State of Illinois

Information and Technology Standard Terms and Conditions

For additional requirement pertaining to cloud hosted information see *Appendix A: Cloud Hosting Terms and Conditions*

1. TERMINATION

1.1 TERMINATION FOR CAUSE: The State may terminate this Contract, in whole or in part, immediately upon notice to Vendor if: (a) the State determines that the actions or inactions of Vendor, its agents, employees, or subcontractors have caused, or reasonably could cause, jeopardy to health, safety, or property, or (b) Vendor has notified the State that it is unable or unwilling to perform the Contract.

If Vendor fails to perform to the State's satisfaction any material requirement of this Contract, is in violation of a material provision of this Contract, or the State determines that Vendor lacks the financial resources to perform the Contract, the State shall provide written notice to Vendor to cure the problem identified within the period of time specified in the State's written notice. If not cured by that date the State may either: (a) immediately terminate the Contract without additional written notice or (b) enforce the terms and conditions of the Contract.

For termination due to any of the causes contained in this Section, the State retains its rights to seek any available legal or equitable remedies and damages.

1.2 TERMINATION FOR CONVENIENCE: The State may, for its convenience and with thirty (30) days' prior written notice to Vendor, terminate this Contract in whole or in part and without payment of any penalty or incurring any further obligation to Vendor.

Upon submission of invoices and proof of claim, Vendor shall be entitled to compensation for supplies and services provided in compliance with this Contract up to and including the date of termination.

1.3 OTHER TERMINATION: The State may also terminate, in whole or in part, this Contract without advance notice pursuant to Section 1.5.

1.4 SUSPENSION: The State may also suspend, in whole or in part, this Contract without advance notice pursuant to Section 1.5.

1.5 AVAILABILITY OF APPROPRIATION: This Contract is contingent upon and subject to the availability of funds. The State, at its sole option, may terminate or suspend this Contract, in whole or in part, without penalty or further payment being required, if (1) the Illinois General Assembly or the federal funding source fails to make an appropriation sufficient to pay such obligation, or if funds needed are insufficient for any reason (30 ILCS 500/20-60), (2) the Governor or the Agency reserves funds, or (3) the Agency determines, in its sole discretion or as directed by the Office of the Governor, that a reduction is necessary or advisable based upon actual or projected budgetary considerations or available funds for payment. Vendor will be notified in writing of the failure of appropriation or of a reduction or decrease and the

Agency’s election to terminate or suspend, in whole or in part, as soon as practicable. Any suspension or termination pursuant to this section will be effective upon the date of the written notice unless otherwise indicated.

2. STANDARD BUSINESS TERMS AND CONDITIONS

2.1 PAYMENT TERMS AND CONDITIONS:

2.1.1 Late Payment: Payments, including late payment charges, will be paid in accordance with the State Prompt Payment Act and rules when applicable. 30 ILCS 540; 74 Ill. Adm. Code 900. This shall be Vendor's sole remedy for late payments by the State. Payment terms contained on Vendor's invoices shall have no force or effect.

2.1.2 Minority Contractor Initiative: Any Vendor awarded a contract of $1,000 or more under Section 20-10, 20-15, 20-25 or 20-30 of the Illinois Procurement Code (30 ILCS 500) is required to pay a fee of $15. The Comptroller shall deduct the fee from the first check issued to Vendor under the Contract and deposit the fee in the Comptroller's Administrative Fund. 15 ILCS 405/23.9.

2.1.3 Expenses: The State will not pay for supplies provided or services rendered, including related expenses, incurred prior to the execution of this Contract by the Parties even if the effective date of the Contract is prior to execution.

2.1.4 Prevailing Wage: As a condition of receiving payment Vendor must (i) be in compliance with the Contract, (ii) pay its employees prevailing wages when required by law, (iii) pay its suppliers and subcontractors according to the terms of their respective contracts, and (iv) provide lien waivers to the State upon request. Examples of prevailing wage categories include public works, printing, janitorial, window washing, building and grounds services, site technician services, natural resource services, security guard and food services. The prevailing wages are revised by the Illinois Department of Labor and are available on the Illinois Department of Labor's official website, which shall be deemed proper notification of any rate changes under this subsection. Vendor is responsible for contacting the Illinois Department of Labor at 217-782-6206 or (*http://labor.illinois.gov*) to ensure understanding of prevailing wage requirements.

2.1.5 Federal Funding: This Contract may be partially or totally funded with Federal funds. If Federal funds are expected to be used, then the percentage of the good/service paid using Federal funds and the total Federal funds expected to be used will be provided to the awarded Vendor in the notice of intent to award.

2.1.6 Invoicing: By submitting an invoice, Vendor certifies that the supplies or services provided meet all requirements of this Contract, and the amount billed and expenses incurred are as allowed in this Contract. Invoices for supplies purchased, services performed, and expenses incurred through June 30 of any year must be submitted to the State no later than July 31 of that year; otherwise, Vendor may have to seek payment through the Illinois Court of Claims. 30 ILCS 105/25. All invoices are subject to statutory offset. 30 ILCS 210.

2.1.6.1 Vendor shall not bill for any taxes unless accompanied by proof that the State is subject to the tax. If necessary, Vendor may request the applicable Agency's Illinois tax exemption number and federal tax exemption information.

2.1.6.2 Vendor shall invoice at this completion of the contract unless invoicing is tied in this contract to milestones, deliverables, or other invoicing requirements agreed to in the contract.

Send invoices to:

Agency:	Department of Insurance- Get Covered Illinois
Attn:	Procurement
Email:	DOI.VendorInvoices@illinois.gov AND DOI.SBMProcurement@illinois.gov

2.2 **ASSIGNMENT**: This Contract may not be assigned or transferred in whole or in part by Vendor without the prior written consent of the State.

2.3 **SUBCONTRACTING:** For purposes of this section, subcontractors are those with contracts with an annual value exceeding $100,000 and who are specifically hired to perform all or part of the work covered by this Contract. Vendor must receive prior written approval before use of any subcontractors in the performance of this Contract. Vendor shall describe, in an attachment if not already provided, the names and addresses of all authorized subcontractors to be utilized by Vendor in the performance of this Contract, together with a description of the work to be performed by the subcontractor and the anticipated amount of money that each subcontractor is expected to receive pursuant to this Contract. If required, Vendor shall provide a copy of any subcontracts within fifteen (15) days after execution of this Contract. All subcontracts must include the same certifications that Vendor must make as a condition of this Contract. Vendor shall include in each subcontract the Standard Illinois Certifications form available from the State. If at any time during the term of this Contract, Vendor adds or changes any subcontractors, then Vendor must promptly notify, by written amendment to this Contract, the State Purchasing Officer or the Chief Procurement Officer of the names and addresses, the expected amount of money that each new or replaced subcontractor will receive pursuant to this Contract, and the general type of work to be performed. 30 ILCS 500/20-120.

