VIRGINIA Cannabis Control Authority

Request for Proposals # BPM049350

Addendum #1

1. **Page 10 of the RFP (line 194) states the timeline. What time of day are the first and second round of questions due on April 9th and April 16th?**

   The first and second rounds of questions are due by 11:59 ET on April 9th and April 16th.

2. **Page 10 of the RFP (line 194) states the timeline. Can the CCA confirm that the deadline for this proposal is Mother's Day, Sunday May 12 at 11:59pm ET? Would the CCA consider extending the proposal submission deadline to give vendors adequate time to adjust their response to the CCA's answers to questions?**

   Yes, the deadline is Sunday, May 12, 2024, at 11:59pm ET. The CCA does not anticipate extending the submission deadline at this time.

3. **What is the contract term resulting from the award of this RFP?**

   The contract term is a two (2) year base period and two (2) three-year option periods.

4. **Page 11 of the RFP (lines 213-214) states, "Signed cover page and declaration of any issues they have with any specific contract or agreement terms" and page 17 (lines 289-297) states, "Additional Clauses and Agreement Terms. Any contract or agreement resulting from this RFP will include the terms laid out in the RFP along with the Commonwealth of Virginia's required contract terms." Other than what is stated in the RFP, where can vendors find a copy of the clauses and terms that will be required?**

   The Commonwealth's standard contract terms and conditions can be found in Appendix B of the Vendors Manual available here: https://dgs.virginia.gov/globalassets/business-units/dps/documents/vendorsmanual/vm_10132023_final.pdf

5. **Can the CCA confirm that it only expects vendors to provide narrative responses to SaaS solution requirements in the provided Excel file? (Versus vendors providing narrative responses in both the Excel file and Proposal? If not, how will scoring be calculated on the same technical requirements in two places?)**

   The vendor is expected to complete the provided Excel file in addition to providing a written proposal. The Excel document contains columns for "Proposal Page Reference" for the vendor to indicate where in the written proposal a specific SaaS solution requirement can be found (if included in the written proposal).

5. **What does the "Proposal Page Reference" mean in the "SaaS solution requirements" Excel document?**

   The Proposal Page Reference is the page number in which the SaaS solution requirement is referenced or evidenced in the vendor's written proposal.

6. **Can the CCA clarify what is to be included in the 50-page proposal? For example, are vendors expected to provide narrative responses for the following: vendor qualifications page 35 of the RFP (lines 810-921), subcontractor qualifications and experience page 39 (lines 922-966), staffing page 42 (lines 1012-1070)? And that SaaS solution requirements (Excel), Offeror Information Sheet page 11 (lines 206-216), Proprietary Information Table page 12 (lines 231-248), Pricing page 12 (249-250), and References page 40 (lines 967-1011), are submitted separately from the Proposal?**

   Vendors are allowed to submit vendor qualifications, subcontractor qualifications and experience, and staffing information as attachments along with the written proposal. The CCA provides areas to upload Proprietary Information, SaaS Solutions Requirements, Pricing Proposal, and References.

7. **Page 14 of the RFP (lines 266-267) states, "One or more Offerors deemed to be fully qualified and best suited among those submitting proposals will be identified on the basis of the evaluation factors stated herein." How does the CCA envision using more than one offeror to provide a statewide software-as-a-service, seed-to-sale tracking system for the Virginia medical cannabis program?**

   The CCA does not envision using more than one Vendor so long as the one Vendor selected meets the requirements set out in the RFP.

6. **Is the CCA open to considering exclusivity for a seed to sale tracking system?**

   No.

7. **Will the CCA be willing to provide a draft contract for review?**

   No.

3. **Page 9, (Lines 184 – 193) states, "Depending on the implementation approach and SaaS product, the CCA may require the completion of data conversion activities from one or more databases containing current system data. Data conversion activities should occur parallel to system implementation and align key project milestones. The CCA expects the Vendor to provide all data conversion software and tools to consume and transform data into the implemented SaaS solution. Data conversion activities should include analysis of existing data structures and fields, mapping to the new target SaaS solutions database tables and tools, transformation of data if necessary and approved, audit reports to document that all data specified was converted successfully and multiple rounds of conversion dry runs and testing to ensure maximum confidence in the integrity of the data conversion process." Questions: Can the CCA provide the format, volume, and**

database platform where current system data resides? Will the new vendor be able to log into these databases, and if so, will someone be available to answer questions about the architecture?

The format and volume of data is ultimately dependent upon the vendor's SaaS solution capabilities. It is the CCA's desire to work with the selected vendor to ensure that the SaaS solution has as complete an accounting of data and records from previous systems and solutions as possible, understanding that there may be legacy records that will need to be maintained outside of the selected vendor's solution. The method of access to data will be determined through plans developed with CCA, existing vendors, and the selected vendor.

4. **Page 32, (Line 721) states, "The data security for the proposed solution(s) must meet the requirements set by the CCA." Question: Where do vendors locate the data security requirements set by the CCA?**

   See IT-002S14 - Third-Party Vendor Data Security Requirements (attached to this Addendum as Appendix A).

5. **Page 33, (Lines 741-747) states, "The system must have an ability to integrate with the following systems: 46.1.1 CCA's Cannabis Patient Certification System; 46.1.2 CCA's Cannabis Business Licensing System; 46.1.3 Virginia's Prescription Monitoring Program; 46.1.4 CCA's Product Registration System; and 46.1.5 Pharmaceutical processor and cannabis dispensing facility point-of-sale (POS) system." Question: What software applications does CCA use for the systems listed in 46.1.1-46.1.4?**

   The CCA currently uses System Automation and BioTrack.

6. **Page 36, (lines 828-829) states, "Provide a statement on how the Vendor will vet, train, and/or supervise employees and/or contract personnel to ensure workforce clearance procedures are followed." Question: Will the CCA please clarify workforce clearance procedures?**

   Workforce clearance procedures are defined as any process necessary to ensure employee separation from the vendor or subcontractor, including full removal of access, data sanitization, and appropriate non-disclosure agreements.

7. **Page 38, (line 909) states, An audit from an independent accounting firm for the previous three (3) fiscal years. Question: As a private company, we are not required to undergo financial audits. However, we elected to do audits for the 2021 and 2022 calendar years but have not yet done an audit for the 2023 calendar year. Is the CCA willing to accept two years of audits in this circumstance?**

   Yes.

8. **Does the CCA have a preferred pricing format? For example, other jurisdictions have requested that the cost to the state be broken down by contract year and type (eg annual SaaS fee, implementation fee, hourly rate for new development, etc).**

   The CCA does not have a preferred pricing format.

9. **Is the page limit for the proposal inclusive of external documentation like Implementation Plans, Disaster Recovery Plans, and Project Management Plans? Are these supplementary documents allowed to be included as separate attachments from the proposal?**

   No. The written proposal is not inclusive of such external documentation. Supporting documents can be uploaded with the proposal without counting towards the 50-page limit.

10. **Can bidders include screenshots within their responses in the SaaS Solution Requirements Excel Document?**

    No, screenshots should not be included in the SaaS Solution Requirements Excel Document.

