As evidence of compliance, Service Provider shall provide a current attestation of compliance signed by a PCI Qualified Security Assessor ("**QSA**") upon request.

If Service Provider is unable to provide a current attestation of compliance, Service Provider shall allow the Joint Commission Enterprise's QSA to assess all the system components in scope that are hosted or managed by Service Provider, and the related processes used to process, transmit, or store cardholder data. Service Provider shall create and maintain reasonably detailed, complete, and accurate documentation describing the systems, processes, network segments, security controls, and dataflow used to receive, transmit, store, and secure cardholder data. Such documentation shall conform to the most current version of PCI DSS. Service Provider shall, upon written request by the Joint Commission Enterprise, make such documentation and the individuals responsible for implementing, maintaining, and monitoring those system components and processes available to: (i) QSAs, forensic investigators, consultants, or attorneys retained by the Joint Commission Enterprise to facilitate the audit and review of the Joint Commission Enterprise's PCI DSS compliance; and/or (ii) the Joint Commission Enterprise's information technology audit staff.

3. **Security Incident**

a) Notwithstanding any provisions in this Data Protection Exhibit or the Agreement to the contrary, Service Provider shall notify the Joint Commission Enterprise immediately in writing no later than one (1) business day after discovery (unless a shorter time period is required by applicable law) in the event: (i) any Personal Data is Processed by Service Provider (including its Subprocessors), in violation of this Data Protection Exhibit or Applicable Privacy Laws; (ii) Service Provider (including its Subprocessors) discovers, is notified of, or reasonably suspects a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data; or (iii) there have been any formal complaints about the Service Provider's (including its 'Subprocessors') data privacy, data protection, or data security practices (each a "**Security Incident**"). Service Provider shall, cooperate fully in the investigation and remediation of the Security Incident, and take reasonable measures to limit further unauthorized disclosure or Processing of Personal Data in connection with the Security Incident. Service Provider shall also indemnify, defend, and hold the Joint Commission Enterprise, including its affiliates, harmless from and against any and all claims, suits, proceedings, damages, costs, and expenses (including, without limitation, reasonable attorneys' fees, court costs, and expert witness costs) brought against or suffered by the Joint Commission Enterprise or any third party arising out of, resulting from, or relating to, any breach by Service Provider of this Data Protection Exhibit.

b) To the extent that a Security Incident gives rise to a need, in the Joint Commission Enterprise's sole judgment to (i) provide notification to government authorities, individuals, or other persons; or (ii) undertake other remedial measures (including, without limitation, notice, credit monitoring, or call center services (collectively, "**Remedial Action**"), at the Joint Commission Enterprise's request, Service Provider shall, at Service Provider's own cost, undertake such Remedial Action. The timing, content, and manner of effectuating any notices shall be determined by the Joint Commission Enterprise in its sole discretion.

4. Subprocessors

Service Provider will not disclose or transfer Personal Data to, or allow access to Personal Data by (each, a "**Disclosure**") any third party without the Joint Commission Enterprise's express prior written consent; provided, however, that Service Provider may Disclose Personal Data to its affiliates and subcontractors for purposes of providing the Services to the Joint Commission Enterprise, subject to the following conditions: (a) Service Provider will maintain a list of the affiliates and subcontractors (with contact information) and the processing activities to be performed in connection with such Disclosures and will provide this list to the Joint Commission Enterprise prior to execution of the Agreement and at any time upon the Joint Commission Enterprise's request; (b) Service Provider will provide the Joint Commission Enterprise with at least 30 days' prior notice of the addition of any affiliate or subcontractor to this list and the opportunity to object to such addition(s); and (c) if the Joint Commission Enterprise makes such an objection on reasonable grounds and Service Provider is unable to modify the Services to prevent Disclosure of Personal Data to the additional affiliate or subcontractor, the Joint Commission Enterprise will have the right to terminate the relevant Processing. If the Joint Commission Enterprise does not object to an added third party, the new third party will be considered an authorized Subprocessor. Service Provider will, prior to any Disclosure, enter into an agreement with such third party that is at least as restrictive as this Data Protection Exhibit. Such agreement will be provided to the Joint Commission Enterprise promptly upon request. Service Provider will be liable for all actions by such third parties with respect to the Disclosure.