2.4 **AUDIT/RETENTION OF RECORDS:** Vendor and its subcontractors shall maintain books and records relating to the performance of the Contract or subcontract and necessary to support amounts charged to the State pursuant the Contract or subcontract. Books and records, including information stored in databases or other computer systems, shall be maintained by Vendor for a period of three (3) years from the later of the date of final payment under the Contract or completion of the Contract, and by the subcontractor for a period of three (3) years from the later of final payment under the term or completion of the subcontract. If Federal funds are used to pay Contract costs, Vendor and its subcontractors must retain their respective records for five (5) years. Books and records required to be maintained under this section shall be available for review or audit by representatives of: the procuring Agency, the Auditor General, the Executive Inspector General, the Chief Procurement Officer, State of Illinois internal auditors or other governmental entities with monitoring authority, upon reasonable notice and during normal business hours. Vendor and its subcontractors shall cooperate fully with any such audit and with any investigation conducted by any of these entities. Failure to maintain books and records required by this section shall establish a presumption in favor of the State for the recovery of any funds paid by the State under this Contract or any subcontract for which adequate books and records are not available to support the purported disbursement. Vendor or subcontractors shall not impose a charge for audit or examination of Vendor's or subcontractors' books and records. 30 ILCS 500/20-65. Vendor and its subcontractors shall upon reasonable notice appear before and respond to requests for information from the Illinois Works Review Panel. 30 ILCS 559/20-25(d).

2.5 TIME IS OF THE ESSENCE: Time is of the essence with respect to Vendor's performance of this Contract. Vendor shall continue to perform its obligations while any dispute concerning the Contract is being resolved unless otherwise directed by the State.

2.6 NO WAIVER OF RIGHTS: Except as specifically waived in writing, failure by a Party to exercise or enforce a right does not waive that Party's right to exercise or enforce that or other rights in the future.

2.7 FORCE MAJEURE: Failure by either Party to perform its duties and obligations will be excused by unforeseeable circumstances beyond its reasonable control and not due to its negligence, including acts of nature, acts of terrorism, riots, labor disputes, fire, flood, explosion, and governmental prohibition. The non-declaring Party may cancel this Contract without penalty if performance does not resume within thirty (30) days of the declaration.

2.8 CONFIDENTIAL INFORMATION: Each Party to this Contract, including its agents and subcontractors, may have or gain access to confidential data or information owned or maintained by the other Party in the course of carrying out its responsibilities under this Contract. Vendor shall presume all information received from the State or to which it gains access pursuant to this Contract is confidential. Vendor information, unless clearly marked as confidential and exempt from disclosure under the Illinois Freedom of Information Act ("FOIA") (5 ILCS 140), shall be considered public. Unless otherwise agreed by the Parties, and then only upon receipt of the State's prior written consent, Vendor and its subcontractors shall not access or attain any personally identifiable information or sensitive information on or from the State's systems, and Vendor agrees that any such information is the confidential information of the State. In any event, Vendor shall implement and maintain reasonable security measures to protect any and all data, information, and records disclosed by the State under this Contract from unauthorized access, acquisition, destruction, use, modification, or disclosure. No confidential data collected, maintained, or used in the course of performance of this Contract shall be disseminated except as authorized by law and with the written consent of the disclosing Party, either during the period of this Contract or thereafter. The receiving Party must return any and all data collected, maintained, created or used in the course of the performance of this Contract, in a non-proprietary, readily usable format, promptly at the end of this Contract, or earlier at the request of the disclosing Party, or notify the disclosing Party in writing of its destruction. The foregoing obligations shall not apply to confidential data or information lawfully in the receiving Party's possession prior to its acquisition from the disclosing Party; received in good faith from a third Party not subject to any confidentiality obligation to the disclosing Party; now is or later becomes publicly known through no breach of confidentiality obligation by the receiving Party; or that is independently developed by the receiving Party without the use or benefit of the disclosing Party's confidential information.

2.9 USE AND OWNERSHIP: All work performed or supplies created by Vendor under this Contract, whether written documents or data, goods, or deliverables of any kind, shall be deemed work for hire under copyright law and all intellectual property and other laws, and the State of Illinois is granted sole and exclusive ownership to all such work, unless otherwise agreed in writing. Vendor hereby assigns to the State all right, title, and interest in and to such work including any related intellectual property rights, and/or waives any and all claims that Vendor may have to such work including any so-called "moral rights" in connection with the work. Vendor acknowledges the State may use the work product for any purpose. Confidential data or information contained in such work shall be subject to the confidentiality provisions of this Contract.

2.10 INDEMNIFICATION AND LIABILITY: Vendor shall indemnify and hold harmless the State, its agencies, officers, employees, agents, and volunteers from any and all costs, demands, expenses, losses, claims, damages, liabilities, settlements, and judgments, including in-house and Contracted attorneys’ fees and expenses, related to: (a) any breach or violation by Vendor of any of its certifications, representations, warranties, covenants, or agreements; (b) any actual or alleged death or injury to any person, damage to any real or personal property, or any other damage or loss claimed to result in whole or in part from Vendor’s negligent performance; (c) any act, activity, or omission of Vendor or any of its employees, representatives, subcontractors, or agents; or (d) any actual or alleged claim that the products or services provided under this Contract infringe, misappropriate, or otherwise violate any intellectual property rights (including but not limited to patent, copyright, trade secret, or trademark rights) of a third party. Vendor shall also defend (subject to the consent of the Office of the Attorney General (“OAG”)) the State against any and all third-party claims related to this Contract. In accordance with Article VIII, Section 1(a) and (b) of the Constitution of the State of Illinois and 1973 Illinois Attorney General Opinion 78, the State may not indemnify private parties absent express statutory authority permitting the indemnification. The State shall not be liable for indirect, special, consequential, or punitive damages.

4.10.1 DATA BREACH PREVENTION, NOTICE, AND REMEDIATION: Vendor shall ensure the security, storage, and integrity of the State’s content, data, computers, networks, and systems (which may include the use of encryption technology to protect the State’s content and data from unauthorized access). Notwithstanding anything to the contrary in this Contract, to the extent that Vendor experiences or causes an information breach or security incident that impacts the State’s data, content, computers, systems, or networks, Vendor shall immediately notify the State and will use best efforts to immediately remedy any such breach or incident, and to prevent any further breach or incident, at Vendor’s expense, in accordance with applicable privacy rights, laws, regulations, policies, and standards, including but not limited to the Illinois Personal Information Protection Act (815 ILCS 530). Vendor shall reimburse the State for any and all costs incurred by the State in responding to, and mitigating damages caused by, any such breach or security incident, including all costs of notice and/or remediation.

4.10.2 DATA LOSS AND DAMAGE TO STATE COMPUTER SYSTEMS: Vendor shall adhere to all indemnification and liability obligations stated in this Contract and will remain liable where any damage or impairment to the State’s computers, systems, and networks, or any loss or corruption of the State’s data or content, is due to Vendor’s negligent or intentional acts and omissions. Further, Vendor shall reimburse the State for any and all costs incurred by the State in restoring such data, content, computers, systems, or networks.