11. **Does the required financial documentation contribute to the 50-page limit or can these documents be referenced and included as separate attachments from the proposal ?**

    Financial documentation can be referenced in the proposal and included as attachments that do not contribute to the 50-page limit.

12. **Is it permissible to include URLs within the proposal for the purpose of referencing documentation such as API documentation, SOC audit documentation, etc.?**

    Yes.

13. **Will the Department provide a cost breakdown template?**

    No.

14. **Do the resumes provided for Vendor staff contribute to the 50-page limit?**

    No. Vendor staff resume documentation can be referenced in the proposal and included as attachments that do not contribute to the 50-page limit.

15. **Does the State require the vendor to offer actual smart chip technology in the plant and inventory tags or does the plant/inventory tag need to at least include a label with a unique identifier that is also scannable?**

    The Commonwealth finds either solution acceptable so long as the identifier is unique and can be scanned.

16. **Is the prior state contract requirement (57.1.1) waiverable for novel and patented technology which would otherwise meet all the mandatory and optional requirements of a track and trace system?**

    Due to accelerated implementation timetable sought in the RFP, the CCA seeks a vendor that can demonstrate a proven track record of performance on state contracts.

17. **Can the vendor be from a country other than USA or does it need to be USA registered entity only?**

    Vendors located in, doing business from, owned, or operated by an entity located in the People’s Republic of China, Russian Federation, Democratic People's Republic of Korea, or

Islamic Republic of Iran will not be considered. Further, the Vendor will not provide access to CCA data to any entity or person(s) located outside the continental United States that are not named in any future contract without the written permission of the CCA. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States. The Vendor shall provide its services to the CCA and storage of CCA data solely from data centers in the continental United States. The Vendor will not allow any state to be provided to or accessed by any entity outside the continental United States. This restriction includes but is not limited to Vendor's employees and contractors. The Vendor shall not allow its employees or contractors to store CCA data on portable devices, including personal computers, except for devices used and kept only at its data centers. The Vendor shall permit its personnel and contractors to access CCA data remotely only as required to provide technical support or fulfill any future contract. If the CCA's data being remotely accessed is legally protected data or considered classified by the CCA, then:

- The device used must be password protected;
- Multifactor Authentication must be used;
- The data is encrypted to at least AES 256 both in transit and in storage;
- Data is not put onto mobile media;
- No non-electronic copies are made of the data; and
- The Vendor maintains a log on what data was accessed, when it was accessed, and by whom it was accessed.

18. Is this RFP for international software vendors as well?

Vendors located in, doing business from, owned, or operated by an entity located in the People's Republic of China, Russian Federation, Democratic People's Republic of Korea, or Islamic Republic of Iran will not be considered. Further, the Vendor will not provide access to CCA data to any entity or person(s) located outside the continental United States that are not named in any future contract without the written permission of the CCA. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States. The Vendor shall provide its services to the CCA and storage of CCA data solely from data centers in the continental United States. The Vendor will not allow any state to be provided to or accessed by any entity outside the continental United States. This restriction includes but is not limited to Vendor's employees and contractors. The Vendor shall not allow its employees or contractors to store CCA data on portable devices, including personal computers, except for devices used and kept only at its data centers. The Vendor shall permit its personnel and contractors to access CCA data remotely only as required to provide technical support or fulfill any future contract. If the CCA's data being remotely accessed is legally protected data or considered classified by the CCA, then:

- The device used must be password protected;
- Multifactor Authentication must be used;

- The data is encrypted to at least AES 256 both in transit and in storage;
- Data is not put onto mobile media;
- No non-electronic copies are made of the data; and
- The Vendor maintains a log on what data was accessed, when it was accessed, and by whom it was accessed.

19. Can international software vendors become subcontractor if they can directly become primary vendor to apply this RFP?

- Subcontractors are subject to the same restrictions as primary vendors in relation to business entity location.
- Vendors located in, doing business from, owned, or operated by an entity located in the People's Republic of China, Russian Federation, Democratic People's Republic of Korea, or Islamic Republic of Iran will not be considered. Further, the Vendor will not provide access to CCA data to any entity or person(s) located outside the continental United States that are not named in any future contract without the written permission of the CCA. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States. The Vendor shall provide its services to the CCA and storage of CCA data solely from data centers in the continental United States. The Vendor will not allow any state to be provided to or accessed by any entity outside the continental United States. This restriction includes but is not limited to Vendor's employees and contractors. The Vendor shall not allow its employees or contractors to store CCA data on portable devices, including personal computers, except for devices used and kept only at its data centers. The Vendor shall permit its personnel and contractors to access CCA data remotely only as required to provide technical support or fulfill any future contract. If the CCA's data being remotely accessed is legally protected data or considered classified by the CCA, then:
    - The device used must be password protected;
    - Multifactor Authentication must be used;
    - The data is encrypted to at least AES 256 both in transit and in storage;
    - Data is not put onto mobile media;
    - No non-electronic copies are made of the data; and
    - The Vendor maintains a log on what data was accessed, when it was accessed, and by whom it was accessed.

Appendix A

Third-Party Vendor Data Security Requirements Standard

Standard Number: IT-002S14
Department: Information Technology
Executive Oversight: Chief Administrative Officer
Date of Last Review:

Purpose:

This standard aims to establish minimum security requirements for the initial and ongoing review and implementation of third-party Information Technology Resources. This standard shall be applied to all Authority third-party vendors and service providers to maintain the confidentiality, integrity, and availability of Authority data.

Standard Statement:

The Third-Party Vendor Data Security Requirements Standard lays out specific elements required by the CCA, not specified in the Vendor Risk Management Standard.

Scope:

All Third-Party Vendors contracted by the Virginia Cannabis Control Authority

Definitions:

Availability
The ability to make information and related physical and logical resources usable.

Confidentiality
Protecting information so that it is only accessed by authorized individuals.

Contractor
A person or a company that undertakes a contract with the Virginia Cannabis Control Authority to provide Information Technology Resources or labor in services of the CCA's mission.

Data
Data are recorded information that documents an Authority business-related transaction or activity by or with any board member, officer, or employee of the Authority. Virginia Cannabis Control Authority data may include but are not limited to personnel, processor, provider, patient, financial, client, and administrative records. Data can be stored in many formats, including but not limited to email, electronic databases, electronic files, audio, video, and images stored electronically.

Integrity

The trustworthiness and dependability of information. More specifically, it is the accuracy, consistency, and reliability of the information content, processes, and Information Technology Resources.

Risk Assessment
A SOC 2 Type II or equivalent external security assessment or alternative self-assessment, provided the controls in the assessment are representative of the vendor's current state.

SOC 2 Type II
Service Organization Control Type II is a voluntary compliance standard for service organizations, developed by the American Institute of CPAs (AICPA), which specifies how organizations should manage customer data. The standard is based on the following Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy.

Third-party Contractors
Any vendor, contractor, consultant, or non-Virginia Cannabis Control Authority employee working on behalf of the Virginia Cannabis Control Authority.