5. Individual Privacy Rights

Service Provider shall assist the Joint Commission Enterprise by implementing appropriate administrative, technical, and organizational measures for responding to individual's requests relating to their privacy rights, including but not limited to the rights of: (i) access; (ii) rectification; (iii) erasure; (iv) restriction of Processing; (v) data portability; (vi) objection to Processing; and (vii) avoiding automated individual decision making, including profiling. The Joint Commission Enterprise shall, in its sole judgment, determine whether or not an individual has a right to exercise any privacy rights referenced above or under relevant data privacy or data protection law, and give instructions to Service Provider to what extent the assistance is required. Further, Service Provider shall assist the Joint Commission Enterprise with communicating requests to recipients of Personal Data, including but not limited to Subprocessors, and securing such parties' cooperation to address any such individual requests.

6. Audit Rights

Service Provider shall, at no additional cost, keep or cause to be kept full and accurate records relating to all Processing of Personal Data on behalf of the Joint Commission Enterprise as part of the Processing Services, and the Joint Commission Enterprise may request, upon ten (10) days written notice to Service Provider (unless a shorter period is required to meet a legal requirement or request by a government authority), access to Service Provider's facilities, systems, records, and supporting documentation in order to audit, itself or through an independent third-party auditor, Service Provider's compliance with its obligations under or related to this Data Protection Exhibit. Audits shall be subject to all applicable confidentiality obligations agreed to by the Joint Commission Enterprise and Service Provider, and shall be conducted in a manner that minimizes any disruption of Service Provider's performance of services and other normal operations. In the event that any such audit reveals material gaps or weaknesses in Service Provider's Information Security Program or compliance with this Data Protection Exhibit, the Joint Commission Enterprise shall be entitled to suspend transmission of

Personal Data to Service Provider and terminate Service Provider's Processing of Personal Data until such issues are resolved. The Joint Commission Enterprise may also require Service Provider to, upon request, make available to the Joint Commission Enterprise, any information or certifications necessary to demonstrate compliance with the obligations set forth in this Data Protection Exhibit.

7. Cross-Border Transfers from EEA

Except as otherwise set forth in this paragraph, Module 2 Controller to Processor of the 2021 EU Standard Contractual Clauses ((EU) 2021/914) (link), together with the Annexes I and II attached to this Data Protection Exhibit ("**Model Clauses**") will apply to: (i) any transfer of Personal Data that is subject to the EU General Data Protection Regulation ((EU) 2016/679) ("**GDPR**") (or was subject to the GDPR prior to its transfer to Joint Commission Enterprise) to Service Provider located outside the European Economic Area ("**EEA**"); and (ii) any transfer of Personal Data that is subject to the laws of a country outside the EEA in which the competent authority has approved the use of the Model Clauses, including, but not limited to, Switzerland (each, an "**Adopting Country**") (or was subject to the laws of the Adopting Country prior to its transfer to Joint Commission Enterprise), to Service Provider located outside the Adopting Country. Notwithstanding the foregoing, the Model Clauses will not apply to the extent the transfer is covered by an Adequacy Decision (defined below) or Service Provider Binding Corporate Rules for Processors ("**BCR-Ps**") (where such Binding Corporate Rules provide for appropriate safeguards under GDPR or the Adopting Country's data protection laws, as relevant) in accordance with Section 9 below. Pursuant to such Model Clauses, each of the Joint Commission Enterprise's affiliates established in the EEA shall be deemed for the purposes of this Data Protection Exhibit to be the "**data exporter**," and Service Provider and each Subprocessor that stores, accesses, or otherwise Processes such Personal Data shall be deemed for the purposes of this Data Protection Exhibit to be a "**data importer**." For the purposes of this Data Protection Exhibit, an "**Adequacy Decision**" is a decision adopted by a competent authority with jurisdiction over the relevant Joint Commission Enterprise entity declaring that a jurisdiction meets an adequate level of protection of Personal Data. The parties agree:

a) For the purposes of Clause 9(a) of the Model Clauses, all subcontracting will be in accordance with Option 2 of the Model Clauses as described in Section 4 of this Data Protection Exhibit;

b) For the purposes of Clause 17 of the Model Clauses, the parties agree that the Model Clauses will be governed by the law of Ireland for transfers of Personal Data subject to GDPR and by the law of the Adopting Country for transfers of Personal Data subject to the data protection laws of the Adopting Country;