2.11 INSURANCE: Vendor shall, at all times during the term of this Contract and any renewals or extensions, maintain and provide a Certificate of Insurance naming the State as an additionally insured for all required bonds and insurance. Certificates may not be modified or canceled until at least thirty (30) days' notice has been provided to the State. Vendor shall provide: (a) General Commercial Liability insurance in the amount of $1,000,000 per occurrence (Combined Single Limit Bodily Injury and Property Damage) and $2,000,000 Annual Aggregate; (b) Auto Liability, including Hired Auto and Non-owned Auto (Combined Single Limit Bodily Injury and Property Damage), in amount of $1,000,000 per occurrence; and (c) Worker's Compensation Insurance in the amount required by law. Insurance shall not limit Vendor's obligation to indemnify, defend, or settle any claims.

2.12 INDEPENDENT CONTRACTOR: Vendor shall act as an independent contractor and not an agent or employee of, or joint venturer with the State. All payments by the State shall be made on that basis.

2.13 SOLICITATION AND EMPLOYMENT: Vendor shall not employ any person employed by the State during the term of this Contract to perform any work under this Contract. Vendor shall give notice immediately to the Agency's director if Vendor solicits or intends to solicit State employees to perform any work under this Contract.

2.14 COMPLIANCE WITH THE LAW: Vendor, its employees, agents, and subcontractors shall comply with all applicable federal, state, and local laws, rules, ordinances, regulations, orders, federal circulars and all license and permit requirements in the performance of this Contract. Vendor shall be in compliance with applicable tax requirements and shall be current in payment of such taxes. Vendor shall obtain at its own expense, all licenses and permissions necessary for the performance of this Contract.

2.15 BACKGROUND CHECK: Vendor affirms that it checks the criminal records of all applicants for felony convictions and misdemeanor convictions involving a violent act or threat of violence within five (5) years prior to employment, where permitted by law.

Whenever the State deems it reasonably necessary for security reasons, the State may conduct, at its expense, criminal and driver history background checks of Vendors and subcontractors, officers, employees, or agents performing services on State owned, leased, or controlled property. Vendor or subcontractor shall reassign immediately any such individual who, in the reasonable opinion of the State, does not pass the background checks. The background checks shall be in compliance with all federal laws. The State further agrees as follows:

- Use of the information collected will be for the specific purpose of facilitating a background check;
- All information collected will be treated as confidential;
- The State will limit access to the information received and will properly store it in a reasonably secure manner;
- The State will promptly dispose in an appropriate manner all collected information when the purpose for which it was originally collected is no longer valid; and

- State must provide notice and consent forms. Vendor's and subcontractor's officers, employees, or agents performing services on state owned, leased, or controlled property not consenting shall be reassigned.

However, in no event can Vendor agree to waive the rights of its employees, nor can Vendor provide the State with any information protected by law, including but not limited to Vendor's background check data.

2.16 APPLICABLE LAW:

2.16.1 **PREVAILING LAW:** This Contract shall be construed in accordance with and is subject to the laws and rules of the State of Illinois.

2.16.2 **EQUAL OPPORTUNITY:** The Department of Human Rights' Equal Opportunity requirements are incorporated by reference. 44 ILL. ADM. CODE 750.

2.16.3 **COURT OF CLAIMS; ARBITRATION; SOVEREIGN IMMUNITY:** Any claim against the State arising out of this Contract must be filed exclusively with the Illinois Court of Claims. 705 ILCS 505/1. The State shall not enter into binding arbitration to resolve any dispute arising out of this Contract. The State of Illinois does not waive sovereign immunity (including all rights provided in the State Lawsuit Immunity Act, 745 ILCS 5) by entering into this Contract.

2.16.4 **OFFICIAL TEXT:** The official text of the statutes cited herein is incorporated by reference. An unofficial version can be viewed at (*www.ilga.gov/legislation/ilcs/ilcs.asp*).

2.17 ANTI-TRUST ASSIGNMENT: If Vendor does not pursue any claim or cause of action it has arising under Federal or State antitrust laws relating to the subject matter of this Contract, then upon request of the Illinois Attorney General, Vendor shall assign to the State all of Vendor's rights, title, and interest in and to the claim or cause of action.

2.18 CONTRACTUAL AUTHORITY: The Agency that signs this Contract on behalf of the State of Illinois shall be the only State entity responsible for performance and payment under this Contract. When the Chief Procurement Officer or authorized designee or State Purchasing Officer signs in addition to an Agency, he/she does so as approving officer and shall have no liability to Vendor. When the Chief Procurement Officer or authorized designee or State Purchasing Officer signs a master Contract on behalf of State agencies, only the Agency that places an order or orders with Vendor shall have any liability to Vendor for that order or orders.

2.19 EXPATRIATED ENTITIES: Except in limited circumstances, no business or member of a unitary business group, as defined in the Illinois Income Tax Act, shall submit a bid for or enter into a Contract with a State agency if that business or any member of the unitary business group is an expatriated entity.

2.20 NOTICES: Notices and other communications provided for herein shall be given in writing via electronic mail whenever possible. If transmission via electronic mail is not possible, then notices and other communications shall be given in writing via registered or certified mail with return receipt requested, via receipted hand delivery or via courier (UPS, Federal Express, or other similar and reliable carrier). Notices shall be sent to the individuals who signed this Contract using the contact information provided with the signatures. Each such notice shall be deemed to have been provided at the time it is actually received. By giving notice, either Party may change its contact information.

2.21 MODIFICATIONS AND SURVIVAL: Amendments, modifications, and waivers must be in writing and signed by authorized representatives of the Parties. Any provision of this Contract officially declared void, unenforceable, or against public policy, shall be ignored and the remaining provisions shall be interpreted, as far as possible, to give effect to the Parties' intent. All provisions that by their nature would be expected to survive, shall survive termination. In the event of a conflict between the State's and Vendor's terms, conditions, and attachments, the State's terms, conditions, and attachments shall prevail.

2.22 PERFORMANCE RECORD / SUSPENSION: Upon request of the State, Vendor shall meet to discuss performance or provide contract performance updates to help ensure proper performance of this Contract. The State may consider Vendor's performance under this Contract and compliance with law and rule to determine whether to continue this Contract, suspend Vendor from doing future business with the State for a specified period of time, or whether Vendor can be considered responsible on specific future contract opportunities.

2.23 FREEDOM OF INFORMATION ACT: This Contract and all related public records maintained by, provided to or required to be provided to the State are subject to the Illinois Freedom of Information Act ("FOIA") (5 ILCS 140) notwithstanding any provision to the contrary that may be found in this Contract.

2.24 SCHEDULE OF WORK: Any work performed on State premises shall be performed during the hours designated by the State and performed in a manner that does not interfere with the State and its personnel.

2.25 WARRANTIES FOR SUPPLIES AND SERVICES:

2.25.1. Vendor warrants that the supplies furnished under this Contract will: (a) conform to the standards, specifications, drawing, samples, or descriptions furnished by the State or furnished by Vendor and agreed to by the State, including but not limited to all specifications attached as exhibits hereto; (b) be merchantable, of good quality and workmanship, and free from defects for a period of twelve months or longer if so specified in writing, and fit and sufficient for the intended use; (c) comply with all federal and state laws, regulations, and ordinances pertaining to the manufacturing, packing, labeling, sale, and delivery of the supplies; (d) be of good title and be free and clear of all liens and encumbrances and; (e) not infringe any patent, copyright, or other intellectual property rights of any third party. Vendor agrees to reimburse the State for any losses, costs, damages, or expenses, including without limitations, reasonable attorney's fees and expenses, arising from failure of the supplies to meet such warranties.