Third-Party Hosted
An Information Technology Resource or other technology with user interfaces or applications not directly maintained, managed, or operated by the Virginia Cannabis Control Authority. Generally managed by a Third-Party Contractor.

Roles and Responsibilities:

Employees:

- Before engaging a vendor, consult the Director of Information Technology to see if an existing solution exists.
- Participate in the technology vetting process before procurement.
- Provide the information necessary to perform a Risk Assessment before procurement to the Director of Information Technology.
- Perform an annual review of the Risk Assessment.
- Provide the information to perform a Risk Assessment to Information Security for a full Risk Assessment every three years.

Director of Information Technology:

- Oversees the Third-Party Vendor Management process.
- Performs pre-procurement Risk Assessments.
- Manages the technology vetting process.
- Coordinates with the employee(s), Director of Finance, and Chief Administrative Officer during the technology vetting process.
- Documents risk assessment results from the technology vetting process.

Chief Administrative Officer:

- Ensure all Third-Party Vendors meet all Authority-approved contract language.
- Ensure contracts for all cloud-hosted Information Technology Resources must include language stating that the supplier will comply with all applicable Authority security standards.

Director of Finance:

- Coordinate between the Authority and the Third-Party Vendors subject to the Payment Card Industry Data Security Standard (PCI-DSS) on annual Risk Assessments.
- Coordinate with the Director of Information Technology on pre-procurement Risk Assessments.
- Coordinate with Third-Party Vendors on periodic/annual SOC2 Type II submissions.

Third-party Vendor:

- Comply with the Virginia Cannabis Control Authority security standards.
- Provide annual audits, Service Organization Control Type II (SOC2), or equivalent audit reports.
- Conduct and provide vulnerability scan reports.
- Notify the Virginia Cannabis Control Authority of any security breach via contractually agreed-upon procedures.
- Ensure that the Authority data, including all Information Technology Resources components and services, remain within the continental United States.
- Consent to be subject to recurring Risk Assessments at least annually or immediately following an incident classified as significant and shall provide security assessments upon request.

Procedures:

CONFIDENTIALITY OF INFORMATION

For purposes of this paragraph, “CCA Proprietary Information” shall include all information disclosed to the Vendor by the Virginia Cannabis Control Authority (CCA), licensees of the CCA, applicants to the CCA, or patients using systems operated by the CCA. The Vendor and Vendor’s Subcontractors, Agents, Assigns, and/or Affiliated Entities shall not disclose any CCA Proprietary Information to any third person for any reason without the express written permission of a Virginia Cannabis Control Authority officer or employee with authority to authorize the disclosure. The Vendor and Vendor’s Subcontractors, Agents, Assigns, and/or Affiliated Entities shall not:

- disclose any CCA Proprietary Information to any third person unless otherwise specifically allowed under this Standard;
- make any use of CCA Proprietary Information except to exercise rights and perform obligations under this Standard;
- make CCA Proprietary Information available to any of its employees, officers, agents, or third-party Vendors except those who need to access such information and who have agreed to confidentiality obligations at least as strict as those set out in this Standard.

The Vendor and Vendor's Subcontractors, Agents, Assigns, and/or Affiliated Entities are held to the same standard of care in guarding CCA Proprietary Information as it applies to its own confidential or proprietary information and materials of a similar nature, and no less than holding Commonwealth Proprietary Information in the strictest confidence. The Vendor and Vendor's Subcontractors, Agents, Assigns, and/or Affiliated Entities shall protect the confidentiality of the CCA's information from the time of receipt to the time that such information is either returned to the CCA or destroyed to the extent that it cannot be recalled or reproduced. The Vendor and Vendor's Subcontractors, Agents, Assigns, and/or Affiliated Entities agree to return all information received from the CCA to CCA's custody upon the end of the term of this Standard unless otherwise agreed in writing signed by both parties.

CCA Proprietary Information shall not include information that:

- was in the public domain at the time it was disclosed to the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities;
- was known to the Vendor and Vendor's Subcontractors, Agents, Assigns, and/or Affiliated Entities without restriction at the time of disclosure from the CCA;
- that was disclosed with the prior written approval of CCA's officers or employees having the authority to disclose such information;
- was independently developed by the Vendor and Vendor's Subcontractors, Agents, Assigns, and/or Affiliated Entities without the benefit or influence of the CCA's information;
- becomes known to the Vendor and Vendor's Subcontractors, Agents, Assigns, and/or Affiliated Entities without restriction from a source not connected to the Virginia Cannabis Control Authority.

The CCA Proprietary Information can include names, social security numbers, driver's license numbers, Protected Health Information, business information, employer numbers, addresses, and other data about applicants, employers, or other clients to whom the CCA provides services of any kind. Vendor understands that this information is confidential and protected under Commonwealth law. The parties mutually agree that neither of them nor any Vendor, and Vendor's Subcontractors, Agents, Assigns, and/or Affiliated Entities shall disclose the contents of this Standard except as required by applicable law or as necessary to carry out the terms of the Standard or to enforce that party's rights under this Standard. The vendor acknowledges that the CCA is a public entity and thus may be bound by Virginia open meetings and open records laws. It is, therefore, not a breach of this Standard for the CCA to take any action that the CCA reasonably believes is necessary to comply with Virginia open records or open meetings laws.

CYBER LIABILITY INSURANCE

The Vendor shall maintain cyber liability insurance with liability limits with a minimum amount of $1 million dollars to protect any and all CCA data the Vendor receives as part of the project covered by this Standard, including CCA Proprietary Data that may reside on devices, including laptops, and smartphones, utilized by Vendor employees, whether the employee or the Vendor owns the device. If the Vendor has a contract with a third party to host any CCA data the Vendor receives as part of the project under this Standard, then the Vendor shall include a requirement

for cyber liability insurance as part of the contract between the Vendor and the third party hosting the data in question. The third-party cyber liability insurance coverage will include CCA Proprietary data that resides on devices, including laptops and smartphones, utilized by third-party employees, whether the employee or the third-party Vendor owns the device. The cyber liability insurance shall cover expenses related to managing a data breach incident, the investigation, recovery, and restoration of lost data, data subject notification, call management, credit checking for data subjects, legal costs, and regulatory fines. Before beginning work under this Standard, the Vendor shall furnish the CCA with properly executed Certificates of Insurance, which shall clearly evidence all insurance required in this Standard and which provide that such insurance may not be canceled, except on 30 days prior written notice to the CCA. The Vendor shall furnish copies of insurance policies if requested by the CCA. The insurance will stay in effect for 2 years after the work covered by this Standard is completed.

CESSATION OF BUSINESS

The Vendor will notify the CCA of impending cessation of its business or that of a tiered provider and the Vendor's contingency plan. This plan should include the immediate transfer of any previously escrowed assets and data and CCA access to the Vendor's facilities to remove or destroy any CCA-owned assets and data. The Vendor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the CCA. The Vendor will provide a fully documented service description and perform and document a gap analysis by examining any differences between its services and those to be provided by its successor. The Vendor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the CCA. The Vendor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and impact on the CCA, all such work to be coordinated and performed in advance of the formal, final transition date.