c) For the purposes of Clause 18 of the Model Clauses, the parties agree that any dispute arising from the Model Clauses will be resolved by the courts of Ireland for transfers of Personal Data subject to GDPR and by the courts of the Adopting Country for transfers of Personal Data subject to the data protection laws of the Adopting Country;

d) For the purposes of Annex I.A of the Model Clauses, the data exporters and data importers are listed in the signature pages to the Agreement;

e) For the purposes of Annex I.C of the Model Clauses, the parties agree that Ireland's Data Protection Commissioner is the competent supervisory authority for transfers of Personal Data subject to GDPR and the competent supervisory authority is the data protection authority of the Adopting Country for transfers of Personal Data subject to the data protection laws of the Adopting Country;

f) For the purposes of Annex I.C of the Model Clauses, the parties agree that Ireland's Data Protection Commissioner is the competent supervisory authority for transfers of Personal Data subject to GDPR and the competent supervisory authority is the data protection authority of the Adopting Country for transfers of Personal Data subject to the data protection laws of the Adopting Country; and

g) Where the transfer relates to Personal Data subject to the data protection laws of an Adopting Country, all references in the Model Clauses to "**EU**," "**Union**," or "**Member State**" will be interpreted as references to the Adopting Country and all references to EU law will be interpreted as references to the relevant provisions of the Adopting Country's data protection law.

8. Restricted Transfers from the United Kingdom.

This Section applies with respect to any transfer of Personal Data that is subject to the data protection laws of the United Kingdom, including the UK GDPR as defined in the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, Version B1.0, in force from March 21, 2022 ("**UK 2021 SCCs Addendum**") (link), or any onward transfer of such Personal Data, to Service Provider located in a country outside the United Kingdom for which there is no Adequacy Decision or Service Provider BCR-Ps (where such BCR-Ps provide for appropriate safeguards under UK data protection law) in accordance with Section 9 below. Where the UK 2021 SCCs Addendum applies, the parties agree that:

a) The Model Clauses, together with the UK 2021 SCCs Addendum, including Part 2 'Mandatory Clauses', incorporated herein by reference, shall apply in full;

b) Table 1 of the UK 2021 SCCs Addendum, the names of the parties, their roles and their details shall be considered populated by the information set out in the signature line of the Agreement;

c) Tables 2 and 3 of the UK 2021 SCCs Addendum shall be considered populated by the Model Clauses, including the information set out in the description of transfer and the technical and organizational security measures attached to this Data Protection Exhibit; and

d) For the purposes of Table 4 of the UK 2021 SCCs Addendum, neither party may end the UK 2021 SCCs Addendum.

9. Binding Corporate Rules

When the transfer to Service Provider is covered by **BCR-Ps**, Service Provider will (i) maintain and extend its EEA, Adopting Country or UK (as relevant) authorization of its BCR-Ps for the duration of the Agreement; (ii) promptly notify the Joint Commission of any subsequent material changes in such authorization; and (iii) downstream all of its applicable obligations under its BCR-Ps to Subprocessors by entering into appropriate onward transfer agreements with any such Subprocessor. Service Provider's BCR-Ps will be provided to the Joint Commission Enterprise prior to the execution of the Agreement.

10. Supplemental Privacy Terms

When and as required by the Joint Commission Enterprise from time to time, Service Provider shall execute and/or shall cause its affiliates or Subprocessors to execute supplemental data privacy, data protection, and/or data security terms with the Joint Commission Enterprise, including, but not limited

to, Model Clauses, as required in the Joint Commission Enterprise's sole judgment for the Processing and/or transfer of Personal Data.

11. Compliance with Applicable Privacy Laws

Service Provider will comply with all obligations applicable to Service Provider's Processing of Personal Data under Applicable Privacy Laws. Upon the reasonable request of the Joint Commission Enterprise, Service Provider will promptly make available to the Joint Commission Enterprise all information in its possession necessary to demonstrate Service Provider's compliance with its obligations under Applicable Privacy Laws. Service Provider will notify the Joint Commission Enterprise in writing if Service Provider makes a determination that it can no longer meet its obligations under Applicable Privacy Laws. The Joint Commission Enterprise has the right, upon providing notice to Service Provider, to take reasonable and appropriate steps to stop and remediate unauthorized Processing of Personal Data, including where Service Provider has notified the Joint Commission Enterprise that it can no longer meet its obligations under Applicable Privacy Laws.