2.25.2. Vendor shall ensure that all manufacturers' warranties are transferred to the State and shall provide to the State copies of such warranties. These warranties shall be in addition to all other warranties, express, implied, or statutory, and shall survive the State's payment, acceptance, inspection, or failure to inspect the supplies.

2.25.3. Vendor warrants that all services will be performed to meet the requirements of this Contract in an efficient and effective manner by trained and competent personnel. Vendor shall monitor performances of each individual and shall immediately reassign any individual who does not perform in accordance with this Contract, who is disruptive or not respectful of others in the workplace, or who in any way violates the Contract or State policies.

2.26 REPORTING, STATUS AND MONITORING SPECIFICATIONS: Vendor shall immediately notify the State of any event that may have a material impact on Vendor's ability to perform this Contract.

2.27 EMPLOYMENT TAX CREDIT: Vendors who hire qualified veterans and certain ex-offenders may be eligible for tax credits. 35 ILCS 5/216, 5/217. Please contact the Illinois Department of Revenue (telephone #: 217-524-4772) for information about tax credits.

2.28 SUPPLEMENTAL TERMS: Notwithstanding any provision to the contrary in Vendor's supplemental terms and conditions, or in any licensing agreement attached hereto:

2.28.1 The procuring Agency and the State do not waive sovereign immunity (including all rights provided in the State Lawsuit Immunity Act, 745 ILCS 5);

2.28.2 The procuring Agency and the State do not consent to be governed by the laws of any state other than Illinois;

2.28.3 The procuring Agency and the State do not consent to be represented in any legal proceeding by any person or entity other than the Illinois Attorney General or his or her designee;

2.28.4 The procuring Agency and the State shall not be bound by the terms and conditions contained in any click-wrap agreement, click-wrap license, click-through agreement, click-through license, end user license agreement, or any other agreement or license contained or referenced in the software or any quote provided by Vendor, except as attached to this Contract.

2.28.5 The procuring Agency and the State shall not indemnify Vendor or its subcontractors (including any equipment manufacturers or software companies);

2.28.6 Vendor shall indemnify the procuring Agency and State pursuant to the terms and conditions of the Indemnification and Liability clause of this Contract;

2.28.7 Vendor's liability shall be governed by the terms and conditions contained in the Indemnification and Liability clause of this Contract; and

2.28.8 Vendor must ensure that all information technology, including electronic information, software, systems and equipment, developed or provided under this contract complies with the applicable requirements of the Illinois Information Technology Accessibility Act Standards as published at (www.dhs.state.il.us/iitaa). 30 ILCS 587.

2.29 SECURITY REQUIREMENTS: The State of Illinois has specific security requirements for information and systems. Vendor must ensure these requirements are fully understood and allocate sufficient project time and resources to address the security requirements.

An information security risk assessment, data classification and system categorization process, and the submission of a system security plan must be completed and submitted to the Department of Innovation & Technology, Division of Information Security prior to the commencement of system development or solution delivery activities. Vendor must participate with the risk assessment and data classification and system categorization process. The formal risk assessment and data classification and system categorization process will be administered by the Illinois Department of Innovation & Technology, Division of Information Security. Vendor program and project management personnel must ensure the coordination of these activities with State of Illinois program and project management personnel.

If not specifically addressed in other Vendor Information Technology Requirements, Vendor must adhere to State of Illinois and Illinois Department of Innovation & Technology technology and security Policies, Procedures, and Standards. https://www2.illinois.gov/sites/doit/support/policies/Pages/default.aspx

Vendor must also adhere to a minimum security baseline as identified in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Systems and Organizations. https://doi.org/10.6028/NIST.SP.800-53r5. If not specifically addressed in other Vendor Information Technology Requirements, Vendors must assure the adoption of, at minimum, the low security control baselines. Exceptions to this requirement must be approved by the Illinois Department of Innovation & Technology, Division of Information Security.

Cloud solutions must adhere to recommendations of the Cloud Security Alliance. Vendors may find guidance and cross-referencing to the NIST 800-53, Revision 5 with the Cloud Security Alliance controls at [CSA (cloudsecurityalliance.org)].

State and Federal laws, rules, and regulations as well as industry-specific guidelines require specific and often enhanced security controls on information and systems. The State of Illinois is required to comply with the below laws, standards, and regulations. Vendors must ensure compliance with the below as appropriate based upon the formal risk assessment to include a data classification and system categorization process.

- Illinois Identity Protection Act (5 ILCS 179)
- Illinois Personal Information Protection Act (815 ILCS 530)
- The Family Educational Rights and Privacy Act (“FERPA”) (20 U.S.C. § 1232g; 34 CFR Part 99)
- Federal Bureau of Investigations Criminal Justice Information Services (“CJIS”) Security Policy, version 5.5, issued June 26, 2016
- Federal Centers for Medicare & Medicaid Services (“CMS”) MARS-E Document Suite, Version 2.0 Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges November 10, 2015.

• Federal Centers for Medicare & Medicaid Services Information Security Acceptable Risk Safeguards (“ARS”) CMS Minimum Security Requirements Version 2.0 September 20, 2013.

Appendix A: Cloud Hosting Terms and Conditions

State of Illinois Security Requirements:

1. Vendor will notify the State of Illinois' Chief Information Security Officer within 24 hours of knowledge of any information breach or other security incident which impacts State of Illinois data. Email notification to: DoIT.Security@illinois.gov and Subject Line should state "Breach Notification."

2. Vendor shall have a documented security incident policy and plan. Vendor must supply a copy at the request of the State of Illinois.

3. Vendor must comply with all United States Federal and State of Illinois laws, rules, and regulations.

4. Vendor must comply with all of the State of Illinois Enterprise Security Policies (https://www2.illinois.gov/sites/doit/support/policies/Pages/default.aspx).

5. Vendor must ensure that all information technology, including electronic information, software, systems and equipment, developed or provided under this contract complies with the applicable requirements of the Illinois Information Technology Accessibility Act Standards as published at (www.dhs.state.il.us/iitaa). 30 ILCS 587. If available, Vendor must provide the State of Illinois their most recent Voluntary Product Accessibility Template (VPAT).

6. Vendor program and project management personnel must ensure coordination of activities with the State of Illinois governance program. Vendor must comply with all policies, standards, and procedures defined by the State of Illinois Department of Innovation and Technology's Enterprise Portfolio Management Office.

7. Vendor's system must interface with the State of Illinois' identity and access management solutions if authentication is required for access to the system.

8. Vendor's system must log activity within the system and have capacity to forward log information to the State of Illinois' security incident and event management system (SIEM). Vendor must meet the State of Illinois' Minimum Logging Requirements for the term of the Contract.

    8.1. (See Security Appendix S1)

9. Vendor certifies it has undertaken independent third-party audit Statement on Standards for Attestation Engagements (SSAE-18) certifications and must provide the State of Illinois with a System Operation Controls report (SOC 1) annually and applicable bridge/gap letter when vendor is hosting State of Illinois financial information.