VENDOR TRAINING REQUIREMENTS

The Vendor, Vendor's employee(s), and Vendor's Subcontractors, Agents, Assigns, Affiliated Entities and their employee(s), must successfully complete, at the time of hire and annually thereafter, a cyber-security training program. The training must include but is not limited to:

- Legal requirements for handling data,
- Media sanitation,
- Strong password protection,
- Social engineering, or the psychological manipulation of persons into performing actions that are inconsistent with security practices or that cause the divulging of confidential information,
- Security incident response, and
- Protected Health Information.

NONDISCLOSURE AND SEPARATION OF DUTIES

The Vendor shall enforce separation of job duties and require non-disclosure agreements of all staff that have or can have access to CCA data or the hardware that CCA data resides on. The Vendor will limit staff knowledge to those staff who duties that require them to have access to the CCA's data or the hardware the CCA's data resides on.

EXTRACTION OF DATA

Upon notice of termination by the Vendor or upon reaching the end of the term, any information stored in repositories not hosted on the CCA's infrastructure shall be extracted in a format to enable to CCA to load the information onto/into repositories. If this is not possible the information metadata, including data structure descriptions and data dictionary, and data will be extracted into a text file format and returned to the CCA. Upon the effective date of the termination of the contract, the CCA again requires that CCA applications that store information to repositories not hosted on the CCA's infrastructure require the Vendor before termination (whether initiated by the CCA or the Vendor) to extract the CCA's information such that the CCA is able to load the information onto or into CCA owned-repositories. If the information cannot be extracted in a format that allows the information to be loaded onto or into the CCA's repositories, the information (metadata (data structure descriptions) and data) will be extracted into a text file format and returned to the CCA. The Vendor recognizes and agrees that the CCA cannot enter into an agreement providing for hosting of any of its data on the Vendor's servers and networks without provisions protecting its ability to access and recover its data in a usable, non-proprietary format in the event of termination of this contract with sufficient time to convert that data and the business functions provided by the Vendor to another system and Vendor.

LEGAL REQUESTS FOR DATA

Except as otherwise expressly prohibited by law, the Vendor will:

- Immediately notify the CCA of any subpoenas, warrants, or other legal orders, demands or requests received by the Vendor seeking CCA data maintained by the Vendor;
- Consult with the CCA regarding its response;
- Cooperate with the CCA's requests in connection with efforts by the CCA to intervene and quash or modify the legal order, demand, or request; and
- Upon the CCA's request, provide the CCA with a copy of both the demand or request and its proposed or actual response.

EDISCOVERY

The Vendor shall contact the CCA upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require, access to the data of the CCA. The Vendor shall not respond to service of process and other legal requests related to the CCA without first notifying the CCA unless prohibited by law from providing such notice.

SERVICE LEVEL AGREEMENTS

The Vendor warrants that all services will be performed in a professional and workmanlike manner consistent with industry standards reasonably applicable to such services. The Vendor

further warrants that the services will be operational at least 99.99% of the time in any given month during the term of this Standard. In the event of a service outage, the Vendor will:

- Promptly and at the Vendor's expense, use commercial best efforts to restore the services as soon as possible and
- Unless the outage was caused by a Force Majeure event, refund or credit to the CCA, at the CCA's election, the pro-rated amount of fees corresponding to the time Services were unavailable or $100 US funds per incident, whichever is the greater amount. For the purpose of this Standard, an incident, regardless of time required to return to online position and whether re-keying of data is necessary to return, is defined as any significant reduction in the availability of hosted services lasting more than one minute or resulting in data loss, rework, or occurring more than 3 times in a 24-hour time period. For example, being forced offline no more than twice in 24 hours would not be an incident if the user could get back online within 60 seconds and continue work where he or she left off. Being forced off-line 3 times in a day would be an incident, regardless. Being forced off-line once in a 24-hour period of time, however, that resulted in the user having to rekey data that was lost would be an incident. Entering User authentication to log on shall not be considered data entry.
- The Vendor will provide the CCA with seven days prior notice of scheduled downtime in the provision of services for maintenance or upgrades. To the extent possible, the Vendor will schedule downtime during times of ordinarily low use by the CCA. In the event of unscheduled or unforeseen downtime for any reason, except as otherwise prohibited by law, the Vendor will promptly notify the CCA and respond promptly to the CCA's reasonable requests for information regarding the downtime.

PROVISION OF DATA

Upon notice of termination by either party, the CCA will be provided by the Vendor all current CCA data in a non-proprietary form. CCA data is any data produced or provided by the CCA as well as any data produced or provided for the CCA by a third-party.

DATA SANITIZATION

At the end of the project covered by this Standard the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities shall return the CCA's data and/or securely dispose of all CCA data in all forms, this can include CCA data on media such as paper, magnetic tape, magnetic disks, solid state devices, or optical discs. This data must be permanently deleted by either purging the data or destroying the medium on which the CCA data is found according to the methods given in the most current version of NIST 800-88. Certificates of Sanitization for Offsite Data must be completed by the Vendor and given to the CCA contact. The CCA will review the completed Certificates of Sanitization for Offsite Data. If the CCA is not satisfied by the data sanitization then the Vendor will use a process and procedure that does satisfy the CCA. The only exceptions are when the CCA Data must be maintained after the project is completed for legal reasons or the CCA data is on a backup medium where the CCA data cannot be separated from other data. If the CCA data cannot be sanitized for these reasons, then the Vendor must encrypt the data to at least 256 AES with SHA 2 or SHA 256 hashing and maintain

the medium in a facility that meets the security requirements of the most current version of NIST 800-53 or IRS 1075 whichever is relevant.
This contract clause remains in effect for as long as the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities have the CCA data, even after the contract is terminated or the project is completed.

CHANGE MANAGEMENT PROCESS
From time to time it may be necessary or desirable for either the CCA or the Vendor to propose changes to the Services provided. Such changes shall be effective only if they are in writing and contain the dated signatures of authorized representatives of both parties. Unless otherwise indicated, a change or amendment shall be effective on the date it is signed by both parties. Automatic upgrades to any software used by the Vendor to provide any services that simply improve the speed, efficiency, reliability, or availability of existing services and do not alter or add functionality, are not considered "changes to the Services" and such upgrades will be implemented by the Vendor on a schedule no less favorable than that provided by the Vendor to any other customer receiving comparable levels of services.

USE OF PORTABLE DEVICES
The Vendor shall prohibit its employees, agents, affiliates, and subcontractors form storing CCA data on portable devices, including personal computers, except for devices that are used and kept only at the Vendor's data center(s). All portable devices used for storing CCA Data must be password protected and encrypted.

USE OF PRODUCTION DATA IN A NON-PRODUCTION ENVIRONMENT
The Vendor cannot use protected CCA data, whether legally protected or protected by industry standards, in a non-production environment. Any non-production environment that is found to have legally protected production data, must be purged immediately and the CCA Contact notified. The CCA will decide if this event is to be considered a security incident. "Legally protected production data" is any data protected under Federal or Commonwealth Statute or regulation. "Industry standards" are data handling requirements specific to an industry. An example of data protected by industry standards is payment card industry information (PCI). Protected data that is de-identified, aggregated or hashed is no longer considered to be legally protected.