12. De-identification and Aggregation

In the event the Agreement permits or instructs Service Provider to Process information in de-identified and/or aggregated form, Service Provider will ensure that any such information qualifies and remains qualified as de-identified information, de-identified data, and/or aggregate information as defined by Applicable Privacy Laws. Service Provider will make no attempt to re-identify any individual to whom such information relates, will publicly commit to maintaining and using such information without attempting to re-identify it, and will take reasonable measures to prevent such re-identification.

13. Post-Termination

Notwithstanding any other provision of the Agreement or this Data Protection Exhibit to the contrary, when Service Provider (including any of its Subprocessors) ceases to perform Processing Services for the Joint Commission Enterprise upon termination of this Data Protection Exhibit or otherwise, Service Provider shall, at the choice of the Joint Commission Enterprise: (i) return Personal Data (and all media containing copies of Personal Data) to the Joint Commission Enterprise; and/or (ii) securely purge, delete, and destroy Personal Data, unless legislation imposed upon Service Provider prevents it from returning or destroying all or part of Personal Data transferred; in such case, Service Provider must communicate in writing the legal basis preventing it from returning or destroying the Joint Commission Enterprise's Personal Data, and warrants that it shall guarantee the confidentiality of the Joint Commission Enterprise's Personal Data and shall not actively Process Personal Data. Electronic media containing Personal Data shall be disposed of in a manner that renders Personal Data unrecoverable. Upon request, Service Provider shall provide the Joint Commission Enterprise with an Officer's Certificate or other proof acceptable to the Joint Commission Enterprise to certify its compliance with this provision.

14. Entry into Data Protection Exhibit

Each Joint Commission Enterprise entity that will receive Processing Services under the Agreement shall be entitled to and bound by the rights and obligations of this Data Protection Exhibit. Notwithstanding anything to the contrary, however, each Joint Commission Enterprise entity shall

exercise its rights under this Data Protection Exhibit through the Joint Commission Enterprise, unless otherwise required by applicable law.

15. Limitation of Liability

For purposes of limitation of liability as described in the Agreement, the limitations of liability set forth in the Agreement shall not apply to any breach of this Data Protection Exhibit. In the event of a breach of this Data Protection Exhibit, Service Provider's liability for all claims and costs in the aggregate shall be the greater of applicable insurance, $500,000 or the fees paid under the Agreement during the two (2) year period preceding the date on which the last event giving rise to the claim or cost occurs.

16. Privacy Contact

Service Provider shall designate a contact person within its organization who is authorized to respond to inquiries concerning the Processing of Personal Data, and shall fully cooperate with the Joint Commission Enterprise concerning all such inquiries if so requested. Initially, Service Provider's contact person at the Joint Commission Enterprise shall be Fran Carroll, Corporate Compliance and Privacy Officer for data privacy, security, and compliance related matters.

17. Effective Date

This Data Protection Exhibit shall be effective as of the effective date of the Agreement.

ANNEX I

Description of Transfer

1. Data subjects
The Personal Data Processed concern the following categories of data subjects:

[please specify--e.g.,

- *the Joint Commission Enterprise employees*
- *the Joint Commission Enterprise customers*
- *the Joint Commission Enterprise partners/suppliers*
- *the Joint Commission Enterprise contractors]*

2. Categories of Personal Data
The Personal Data Processed concern the following categories of data:

[please specify--e.g.,

- *contact data, such as name, company, address, phone number, email, username, password;*
- *financial data, such as credit/debit card number, access code; and*
- *online tracking data, such as cookies, tags, IP address, location information, device name, domain name, and similar tracking technologies]*

3. Sensitive data - *Note: Most likely relevant for vendors processing employee or contractor personal data*
[please specify--e.g.,

- *racial or ethnic origin;*
- *political opinions;*
- *religious or philosophical beliefs;*
- *trade union membership;*
- *genetic data;*
- *biometric data for the purpose of uniquely identifying a natural person;*
- *data concerning health or data concerning a natural person's sex life or sexual orientation;*
- *Personal Data relating to criminal convictions and offences or related security measure; or state (if applicable): The Processing of sensitive data is not anticipated.]*

4. Applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions for sensitive data:

The safeguards applied to sensitive data include limiting access to staff having completed specialized training, keeping a record of access to the data, restricting onward transfers. See Annex II for additional security measures.