10. Vendor certifies it can comply with at least one of the following requirements listed in order of preference.

    10.1 Vendor certifies it has undertaken independent third-party audit Statement on Standards for Attestation Engagements (SSAE-18) certifications and must provide the State of Illinois with a System Operation Controls report (SOC 2 type 2) annually and applicable bridge/gap letter.

    10.2 Vendor must provide the State of Illinois with a 3rd party risk assessment of the Vendor's system conducted within the last year including a 3rd party penetration test.

    10.3 Vendor must provide the State of Illinois with a 3rd party risk assessment of the Vendor's system conducted within the last year.

    10.4 Vendor must provide the State of Illinois with a 3rd party penetration test conducted within the last year.

    10.5 Vendor must perform an internal security controls assessment to demonstrate compliance with the State of Illinois Vendor Security Controls, based on the current revision of NIST 800-53 security controls for a moderate system. *(See Security Appendix S2)*

11. Vendor must participate in an annual risk assessment and data classification and system categorization process. The formal risk assessment will be administered by the State of Illinois.

    If Vendor cannot provide the SOC 1 and/or 2 report required above and any necessary bridge/gap letter or another appropriate third-party risk assessment as determined by the State of Illinois, then Vendor must perform an internal security controls assessment to demonstrate compliance with the State of Illinois Vendor Security Controls, based on the current revision of NIST 800-53 security controls for a moderate system. Vendor must provide attestation of compliance along with the results of this assessment documented in a Security Assessment Report (SAR) to the State of Illinois. This does not relieve the Vendor of the above requirement to submit a required SOC 1 and/or SOC 2.

    11.1. (See Security Appendix S2)

12. Vendor must provide a Plan of Action and Milestones (POA&M) to the State of Illinois that addresses any control deficiencies identified during the State of Illinois' risk assessment, review of Vendor's SOC report(s), third-party assessment, and internal security controls assessment. The POA&M should describe the deficiencies in the security controls, address the residual risk, and detail plans for remediation. Vendor must provide the State of Illinois monthly updates regarding progress toward remediation of identified deficiencies.

12.1. *(See Security Appendix S3)*

13. Vendor must complete and provide the State of Illinois an Authority to Operate (ATO) or Authority to Connect (ATC) packet at the State of Illinois' request. This packet must be renewed annually.

    13.1. *(See Security Appendix S4)*

14. Vendor must ensure all hosted data pertinent to this contract shall remain located within the contiguous United States.

15. Vendor must ensure encryption of State of Illinois data at rest and in motion. This encryption must comply with encryption security controls as defined in the most current version of the Federal Information Processing Standard (FIPS) 140 using Advanced Encryption Standard (AES) encryption with a minimum key length of 256 bits. Vendor must provide proof of encryption. Vendor must provide the State of Illinois with the capabilities to manage encryption keys for data at rest.

16. Vendor must store data in a non-proprietary, readily accessible format, or Vendor must provide a solution, at no additional cost to the State of Illinois, to extract any State of Illinois data stored in Vendor's solution.

17. Vendor must only use State of Illinois data, for the purposes stated in this contract.

18. Vendor must maintain a robust and reliable data backup system. Vendor must supply a description of backup methodology, and this methodology must meet defined Maximum Tolerable Downtime (MTD) and Return to Operations (RPO) requirements.

19. At the State's request, Vendor must provide a written disaster recovery methodology and provide proof of annual disaster recovery testing, including issues discovered and remediation plans for the issues discovered.

20. Vendor may not use any State of Illinois data in any non-production system or in any other system outside the application/service procured under this contract.

21. Vendor must provide a copy of all State of Illinois data (in a non-proprietary format) to the State of Illinois without delay upon request by the State of Illinois.

22. Vendor must provide a copy of all State of Illinois data (in a non-proprietary format) to the State of Illinois prior to termination of contract.

23. Vendor must sanitize all media that contains or contained State of Illinois data. Vendor must use the more current revision of NIST Special Publication 800-88; Guidelines for Media

Sanitization. Vendor must provide the State of Illinois with a written certification of media sanitization including the method, date and time.

24. Vendor must use a form of "crypto shredding" acceptable to the State of Illinois for rendering all State of Illinois data hosted by the Vendor inaccessible after a copy of all data has been provided to the State of Illinois.

25. Vendor and/or its agents must not resell nor otherwise redistribute information gained from its access to the State of Illinois data.

26. Vendor must not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the State of Illinois.

27. Vendor must allow the State of Illinois to perform vulnerability assessments.

    27.1. (See Security Appendix S5)

28. Vendor must immediately remediate critical, high, and medium vulnerabilities within the application that are detected during the security assessments and are determined by the State of Illinois to pose an unacceptable risk.

29. Vendor must secure independent third-party penetration testing at regular intervals, in accordance with Cloud Security Alliance (CSA) and Open Web Application Security Project (OWASP) recommendations. Vendor must supply the results of the testing to the State of Illinois upon request.

30. Vendor must supply a list of all non-proprietary/open source software used in their solution. Vendor must also include the version and Open Source Initiative (OSI) approved license type used for any open source software. If Open Source uses non-OSI approved licensing Vendor must include licensing terms and conditions.

Security Appendix S1 – Minimum Logging Requirements

- Input validation failures (e.g., protocol violations, unacceptable encodings, invalid parameter names and values)
- Output validation failures (e.g., database record set mismatch, invalid data encoding)
- Authentication successes and failures
- Authorization (access control) failures
- Session management failures (e.g., cookie session identification value modification)
- Application errors and system events (e.g., syntax and runtime errors, connectivity problems, performance issues, third-party service error messages, file system errors, file upload virus detection, configuration changes)
- Application and related systems start-ups and shut downs, and logging initialization (starting, stopping, or pausing)
- Use of higher-risk functionality (e.g., network connections, addition or deletion of users, changes to privileges, assigning users to tokens, adding or deleting tokens, use of systems administrative privileges, access by application administrators, all actions by users with administrative privileges, access to payment cardholder data, use of data encrypting keys, key changes, creation and deletion of system-level objects, data import and export including screen-based reports, submission of user-generated content - especially file uploads)
- Legal and other opt-ins (e.g., permissions for mobile phone capabilities, terms of use, terms & conditions, personal data usage consent, permission to receive marketing communications)

Security Appendix S2: Security Controls for Vendors

Authoritative Document **NIST 800-53 v4 – Security and Privacy Controls**

Access and Control (AC)

Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

AC Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Access Control Policy and Procedures	AC-1	
• Account Management	AC-2	(1), (2), (3), (4)
• Access Enforcement	AC-3	
• Information Flow Enforcement	AC-4	
• Separation of Duties	AC-5	
• Least Privilege	AC-6	(1), (2), (5), (9), (10)
• Unsuccessful Logon Attempts	AC-7	
• System Use Notification	AC-8	
• Session Lock	AC-11	(1)
• Session Termination	AC-12	
• Permitted Actions without Identification or Authentication	AC-14	
• Remote Access	AC-17	(1), (2), (3), (4)
• Wireless Access	AC-18	(1)
• Access Control for Mobile Devices	AC-19	(5)
• Use of External Information Systems	AC-20	(1), (2)
• Information Sharing	AC-21	
• Publicly Accessible Content	AC-22	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

Awareness and Training (AT)

Organizations must (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

AT - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	**Control #**	**Enhancement #'s**
• Security Awareness and Training Policy and Procedures	AT-1	
• Security Awareness Training	AT-2	(2)
• Role-Based Security Training	AT-3	
• Security Training Records	AT-4	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

Audit and Accountability (AU)

Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users, so they can be held accountable for their actions.

AU - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Audit and Accountability Policy and Procedure	AU-1	
• Audit Events	AU-2	(3)
• Content of Audit Records	AU-3	(1)
• Audit Storage Capacity	AU-4	
• Response to Audit Processing Failures	AU-5	
• Audit Review, Analysis, and Reporting	AU-6	(1), (3)
• Audit Reduction and Report Generation	AU-7	(1)
• Time Stamps	AU-8	(1)
• Protection of Audit Information	AU-9	(4)
• Audit Record Retention	AU-11	
• Audit Generation	AU-12	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

Certification, Accreditation, and Security Assessments (CA)

Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organization information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

CA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	**Control #**	**Enhancement #'s**
• Security Assessment and Authorization Policy and Procedures	CA-1	
• Security Assessments	CA-2	(1)
• System Interconnections	CA-3	(5)
• Plan of Action and Milestones	CA-5	
• Security Authorization	CA-6	
• Continuous Monitoring	CA-7	(1)
• Internal System Connections	CA-9	

Authority	
NIST	SP 800-53 Security and Privacy Controls
NIST	SP 800-53A Assessing Security Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

Configuration Management (CM)

Vendors must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

CM - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Configuration Management Policy and Procedures	CM-1	
• Baseline Configuration	CM-2	(1), (3), (7)
• Configuration Change Control	CM-3	(2)
• Security Impact Analysis	CM-4	
• Access Restrictions for Change	CM-5	
• Configuration Settings	CM-6	
• Least Functionality	CM-7	(1), (2), (4)
• Information System Component Inventory	CM-8	(1), (3), (5)
• Configuration Management Plan	CM-9	
• Software Usage Restrictions	CM-10	
• User-Installed Software	CM-11	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

Contingency Planning (CP)

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

CP - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Contingency Planning Policy and Procedures	CP-1	
• Contingency Plan	CP-2	(1), (3), (8)
• Contingency Training	CP-3	
• Contingency Plan Testing	CP-4	(1)
• Alternate Storage Site	CP-6	(1), (3)
• Alternate Processing Site	CP-7	(1), (2), (3)
• Telecommunications Services	CP-8	(1), (2)
• Information System Backup	CP-9	(1)
• Information System Recovery and Reconstitution	CP-10	(2)

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

Identification and Authentication (IA)

Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices as a prerequisite to allowing access to organizational information systems.

IA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Identification and Authentication Policy and Procedures	IA-1	
• Identification and Authentication (Organizational Users)	IA-2	(1), (2), (3), (8), (11), (12)
• Device Identification and Authentication	IA-3	
• Identifier Management	IA-4	
• Authentication Management	IA-5	(1), (2), (3), (11)
• Authenticator Feedback	IA-6	
• Cryptographic Module Authentication	IA-7	
• Identification and Authentication (Non-Organizational Users)	IA-8	(1), (2), (3), (4)

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

Incident Response (IR)

Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

IR - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Incident Response Policy and Procedures	IR-1	
• Incident Response Training	IR-2	
• Incident Response Testing	IR-3	(2)
• Incident Handling	IR-4	(1)
• Incident Monitoring	IR-5	
• Incident Reporting	IR-6	(1)
• Incident Response Assistance	IR-7	(1)
• Incident Response Plan	IR-8	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

Maintenance (MA)

Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

MA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	**Control #**	**Enhancement #'s**
• System Maintenance Policy and Procedures	MA-1	
• Controlled Maintenance	MA-2	
• Maintenance Tools	MA-3	(1), (2)
• Nonlocal Maintenance	MA-4	(2)
• Maintenance Personnel	MA-5	
• Timely Maintenance	MA-6	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

Media Protection (MP)

Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

MP - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	**Control #**	**Enhancement #'s**
• Media Protection Policy and Procedures	MP-1	
• Media Access	MP-2	
• Media Marking	MP-3	
• Media Storage	MP-4	
• Media Transport	MP-5	(4)
• Media Sanitization	MP-6	
• Media Use	MP-7	(1)

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

Physical and Environmental Protection (PE)

Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

PE - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Physical and Environmental Protection Policy and Procedures	PE-1	
• Physical Access Authorizations	PE-2	
• Physical Access Control	PE-3	
• Access Control for Transmission Medium	PE-4	
• Access Control for Output Devices	PE-5	
• Monitoring Physical Access	PE-6	(1)
• Visitor Access Records	PE-8	
• Power Equipment and Cabling	PE-9	
• Emergency Shutoff	PE-10	
• Emergency Power	PE-11	
• Emergency Lighting	PE-12	
• Fire Protection	PE-13	(3)
• Temperature and Humidity Controls	PE-14	
• Water Damage Protection	PE-15	
• Delivery and Removal	PE-16	
• Alternate Work Site	PE-17	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

Planning (PL)

Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

PL - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	**Control #**	**Enhancement #'s**
• Security Planning Policy and Procedures	PL-1	
• System Security Plan	PL-2	(3)
• Rules of Behavior	PL-4	(1)
• Information Security Architecture	PL-8	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

Personnel Security (PS)

Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions, such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

PS - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	**Control #**	**Enhancement #'s**
• Personnel Security Policy and Procedures	PS-1	
• Position Risk Designation	PS-2	
• Personnel Screening	PS-3	
• Personnel Termination	PS-4	
• Personnel Transfer	PS-5	
• Access Agreements	PS-6	
• Third-Party Personnel Security	PS-7	
• Personnel Sanctions	PS-8	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

Risk Assessment (RA)

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

RA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Risk Assessment Policy and Procedures	RA-1	
• Security Categorization	RA-2	
• Risk Assessment	RA-3	
• Vulnerability Scanning	RA-5	(1), (2), (5)

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

System and Services Acquisition (SA)

Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and or services outsourced from the organizations.

SA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	**Control #**	**Enhancement #'s**
• System and Services Acquisition Policy and Procedures	SA-1	
• Allocation of Resources	SA-2	
• System Development Life Cycle	SA-3	
• Acquisition Process	SA-4	(1), (2), (9), (10)
• Information System Documentation	SA-5	
• Security Engineering Principles	SA-8	
• External Information System Services	SA-9	(2)
• Developer Configuration Management	SA-10	
• Developer Security Testing and Evaluation	SA-11	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

System and Communications Protection (SC)

Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries for the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

SC - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• System and Communication Protection Policy and Procedures	SC-1	
• Application Partitioning	SC-2	
• Information in Shared Resources	SC-4	
• Denial of Service Protection	SC-5	
• Boundary Protection	SC-7	(3), (4), (5), (7)
• Transmission Confidentiality and Integrity	SC-8	(1)
• Network Disconnect	SC-10	
• Cryptographic Key Establishment and Management	SC-12	
• Cryptographic Protection	SC-13	
• Collaborative Computing Devices	SC-15	
• Public Key Infrastructure Certificates	SC-17	
• Mobile Code	SC-18	
• Voice Over Internet Protocol	SC-19	
• Secure Name/Address Resolution Service (Authoritative Source)	SC-20	
• Secure Name/Address Resolution Service (Recursive or Caching Resolver)	SC-21	
• Architecture and Provisioning for Name/Address Resolution Service	SC-22	
• Session Authenticity	SC-23	
• Protection of Information at Rest	SC-28	
• Process Isolation	SC-39	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

System and Information Integrity (SI)

Organizations must: (i) identify, report, and correct information and information systems flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems, and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

SI - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• System and Information Integrity Policy and Procedures	SI-1	
• Flaw Remediation	SI-2	(2)
• Malicious Code Protection	SI-3	(1), (2)
• Information System Monitoring	SI-4	(2), (4), (5)
• Security Alerts, Advisories and Directives	SI-5	
• Software, Firmware, and Information Integrity	SI-7	(1), (7)
• Spam Protection	SI-8	(1), (2)
• Information Input Validation	SI-10	
• Error Handling	SI-11	
• Information Handling and Retention	SI-12	
• Memory Protection	SI-16	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

Security Appendix S3 - Plan of Actions and Milestones Template

Identified Deficiency	Residual Risk	Detailed Remediation Plan with Timeline	Expected Completion Date

Security Appendix 4 – Authority to Operate / Authority to Connect Packet

STATE OF ILLINOIS NIST and FISMA Compliance Document

Project Name:
Date:
Duration of Project:
Vendor Name:
Vendor Contact Information:

A. The departments and agencies within all branches of the Federal Government are required by Federal Information Security Modernization Act (FISMA) of 2014 to comply with OMB E-GOV guidance to provide information security for the information and information systems that support the operations and assets under their control. The Federal Office of Management and Budget (OMB) has published guidance for the executive branch in OMB Circulars A-123, Appendix D and A-130.

B. STATE OF ILLINOIS recognizes that FISMA compliance, effective information security management, and continuous monitoring of information systems are paramount to the success of information technology (IT) systems. In order to establish an information security program in accordance with FISMA, Vendor must follow the National Institute for Standards and Technology (NIST) Guidelines of the NIST Risk Management Framework (RMF), as amended.

C. ***Requirements***

(1) Each requirement in the table below is understood to contain the implied prefix, " Vendor shall..."

Area	Requirement ID	Description
NIST and FISMA Compliance	1	Describe in detail how Vendor will meet all NIST and FISMA requirements before the solution or projects approved for production.
VENDOR RESPONSE:		
NIST and FISMA Compliance	2	Describe in detail how Vendor will define information system boundaries for authorization.
VENDOR RESPONSE:		
NIST and FISMA Compliance	3	Describe in detail how Vendor will assess, review, and evaluate the information systems to be implemented based upon security categorization in accordance with Federal Information Processing Standards (FIPS) Publication 199 Standards for Security Categorization of Federal Information and Information Systems. Additional guidance on defining the information type can be obtained from National Institute Technological Standards (NIST) SP 800-60.

VENDOR RESPONSE:		
NIST and FISMA Compliance	4	Describe in detail how Vendor will select the baseline controls described in FIPS 200 and NIST SP 800-53 to develop a System Security Plan (SSP).
VENDOR RESPONSE:		
NIST and FISMA Compliance	5	Describe in detail how Vendor will meet security requirements with regard to protecting the confidentiality, integrity, and availability of the system and the information processed, stored, and transmitted by the system.
VENDOR RESPONSE:		
NIST and FISMA Compliance	6	Describe in detail how Vendor will perform continuous monitoring of the system in compliance with NIST SP 800-137.
VENDOR RESPONSE:		

(2) Vendor shall provide the following System Security Plan (SSP):

The Vendor must develop a SSP using the guidance from NIST Risk Management Framework (RMF) (NIST SP 800-18) to establish an information security program in accordance with the Federal Information Security Management Act (FISMA) and demonstrate compliance.
This SSP must be approved by an authorizing official within the STATE OF ILLINOIS. The SSP must include, but shall not be limited to, the following:

i. Description of how the system is to be compliant with all the United States Federal and State of Illinois laws regarding the security and privacy of medical data and records and of all protected health information (PHI), including:

a) The Code of Federal Regulations (at 45 CFR 95.621), which provides that State of Illinois agencies are responsible for the security of all automated data processing systems involved in the administration of Department of Health and Human Services' programs, and which includes the establishment of a security plan that outlines how software and data security will be maintained. This section further requires that State of Illinois agencies conduct a review and evaluation of physical and data security operating procedures and personnel practices on a biennial basis.
b) The security and privacy standards contained in Pub. L. 104–191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and adopted in 45 CFR Part 164, Subparts C and E, as follows: The security standards require that measures be taken to secure protected heath information that is transmitted or stored in electronic format. The

privacy standards apply to protected health information that may be in electronic, oral, and paper form.

c) The requirements in section 1902(a)(7) of the Social Security Act (the Act), as further interpreted in Federal regulations at 42 CFR 431.300 to 307.

ii. Description of measures to secure data and software;

iii. Description of how data is encrypted in transit and in storage;

iv. Description of physical and equipment security measures;

v. Description of personnel security;

vi. Description of software used for security;

vii. Description of the user roles and the access capabilities of each role;

viii. Description of how users are assigned certain roles;

ix. Identification of the staff responsible for controlling the system security;

x. Description of contingency security procedures during a disaster recovery event;

xi. Description of how Vendor works with Office of the Statewide Chief Information Security Officer to conduct annual security review;

xii. Description of how Vendor will ensure password security

xiii. Audit trails for all data access;

xiv. Acknowledgement that Vendor will be responsible for all costs associated with Identify theft, resulting from security breach.

D. **Security Risk Assessment**. STATE OF ILLINOIS or an independent entity will perform a security control assessment. STATE OF ILLINOIS will provide Vendor a copy of the approved security control assessment. Once Vendor receives the approved assessment, Vendor must then develop a Security Risk Assessment based on the applicable security controls. Guidance on conducting and documenting the Security Risk Assessment can be obtained in NIST SP 800-30.

E. **Plan of Action and Milestones (POA&M).** After STATE OF ILLINOIS reviews and approves the Security Risk Assessment, Vendor should begin to develop a POA&M. The POA&M should be a living document that is based on the findings and recommendations of the security assessment report. The POA&M should describe the deficiencies in the security controls, address the residual risk, and detail plans for remediation and identify timeline for such remediation.

F. **Authorization Approval Package**.

(a) After STATE OF ILLINOIS reviews and approves the POA&M, Vendor must prepare a transmittal letter to request approval of the entire authorization package. The authorization package must include at a minimum the following documents:

i. Transmittal Letter

ii. Updated System Security Plan

iii. Security Assessment Plan (include the STATE OF ILLINOIS/independent security assessment)

iv. Security Assessment Report (include the STATE OF ILLINOIS/independent security assessment)

v. Security Risk Assessment

vi. Plan of Action and Milestones

vii. Supporting Documentation including but not limited to design documentation, “As Built” documentation, operational documentation, validation documentation, prior authorization documentation, and other artifacts associated with the implementation and monitoring of the security controls.

(b) The authorizing official will determine the risk to the organizational operation and determine if the system is authorized to proceed. The authorizing official will deliver to Vendor a letter of authorization specifying any limitations or restriction placed on the operation of the system. Additionally, this letter should establish an end date for the security authorization.

(c) If the authorizing official denies the authorization, STATE OF ILLINOIS will continue to work with Vendor until an acceptable level of residual risk for the system is achieved. This work should include the continued remediation listed in the POA&M.

G Life-Cycle Management

Vendor shall perform security system reviews and reauthorization of the system at the direction of STATE OF ILLINOIS. Vendor shall be responsible for meeting the following requirements:

(a) Performing continuous monitoring of the security system. Vendor’s continuous monitoring must include periodically selecting a subset of the baseline controls for assessment. Based on assessment of these controls, subsequent remediation actions must be identified and implemented. The ongoing remediation process should include updating key documents such as the SSP, SAR, and POA&M.

(b) Prior to any system or environmental modifications, Vendor must perform a security impact analysis. This must be included as a part of any change management or configuration management process. If the results of the modification indicate changes to the security posture of the system, corrective actions should be initiated and appropriate documents revised and updated. The updating of the documentation and continuous monitoring should provide near real-time risk management.

(c) A monthly Security Status Report must be produced by Vendor for STATE OF ILLINOIS. The Security Status Report should provide essential information regarding the security posture of the system as well as the effectiveness of the controls deployed. Ongoing monitoring activities should be detailed as well as ongoing remediation efforts to address known vulnerabilities. Additional guidance for the monitoring of system security can be obtained in NIST SP 800-137.

Security Appendix S5 – Vulnerability Assessment

- Vendor must obtain approval on behalf of the State of Illinois to perform vulnerability assessments on the cloud-hosting vendor's website(s).

- Vendor must execute the State of Illinois Vulnerability Scanning Agreement prior to the vulnerability assessment.
  (See DoIT Scanning Agreement)

- State of Illinois may, with reasonable notice to Vendor, conduct a security assessment of Vendor's solution, which may include the following:

    - Prior to initial "official" production role out of the application,
        - Whitelisted scanning and manual testing of the application only, with application credentials equal to the least privileged role within the application
        - Manual verification of scan results with the same credentials
        - Manual testing of the application for vulnerabilities
        - State of Illinois will not conduct any Denial of Service (DOS) attacks
        - State of Illinois will not scan or test any infrastructure devices (servers, switches, routers, intrusion protection system, firewalls, etc.)

    - On a quarterly basis for the for the first year after initial production deployment,
        - Whitelisted scanning and manual testing of the application only, with application credentials equal to the least privileged role within the application
        - Manual verification of scan results with the same credentials
        - Manual testing of the application for vulnerabilities
        - State of Illinois will not conduct any DOS attacks
        - State of Illinois will not scan or test any infrastructure devices (servers, switches, routers, intrusion protection system, firewalls, etc.)

    - Prior to any enhancements or upgrades being deployed to production after the initial "official" production role out of the application,
        - Whitelisted scanning and manual testing of the application only, with application credentials equal to the least privileged role within the application
        - Manual verification of scan results with the same credentials
        - Manual testing of the application for vulnerabilities
        - State of Illinois will not conduct any DOS attacks
        - State of Illinois will not scan or test any infrastructure devices (servers, switches, routers, intrusion protection system, firewalls, etc.)

    - Monthly vulnerability scan – no whitelisting, non-credentialed scan (same day every month)

DoIT Scanning Agreement

Agreement

This agreement is between Department of Innovation & Technology \ Offensive Security Unit (hereinafter referred to as the "risk assessor") and Penetration Testing Services client (hereinafter referred to as the "client") for the supply of Penetration Testing services by the risk assessor for the client.

Whereas the risk assessor provides certain computer and systems security consulting and testing services including Penetration Testing services; and

Whereas the client wishes to retain the risk assessor to provide computer and systems security services, specifically Penetration Testing services; therefore

The client does hereby retain the risk assessor for the purpose of providing Penetration Testing services on the client's computers and/or systems.

The risk assessor will notify the client's project leader of the approximate times that the penetration tests will take place.

The objective of the Penetration Testing service is to identify and report on security vulnerabilities to allow the client the opportunity to address the identified issues in a planned manner, thus providing them the opportunity to significantly raise the level of their security protection. The client understands that Internet security is a continually growing and changing field and that testing by Department of Innovation & Technology \ Offensive Security Unit does not mean that the client's site is secure from every form of attack. There is no such thing as 100% security testing, and for example it is never possible to test for vulnerabilities in software or systems that are not known at the time of testing or the mathematically complete set of all possible inputs/outputs for each software component in use. Further security breaches can and frequently do come from internal sources whose access is not a function of system configuration and/or external access security issues.

The client has provided the risk assessor with certain required information regarding the scope and range of the tests and the client hereby warrants that all information provided is true and accurate and that the client owns or is authorized to represent the owners of the computers and systems described. The client further warrants and represents that he/she is authorized to enter into binding legal agreements. The services provided by the risk assessor are provided in reliance on the above warrants.

The risk assessor shall be under no liability whatsoever to the client for any indirect loss and/or expense (including loss of profit) suffered by the client arising out of any actual or possible breach, by the risk assessor, of this agreement. In the event of any breach of this agreement by the risk assessor the remedies of the client shall be limited to a maximum of the fees paid by the client, for this engagement.

Both parties shall maintain this agreement as confidential. Unless required by law, no information about this agreement (including the agreement terms and fees) shall be released by either party. Information about the client's business, computer systems or security situation that the risk assessor obtains during the course of the work will not be released to any third party without prior written approval unless required by law.

The risk assessor and the client have imparted and may from time to time impart to each other certain confidential information relating to each other's business including specific documentation. Each party agrees that it shall use such confidential information solely for the purposes of the service and that it shall not disclose directly or indirectly to any third party such information. Where disclosure to a third party is required, prior notice of such disclosure will be made. The third party to which such discloser will be made, will be required to agree to a duly binding agreement to maintain in confidence the information to be disclosed to the same extent at least as the parties are bound. To the extent that disclosure is requested by the Auditor General or otherwise authorized auditor, no additional agreement will be required.

Upon completion of the Penetration Testing service, the reports (deliverables) will be encrypted and delivered to the client while all other data related to the service will be securely stored, destroyed, or returned to the client (at client's option).

This agreement is subject to the laws of the State of Illinois, USA. All disputes arising out of this agreement shall be subject to the exclusive jurisdiction of the State of Illinois, USA.

Neither party shall be liable for any default due to any act of God, war, strike, lockout, industrial action, fire, flood, drought, storm or other event beyond the reasonable control of either party.

Signature ________________________________ Date __________________

Authorized Client

Signature ________________________________ Date __________________

Authorized Risk Assessor