SYSTEM UPGRADES
Advance notice of 30 days shall be provided the CCA of any major upgrades or system changes the Vendor will be implementing unless the changes are for reasons of security. A major upgrade is a replacement of hardware, software or firmware with a newer or improved version, in order to bring the system up to date or to improve its characteristics. The CCA reserves the right to postpone these changes unless the upgrades are for security reasons. The CCA reserves the right to scan the Vendor's systems for vulnerabilities after a system upgrade. These vulnerability scan can include penetration testing of a test system at the CCA's discretion.

BUSINESS CONTINUITY AND DISASTER RECOVERY

The Vendor shall provide a business continuity and disaster recovery plan upon request and ensure that the Commonwealth's Recovery Time Objective (RTO) of one hour (1) hour and Recovery Point objective (RPO) of twenty four (24) hours is met. For purposes of this contract, a "Disaster" shall mean any unplanned interruption of the operation of or inaccessibility to the Vendor's service in which the CCA, using reasonable judgment, requires relocation of processing to a recovery location. The CCA shall notify the Vendor as soon as possible after the CCA deems a service outage to be a Disaster.

DATA RECOVERY

The Vendor must be able to recover the CCA's data in the same state it was sent to the Vendor for 13 months. If the Vendor system or the third-party system that is hosting data for the Vendor is subjected to a disaster severe enough to implement disaster recovery procedures, then recovery of the CCA data will follow the disaster recovery requirements for Recovery Time Objective and Recovery Point Objective agreed to by the CCA and the Vendor.

THREAT NOTIFICATION

Upon becoming aware of a credible security threat with the Vendor's product(s) and or service(s) being used by the CCA, the Vendor or any subcontractor supplying product(s) or service(s) to the Vendor needed to fulfill the terms of this Standard will notify the CCA within two (2) business days of any such threat. If the CCA requests, the Vendor will provide the CCA with information on the threat. A credible security threat consists of the discovery of an exploit that a person considered an expert on Information Technology security believes could be used to breach one or more aspects of a system that is holding CCA data, or a product provided by the Vendor.

SECURITY INCIDENT NOTIFICATION

For protected non-health information only, the Vendor will implement, maintain, and update Security Incident procedures that comply with all CCA standards and Federal and Commonwealth requirements. A Security Incident is a violation of any CCA security or privacy policies or contract agreements involving sensitive information, or the imminent threat of a violation. The CCA security policies can be furnished upon request. The CCA requires notification of a Security Incident involving any of the CCA's classified data in the Contractor's possession. CCA Data is any data produced or provided by the CCA as well as any data produced or provided for the CCA by a third-party. The parties agree that, to the extent probes and reconnaissance scans common to the industry constitute Security Incidents, this Standard constitutes notice by Vendor of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the CCA shall be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Vendor's firewall, port scans, and unsuccessful log-on attempts, as long as such probes and reconnaissance scans do not result in a Security Incident as defined above. Except as required by other legal requirements the Vendor shall only provide notice of the incident to the CCA. The CCA will determine if notification to the public will be by the CCA or by the Vendor. The method and content of the notification of the affected parties will be coordinated with, and is subject to approval by the CCA, unless required otherwise by legal requirements. If the CCA decides that the Vendor will be distributing,

broadcasting to or otherwise releasing information on the Security Incident to the news media, the CCA will decide to whom the information will be sent, and the CCA must approve the content of any information on the Security Incident before it may be distributed, broadcast or otherwise released. The Vendor must reimburse the CCA for any costs associated with the notification, distributing, broadcasting or otherwise releasing information on the Security Incident.

A. The Vendor shall notify the CCA Contact within twelve (12) hours of the Vendor becoming aware that a Security Incident has occurred. If notification of a Security Incident to the CCA Contact is delayed because it may impede a criminal investigation or jeopardize homeland or federal security, notification must be given to the CCA within twelve (12) hours after law-enforcement provides permission for the release of information on the Security Incident.

B. Notification of a Security Incident at a minimum is to consist of the nature of the data exposed, the time the incident occurred and a general description of the circumstances of the incident. If not all of the information is available for the notification within the specified time period Vendor shall provide the CCA with all of the available information along with the reason for the incomplete notification. A delay in excess of twelve (12) hours is acceptable only if it is necessitated by other legal requirements.

   At the CCA's discretion, the Vendor must provide to the CCA all data available including:
   a. Name of and contact information for the Vendor's Point of Contact for the Security Incident;
   b. date and time of the Security Incident;
   c. date and time the Security Incident was discovered:
   d. description of the Security Incident including the data involved, being as specific as possible;
   e. the potential number of records, and if unknown the range of records;
   f. address where the Security Incident occurred: and,
   g. the nature of the technologies involved.

C. Notifications must be sent electronically and encrypted via NIST or other applicable federally approved encryption techniques. If there are none, use AES256 encryption. Vendor shall use the term "data incident report" in the subject line of the email. If not all of the information is available for the notification within the specified time period Vendor shall provide the CCA with all of the available information along with the reason for the incomplete information. A delay in excess of twelve (12) hours is acceptable only if it is necessitated by other legal requirements.

D. If the information from the Breach of System Security includes Commonwealth of Virginia residents whose personal or protected information was, or is reasonably believed to have been, acquired by an unauthorized person Vendor must notify the resident(s) in accordance with Title 59.1 Chapter 53 of the Code of Virginia (Consumer

Data Protection Act). Both notifications must be within sixty (60) days of the discovery of the breach. The Vendor shall also notify, without unreasonable delay, all consumer reporting agencies, as defined under 15 U.S.C. § 1681a in effect as of January 1, 2018, and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notice. The Vendor is not required to make a disclosure under this section if, following an appropriate investigation and notice to the ATG, the Vendor reasonably determines that the breach will not likely result in harm to the affected person. The Vendor shall document the determination under this section in writing and maintain the documentation for not less than three (3) years.

The requirements of section D do not replace the requirements of sections A, B and C but are in addition to them.

HANDLING OF SECURITY INCIDENT

For Security Incidents of protected non-health information under the Vendor's control and at the CCA's discretion the Vendor will preserve all evidence regarding a security incident including but not limited to communications, documents, and logs. The Vendor will also:

- fully investigate the incident,
- cooperate fully with the CCA an Commonwealth of Virginia's investigation of, analysis of, and response to the incident,
- make a best effort to implement necessary remedial measures as soon as it is possible and,
- document responsive actions taken related to the Security Incident, including any post-incident review of events and actions taken to implement changes in business practices in providing the services covered by this Standard.

If, at the CCA's discretion, the Security Incident was due to the actions or inactions of the Vendor and at the Vendor's expense the Vendor will use a credit monitoring service, call center, forensics company, advisors, or public relations firm whose services are acceptable to the CCA. At the CCA's discretion the Vendor shall offer 3 years of credit monitoring to each person whose data was compromised. The CCA and Commonwealth of Virginia will set the scope of any investigation. The CCA can require a risk assessment for which the Vendor, the CCA will mandate the methodology and the scope. At the CCA's discretion a risk assessment may be performed by a third party at the Vendor's expense.