5. The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

Continuous.

6. Nature of the processing/Processing operations.

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

[insert general description of the services to be provided.]

7. Purpose(s) of the data transfer and further processing.

[insert general description of the purposes that Personal Data will be Processed.]

8. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.

For term of Processing Services as provided for in the Agreement or as otherwise instructed by the Joint Commission Enterprise.

9. For transfers to processors, also specify subject matter, nature and duration of the processing.

[Insert general description of the subject matter, nature and duration of Personal Data Processing or refer to sections above.]

ANNEX II

Technical and Organizational Security Measures

To the extent that the Joint Commission Enterprise provides to Service Provider or Service Provider otherwise accesses the Joint Commission Enterprise's Personal Data in connection with this Data Protection Exhibit, Service Provider shall implement an Information Security Program that includes administrative, technical and physical safeguards to ensure the confidentiality, integrity and availability of Personal Data, protect against any reasonably anticipated threats or hazards to the confidentiality, integrity and availability of Personal Data, and protect against unauthorized access, use, disclosure, alteration or destruction of Personal Data. In particular, Service Provider's Information Security Program shall include, but not be limited to the following safeguards where appropriate or necessary to ensure the protection of Personal Data:

(i) Access Controls – policies, procedures and physical and technical controls: (i) to limit physical access to its information systems and the facility or facilities in which they are housed to properly authorized persons; (ii) to ensure that all members of its workforce who require access to Personal Data have appropriately controlled access, and to prevent those workforce members and others who should not have access from obtaining access; (iii) to authenticate and permit access only to authorized individuals and to prevent members of its workforce from providing Personal Data or information relating thereto to unauthorized individuals; and (iv) to encrypt and decrypt Personal Data where appropriate.

(ii) Security Awareness and Training – a security awareness and training program for all members of Service Provider's workforce (including management), which includes training on how to implement and comply with its Information Security Program.

(iii) Security Incident Procedures – policies and procedures to detect, respond to and otherwise address security incidents, including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into Personal Data or information systems relating thereto, and procedures to identify and respond to suspected or known security incidents, mitigate harmful effects of security incidents, and document security incidents and their outcomes.

(iv) Contingency Planning – policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages Personal Data or systems that contain Personal Data, including a data backup plan and a disaster recovery plan.

(v) Device and Media Controls – policies and procedures that govern the receipt and removal of hardware and electronic media that contain Personal Data into and out of a Service Provider facility, and the movement of these items within a Service Provider facility, including policies and procedures to address the final disposition of Personal Data and/or the hardware or electronic media on which it is stored, and procedures for removal of Personal Data from electronic media before the media are made available for re-use.

(vi) Audit Controls – hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements and compliance therewith.

(vii) Data Integrity – policies and procedures to ensure the confidentiality, integrity and availability of Personal Data and protect it from disclosure, improper alteration or destruction.

(viii) Storage and Transmission Security – technical security measures to guard against unauthorized access to Personal Data that is being transmitted over an electronic communications network, including a mechanism to encrypt electronic information whenever appropriate, such as while in transit or in storage on networks or systems to which unauthorized individuals may have access.

(ix) Secure Disposal – policies and procedures regarding the disposal of Personal Data, and tangible property containing Personal Data, taking into account available technology so that Personal Data cannot be practicably read or reconstructed.

(x) Assigned Security Responsibility – Service Provider shall designate a security official responsible for the development, implementation and maintenance of its Information Security Program. Service Provider shall inform the Joint Commission Enterprise as to the person responsible for security.

(xi) Testing – Service Provider shall regularly and no less than one time per year test the key controls, systems and procedures of its Information Security Program to ensure that they are properly implemented and effective in addressing the threats and risks identified. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

(xii) Adjust the Program – Service Provider shall monitor, evaluate and adjust, as appropriate, the Information Security Program in light of any relevant changes in technology or industry security standards, the sensitivity of Personal Data, internal or external threats to Service Provider or Personal Data, requirements of applicable work orders, and Service Provider's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to information systems.