If the Vendor is required by federal law or regulation to conduct a Security Incident or data breach investigation, the results of the investigation must be reported to the CCA within twelve (12) hours of the investigation report being completed. If the Vendor is required by federal law or regulation to notify the affected parties, the CCA must also be notified, unless otherwise required by law.

Notwithstanding any other provision of this Standard, and in addition to any other remedies available to the CCA under law or equity, the Vendor will reimburse the CCA in full for all costs

incurred by the Commonwealth in investigation and remediation of the Security Incident including, but not limited, to providing notification to regulatory agencies or other entities as required by law or contract. The Vendor shall also pay all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident.

SECURITY INCIDENTS REGARDING PROTECTED HEALTH INFORMATION

Security Incident means the successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system that may threaten the security of the Commonwealth's data or communications or result in the exposure of data protected by federal or state laws as defined in Virginia Code § 2.2-5514. The Vendor shall alert the CCA Contact within twelve (12) hours of a Security Incident and provide daily updates to the CCA Contact at their request. The parties agree that, to the extent probes and reconnaissance scans common to the industry constitute a Security Incident, this Standard constitutes notice by Vendor of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the CCA shall be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Vendor's firewall, port scans, and unsuccessful log-on attempts, as long as such probes and reconnaissance scans do not result in a Security Incident as defined above. The CCA can require the Vendor to conduct a review or investigation within the scope and methodology determined by the CCA. At the CCA's discretion, the review or investigation may be performed by a third party at the Vendor's expense.

Notwithstanding any other provision of this Standard and in addition to any other remedies available to the CCA under law or equity, in the event the investigation or review determines that the Vendor is responsible for the Security Incident, and where the CCA incurs any costs in the investigation, review or remediation of the Security Incident, the Vendor shall reimburse the CCA in full for all such costs. Costs include, but are not limited to, providing notification to regulatory agencies or other entities as required by law or contract. In the event the investigation or review determines that the Vendor is responsible for the Security Incident, the Vendor shall also pay any and all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident, and all costs associated with the remediation of the Vendor's services and/or product(s).

ADVERSE EVENT

The Vendor shall notify the CCA Contact within two (2) days if the Vendor becomes aware that an Adverse Event has occurred. An Adverse Event is the unauthorized use of system privileges, unauthorized access to CCA data, execution of malware, physical intrusions and electronic intrusions that may include network, applications, servers, workstations and social engineering of staff. If the Adverse Event was the result of the Vendor's actions or inactions. The CCA can require a risk assessment of the Vendor the CAA mandating the methodology to be used as well as the scope. At the CCA's discretion a risk assessment may be performed by a third party at the Vendor's expense. CCA Data is any data produced or provided by the CCA as well as any data produced or provided for the CCA by a third-party.

The Vendor also acknowledges that if not kept secure, the CCA's data could be, in aggregate, used for illegal purposes.

Except as mandated by other legal requirements the Vendor shall provide notice of the disclosure only to the CCA. Notification to the CCA of an Adverse Event involving the disclosure of Commonwealth Data shall consist of a description of the data disclosed, the time the disclosure occurred, and a general description of the circumstances of the disclosure.

If all this information is not available for the notification within the specified time, the Vendor shall provide the CCA with all the available information along with the reason for the incomplete notification.

The parties agree with respect to any Adverse Event that the Vendor shall at its sole expense:

- Promptly and fully investigate the cause of the Adverse Event;
- Cooperate fully with the Commonwealth's investigation of, analysis of, and response to the incident;
- Take all reasonable steps to mitigate any harm caused to affected individuals and/or entities and to prevent any future reoccurrence;
- Provide the CCA with documentation of responsive actions taken related to the disclosure, including any post-incident review of events and actions taken to implement changes in business practices in providing the services covered by this Standard; and
- Comply with applicable data breach notification laws, including without limitation the provision of credit monitoring and other fraud prevention measures, for a period of twelve (12) months from the date that Vendor notifies Customer of the Adverse Event.

The CCA will determine if notification to individuals or entities other than the CCA is required and if the notification will be carried out by the CCA or by the Vendor. The method and content of the notification of the affected parties will be subject to approval by the CCA.

At the CCA's discretion and at the Vendor's expense the Vendor may be required to use a credit monitoring service, call center, and/or a forensics company.

Notwithstanding any other provision of this Standard, and in addition to any other remedies available to the CCA under law or equity, the Vendor will reimburse the CCA in full for all costs incurred by the CCA in the notification, investigation and remediation of the disclosure.

MALICIOUS CODE

The Vendor warrants that the service/ licensed software contains no code that does not support an application requirement.

The Vendor warrants that the service/ licensed software contains no malicious code.

The Vendor warrants that the Vendor will not insert into the service/ licensed software or an media on which the service/ licensed software is delivered any malicious or intentionally destructive code.

The Vendor warrants that the Vendor will use commercially reasonable efforts consistent with industry standards to scan for and remove any malicious code from the service/ licensed software before installation. In the event any malicious code is discovered in the service/ licensed software delivered by the Vendor, the Vendor shall provide the CCA at no charge with a copy of the applicable service/ licensed software that contains no malicious code or otherwise correct the affected portion of the services provided to the CCA. The remedies in this paragraph are in addition to other additional remedies available to the CCA.

OFFSHORE SERVICES

The Vendor will not provide access to CCA data to any entity or person(s) located outside the continental United States that are not named in this Standard without the written permission of the CCA. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States.

DATA LOCATION

The Vendor shall provide its services to the CCA as well as storage of CCA data solely from data centers in the continental United States. The Vendor will not allow any state to be provided to or accessed by any entity outside the continental United States. This restriction includes but is not limited to Vendor's employees and contractors. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States. The Vendor shall not allow its employees or contractors to store CCA data on portable devices, including personal computers, except for devices that are used and kept only at its data centers. The Vendor shall permit its personnel and contractors to access CCA data remotely only as required to provide technical support or to fulfill the terms of this Standard. If the CCA's data being remotely accessed is legally protected data or considered classified by the CCA, then:

- The device used must be password protected;
- Multifactor Authentication must be used;
- The data is encrypted to at least AES 256 both in transit and in storage;
- Data is not put onto mobile media;
- No non-electronic copies are made of the data;
- The Vendor maintains a log on what data was accessed, when it was accessed, and by whom it was accessed;

The CCA's Data Sanitization policies are to be followed when the data is no longer needed on the device used to access the data remotely.

REMOTE ACCESS
The Vendor shall prohibit its employees, agents, affiliates, and subcontractors from accessing CCA data remotely except as necessary to provide the services under this Standard and consistent with all contractual and statutory requirements. The accounts used for remote access cannot be shared accounts and must include multifactor authentication.

INTENDED DATA ACCESS METHODS
The Vendor's application will not allow a user, external to the CCA's domain, to bypass logical access controls required to meet the application's functional requirements. All database queries using the Vendor's application can only access data by methods consistent with the intended business functions. If the CCA can demonstrate the application flaw, to the CCA's satisfaction, then the Vendor will rectify the issue, to the CCA's satisfaction, at no cost to the CCA.

MULTIFACTOR AUTHENTICATION FOR HOSTED SYSTEMS
If the Vendor is hosting on their system or performing Software as a Service where there is the potential for the Vendor and/or the Vendor's subcontractor to see protected CCA data, then Multifactor Authentication (MFA) must be used to before this data can be accessed. The Vendor's MFA, at a minimum must adhere to the requirements of Level 3 Authentication Assurance for MFA as defined in NIST 800-63.

MOVEMENT OF PROTECTED CCA DATA
Any CCA data that is protected by Federal or Commonwealth of Virginia statute or requirements or by industry standards must be kept secure. When protected CCA data is moved to any of the Vendor's production or non-production systems, security must be maintained. The Vendor will ensure that that data will at least have the same level of security as it had on the CCA's environment.

ACCESS ATTEMPTS
All access attempts, whether failed or successful, to any system connected to the hosted system which can access, read, alter, intercept, or otherwise impact the hosted system or its data or data integrity shall be logged by the Vendor. For all systems, the log must include at least: log-in page used, username used, time and date stamp, incoming IP for each authentication attempt, and the authentication status, whether successful or not. Logs must be maintained not less than 7 years in a searchable database in an electronic format that is un-modifiable. At the request of the CCA, access must be granted to search those logs as needed to demonstrate compliance with the terms of this contract, and any and all audit requirements related to the hosted system.

ACCESS TO CCA DATA
Unless the contract with the CCA is terminated, CCA's access to CCA data amassed under the project covered by this Standard will not be hindered if there is a:

- Contract dispute between the parties.
- There is a billing dispute between the parties.
- The Vendor merges with or is acquired by another company.

The Vendor will also maintain all security requirements of the CCA as well as any disaster recovery commitments made under this Standard.

USAGE OF COMMONWEALTH DATA IN ARTIFICIAL INTELLIGENCE
The Vendor shall not use CCA data for the training or usage in any Artificial Intelligence model or product.

PASSWORD PROTECTION
The website(s) and or service(s) that will be hosted by the Vendor for the CCA will be password protected. If the Vendor provides the user with a preset or default password that password cannot include any Personally Identifiable Information, Protected Health Information, Federal Tax Information or any information defined under CCA statute as Confidential Information or fragment thereof.

MULTIFACTOR IDENTIFICATION
The Vendor's and the Vendor's subcontractors will not access the CCA's network except through the CCA's Multifactor Authentication process. For purposes of remote access to the CCA systems on the CCA's domain, the Vendor will adhere to the CCA's requirements for Multifactor Authentication upon receipt of notification from the CCA that such requirements have been implemented. The Vendor will also require adherence to the CCA's requirements by any of the Vendor's officers, employees, subcontractors, agents, assigns, and affiliated entities who will have remote access to CCA systems on the CCA's domain.

PASSWORD POLICIES
Password policies for all Vendor employees will be documented and provided to the CCA to assure adequate password protections are in place. Logs and administrative settings will be provided to the CCA on request to demonstrate such policies are actively enforced. The process used to reset a password must include security questions or Multifactor Authentication.

LICENSE GRANT
The Vendor grants to the CCA an annual, worldwide, nonexclusive license to use the software and associated documentation, plus any additional software which shall be added by mutual agreement of the parties during the term of this Standard.

The license usage model is based on an unknown number of Commonwealth users and an unknown number of private business users.

The license grant may be extended to any contractors, subcontractors, outsourcing Vendors and others who have a need to use the software for the benefit of the CCA.

LICENSE AGREEMENTS
Vendor warrants that it has provided to the CCA and incorporated into this Standard all license agreements, End User License Agreements, and terms of use regarding its software or any

software incorporated into its software before execution of this Standard. Failure to provide all such license agreements, End User License Agreements (EULA), and terms of use shall be a breach of this Standard at the option of the CCA. The parties agree that neither the CCA nor its end users shall be bound by the terms of any such agreements not timely provided pursuant to this paragraph and incorporated into this Standard. Any changes to the terms of this Standard or any additions or subtractions must first be agreed to by both parties in writing before they go into effect. This paragraph shall control and supersede the language of any such agreements to the contrary.

RIGHTS AND LICENSE IN AND TO CCA DATA

The parties agree that between them, all rights including all intellectual property rights in and to CCA's data shall remain the exclusive property of the CCA, and that the Vendor has a limited, nonexclusive license to use these data as provided in this Standard solely for the purpose of performing its obligations hereunder.

This Standard does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.

VENDOR'S SOFTWARE LICENSES

The Vendor must disclose to the CCA the license(s) for any third-party software and libraries used by the Vendor's product(s) (and/or in the project by the Vendor) covered under this Standard if the CCA will not be the license(s) holder. The Vendor is required to provide copies of the license(s) for the third-party software and libraries to the CCA upon request. No additional software and libraries may be added to the project after the contract is signed without notifying the CCA and providing the licenses of the software and libraries.

Open source software and libraries are also covered by this clause. Any validation of any license(s) used by the Vendor to fulfill the Vendor's commitments agreed to in this Standard is the responsibility of the Vendor, not the CCA.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Any service provider who possesses or interacts with payment card data must stay current with the Payment Card Industry (PCI) Data Security Standards. The Vendor shall enter into a contract with one or more service providers for payment card services under this Standard. The Vendor shall provide to the CCA a written acknowledgement from any such service provider with whom the Vendor contracts for such services under this Standard which acknowledgement shall CCA that the service provider is committed to maintaining proper security of the payment card data in its possession and is responsible for the security of payment card data the service provider possesses or otherwise stores, processes, or transmits on behalf of the Vendor. The Vendor must ensure that the service provider(s) used by the Vendor meet the Payment Card Industry Data Security Standards. The Vendor will annually review the service provider(s) policies and procedures and supporting documentation. The CCA at its discretion, can require the Vendor to provide the CCA with an annual report on the status of compliance of their service provider(s) with the Payment Card Industry Data Security Standards.

CURRENT PAYMENT CARD INDUSTRY DATA SECURITY STANDARD
The service provider must stay current with the Payment Card Industry (PCI) Data Security Standards. The CCA requires an acknowledgement from all service providers who possess or interact with payment card holder data that the service provider is committed to maintaining proper security of the payment card holder data in their possession and is responsible for the security of payment card data the service providers possess or otherwise store, process, or transmit on behalf of the CCA. To assure continued compliance with the current Payment Card Industry Data Security Standard, the CCA requires that the service provider acknowledge its understanding and acceptance of this requirement and provide an annual report on the service provider's Payment Card Industry Data Security Standard compliance status.

PAYMENT CARD INDUSTRY QUALIFICATION REQUIREMENTS FOR QUALIFIED INTEGRATORS AND RESELLERS
When having a payment card application implemented, configured and or supported the Vendor and any subcontractor(s) used by the Vendor to fulfill the terms of this contract will have successfully met the Payment Card Industry qualification requirements for Qualified Integrators and Resellers (QIR). Should the Vendor or any subcontractor(s) used by the Vendor have their QIR revoked or fail to maintain their QIR the Vendor must immediately cease trying to implement, configuring and or supporting payment card application(s) required by the terms of this Standard and inform the CCA Contact. At the CCA's discretion the Agreement may be terminated without any further obligation of the CCA.

BROWSER
The system, site, and/or application must be compatible with vendor-supported versions of Edge, Chrome, Safari, and Firefox browsers. Silverlight, QuickTime, PHP, Adobe ColdFusion and Adobe Flash will not be used in the system, site, and/or application. There shall be no expectation that an end-user must install any extension, add-on, plug-in or other addition to their web browser to use the system, site, and/or application.

WEBSITE PERFORMANCE REPORT
The vendor will provide the capability to include website analytics of the CCA's choosing or provide website performance reporting on-demand that includes:

- The total number of visits to the website,
- The average time the website takes to load, and
- the average length of time a transaction takes on the website.

DOMAIN NAME OWNERSHIP
Any website(s) that the Vendor creates as part of this project must have the domain name registered by and owned by the CCA. If as part of this project the Vendor is providing a service that utilizes a website with the domain name owned by the Vendor, the Vendor must give thirty (30) days' notice before abandoning the site. If the Vendor intends to sell the site to another party the Vendor must give the CCA thirty days (30) notice and grant the CCA the right of first refusal. For any site or domain, whether hosted by the Vendor or within the CCA web

infrastructure, any and all new web content should first be created in a development environment and then subjected to security scan before being approved for a move up to the production level.

WEB AND MOBILE APPLICATION

The Vendor's application is required to;

- have no code or services including web services included in or called by the application unless they provide direct, functional requirements that support the Commonwealth's business goals for the application;
- encrypt data in transport and at rest using a mutually agreed upon encryption format;
- close all connections and close the application at the end of processing;
- the documentation will be in grammatically complete text for each call and defined variables (Use no abbreviations and use complete sentences, for example) and sufficient for a native speaker of English with average programming skills to determine the meaning and/or intent of what is written without prior knowledge of the application.
- have no code not required for the functioning of application;
- have no "back doors", a back door being a means of accessing a computer program that bypasses security mechanisms, or other entries into the application other than those approved by the CCA;
- permit no tracking of device user's activities without providing a clear notice to the device user and requiring the device user's active approval before the application captures tracking data;
- have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation;
- fully disclose in the "About" information that is the listing of version information and legal notices, of the connections made, permission(s) required, and the purpose of those connections and permission(s);
- ask only for those permissions and access rights on the user's device that are required for the defined requirements of the Vendor's application;
- access no data outside what is defined in the "About" information for the Vendor's application;
- conform to Web Content Accessibility Guidelines 2.0 AA standard;
- password protect any application to be used on a mobile device.

The Vendor is required to disclose all:

- functionality;
- device and functional dependencies;
- third-party libraries used;
- methods user data is being stored, processed, or transmitted;
- methods used to notify the user how their data is being stored, processed and or transmitted;
- positive actions required by the user to give permission for their data to be stored, processed and or transmitted;

- methods used to record the user's response(s) to the notification that their data is being stored, processed and or transmitted;
- methods used to secure the data in storage, processing or transmission; and
- forms of authentication required for a user to access the application or any data it gathers stores, processes and or transmits;
- methods used to create and customize existing reports;
- methods used to integrate with external data sources;
- methods used if integrates with public cloud provider;
- methods and techniques used and the security features that protect data, if a public cloud provider is used; and
- formats the data and information uses.

If the application does not adhere to the requirements given above or the Vendor has unacceptable disclosures, at the CCA's discretion, the Vendor will rectify the issues at no cost to the CCA.

BANNED HARDWARE

The Vendor will not provide to the CCA any computer hardware or video surveillance hardware, or any components thereof, or any software that was manufactured, provided, or developed by a covered entity. As used in this paragraph, "covered entity" means the following entities and any subsidiary, affiliate, or successor entity and any entity that controls, is controlled by, or is under common control with such entity: Kaspersky Lab, Huwaei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, or any entity that has been identified as owned or controlled by, or otherwise connected to, People's Republic of China, Russian Federation, Democratic People's Republic of Korea, or the Islamic Republic of Iran. The Vendor will immediately notify the CCA if the Vendor becomes aware of credible information that any hardware, component, or software was manufactured, provided, or developed by a covered entity.

BANNED SERVICES

The Vendor warrants that any hardware or hardware components used to provide the services covered by this Standard were not manufactured by Huawei Technologies Company or ZTE Corporation or any subsidiary or affiliate of such entities. Any company considered to be a security risk by the government of the United States under the International Emergency Economic Powers Act or in a United States appropriation bill will be included in this ban.

INDEPENDENT AUDIT

The Vendor will disclose any independent audits that are performed on any of its systems. The systems included under this requirement are the Vendor's data center. This information on an independent audit(s) shall be provided to the CCA in any event, whether the audit or certification process is successfully completed or not. The audit shall also be disclosed if the

audit process did not result in a positive outcome. The Vendor will provide a copy of the findings of the audit(s) to the CCA.

ANNUAL RISK ANALYSIS

The Vendor will conduct a risk analysis annually or when there has been a significant system change. The Vendor will provide verification to the CCA Contact upon request that the risk analysis has taken place. At a minimum the risk analysis will include a review of the:

- Penetration testing of the Vendor's system.
- Security policies and procedures.
- Disaster recovery plan.
- Security incident plan.
- Business Associates Agreements.
- Inventory of physical systems, devices and media that store or utilize ePHI for completeness.

If the risk analysis provides evidence of deficiencies a risk management plan will be produced. A summary of the risk management plan will be sent to the CCA Contact. The summary will include completion dates for the plan's milestones. Updates on the risk management plan will be sent to the CCA Contact upon request.

REQUIRED REPORTING

Report	Frequency	Due Date
Breach Notification	Immediately	With 24 hour of breach identification
Scanning Reports (OS, middleware, applications, and interfaces)	Monthly	by the 5th day of the month
Information Technology Resource/Application Patching Compliance	Quarterly	by the 5th day of the first month in the quarter
Summary report of Intrusion Detection Scans and Intrusion Prevention Scans	Quarterly	by the 5th day of the first month in the quarter
Geographic Location of data being hosted	Upon change	5 days after any change in the geographic location of data storage
SOC II Type II	Initial review due within 90 days of contract effective date. Afterward, due Annually.	the Supplier is to provide a target annual date; by default, it is due by the anniversary of the contract's effective date

References:

IT-002-Information Security Policy
IT-002S1 - Incident Response Standard
IT-002S2 - Security Monitoring and Logging Standard
IT-002S3 - Account Management Standard
IT-002S4 - System and Software Patching Standard
IT-002S6 - Password and Authentication Standard
IT-002S10 - Vulnerability Assessment and Remediation Standard
IT-003-Unified Data Policy
IT-003S1 - Data Classification Standard
IT-003S2 - Data Protection Standard
IT-004-Change Management Policy

Review Schedule:

Approval and Revisions: