Pennsylvania Treasury Department Information Security Addendum

This Pennsylvania Treasury Department Information Security Addendum, incorporated within the Terms and Conditions set forth in this Part IV. The terms and provisions contained herein will be deemed accepted and will become a part of the contract(s) or purchase order(s) unless the Proposal identifies an objection.

This Information Security Addendum ("Addendum") made as of the Effective Date, by and between the Commonwealth of Pennsylvania, Pennsylvania Treasury Department ("Treasury") and _____ ("Contractor") sets forth additional terms and conditions with respect to information security applicable to _____ (the "Agreement). The terms and conditions agreed to in this Addendum are the minimum required for the Agreement and shall take precedence over any term of the Agreement which attempts to reduce, waive or remove these terms and conditions.

BACKGROUND: Treasury wishes to disclose certain information to Contractor pursuant to the terms of the Agreement, and Contractor is authorized to collect and/or use certain information, pursuant to the terms of the Agreement. The parties have entered into this Addendum to protect the privacy and provide for the security and confidentiality of such information.

NOW THEREFORE, in consideration of the foregoing, and the mutual promises and undertakings hereinafter set forth, and the exchange of information pursuant to the Agreement and this Addendum, the parties agree as follows:

I. Definitions

A. *Authorized Persons*. Authorized Persons include Contractor's employees and subcontractors who have appropriate clearance and a specific need for such access in order to perform Contractor's services for Treasury.

B. *Industry Standards*. Industry Standards include National Institute of Standards and Technology (NIST) 800 Series, NIST Cybersecurity Framework and ISO 27001/2, or their generally recognized equivalents.

C. *Treasury Data*. Treasury Data is any data or information that Contractor creates for Treasury; obtains, accesses, receives from Treasury or on behalf of Treasury; or hosts for or on behalf of Treasury. Treasury Data includes but is not limited to: computer code; Treasury or Commonwealth bank account information; investment account information; identifiers unique to Treasury; and Personally Identifiable Information.

D. *Personally Identifiable Information or PII.* Personally Identifiable Information or PII means information or data, alone or in combination with other information, that identifies or authenticates a particular individual. PII may include, without limitation, name, date of birth, full address (e.g., house number, city, state, and/or zip code), passwords, PINs, biometric data, unique identification numbers (e.g., social security numbers, tax ID numbers, driver license numbers, credit or debit account numbers, medical record numbers), federal or state tax information, TAP/ABLE account numbers, bank account numbers, ACH information, answers to security questions or other personal identifiers, or which meets the definition

ascribed to the term "Personal Information" under §6809(4) of the Gramm-Leach-Bliley Act.

E. *Public Data*. Public Data means any specific information or data, regardless of form or format, that Treasury has actively and intentionally disclosed, disseminated, or made available to the public. No Contractor shall make a determination on Treasury's behalf whether data is public or would be considered public under state or federal law including the Pennsylvania Right-to-Know Law.

F. *Multi-Factor Authentication*. Multi-Factor Authentication is the use of two or more of the Authentication Methods listed below. Two-factor would employ two of the methods; three-factor would employ one each of all three methods.

i. Something you know (e.g., PIN, password, shared information)

ii. Something you possess (e.g., token, smart card, digital certificate)

iii. Something you are (biometrics – e.g., fingerprint, voice, iris, face).

G. *Services*. Services are the services pursuant to the Agreement and/or any Statement of Work ("SOW") or any subsequent document that may detail services.

H. *Documentation*. Documentation means all technical and user documentation provided by Contractor and any succeeding changes thereto, including, without limitation, all specifications; installation, maintenance, operating and customer manuals, instructions and diagnostics; system administrative materials; configuration guides; product guides; and other documentation provided by Contractor related to the Services.

I. *Treasury Confidential Information*. Treasury Confidential Information means Treasury Data that is not Public Data, including but not limited to information containing Personally Identifiable Information, protected health information ("PHI") and electronic protected health information ("ePHI") as defined in HIPPA regulations, investment portfolio information and trade secrets.

II. Assignment.

Contractor may not assign, in whole or in part, this Agreement or Addendum or its rights, duties, obligations, or responsibilities hereunder without the prior written consent of the Treasury. Such consent may be withheld at the sole and absolute discretion of the Treasury.

III. Software/Platform/Website.

a. Software. If Contractor at any time during the term of the Agreement, or during the term of any applicable license or subscription for any software under the Agreement, becomes aware of any Disabling Device in or affecting any product(s) or other items acquired by Treasury from Contractor, or a security flaw in any such software, or a flaw in such software that has the potential to cause or result in a

security breach, then the Contractor shall notify Treasury within 72 hours thereafter. Any Contractor notice to Treasury shall include notifying Treasury if it has a fix for the issue, if it is working on a fix, or if it does not have a fix. Contractor shall use reasonable commercial efforts to cure or correct any such security flaw as soon as practicable. Nothing herein will limit Contractor's indemnification obligations under the Agreement or this Addendum.

b. Platform and Website. Contractor further represents and warrants that it will take appropriate and reasonable precautions, using commercial grade anti-virus and malware recognition programs, to screen any software provided to Treasury, and the platform and any websites owned or operated by Contractor to conduct, market or promote its activities under this Agreement, for viruses and other malware, and to cause the Contractor's services, any such platform and websites to be made available to Treasury and any other Commonwealth agency free of any Disabling Devices (as defined below) or other malware. For purposes of this Addendum, "Disabling Device" means any malware or other computer code (i) that is designed to disrupt, disable, harm, or otherwise impede in any manner the operation of any software program or code, or any computer system or network (commonly referred to as "malware", " spyware", "viruses" or "worms"); (ii) that would disable or impair the operation thereof or of any software, computer system or network in any way based on the elapsing of a period of time or the advancement to a particular date or other numeral (referred to as "time bombs", " time locks", or "drop dead" devices); (iii) that is designed to or could reasonably be used to permit Contractor or any third party to access any computer system or network (referred to as "trojans", "traps", "access codes" or "trap door" devices); or (iv) that is designed to or could reasonably be used to permit Contractor or any third party to track, monitor or otherwise report the operation and use of any software program or any computer system or network by Treasury, its contractors or third parties, in a manner other than in accordance with the specifications and Documentation therefor provided by Contractor or required under applicable law or regulatory rules or requirements. Notwithstanding the foregoing, any code included or used by Contractor as part of the Contractor's services for the sole purpose of allowing Contractor to perform its obligations under this Agreement, or for operational and quality control purposes in connection with such performance, will not be considered a Disabling Device.

c. Data Security.

i. Industry Standards. The Contractor shall ensure that Services procured under this Agreement comply with the applicable Industry Standards. In the event such standards change during Contractor's performance, and the Commonwealth requests that Contractor comply with the changed standard, then any incremental costs incurred by Contractor to comply with such changes shall be paid for pursuant to a change order to the Agreement.

ii. Data Protection. To the extent that Contractor is charged with creating, accessing, transmitting, maintaining, hosting or using Treasury Data under the Agreement, Contractor shall preserve the confidentiality, integrity and availability of Treasury Data by implementing and maintaining administrative, technical and physical controls that conform to Industry

Standards. Implemented security controls shall provide a level of security which is commensurate with the sensitivity of the data to be protected.

iii. Data Use and Access. Contractor shall use Treasury Data only and exclusively to support the performance of Services for Treasury under the Agreement and not for any other purpose. With the exception of Public Data, absent Treasury's prior written consent, Contractor shall not at any time during or after the term of the Agreement disclose Treasury Data to any person, other than Authorized Persons and Treasury personnel in connection with the performance of the Services (except as required by law). If such disclosure is required by law, Contractor shall limit such disclosure to information required to be disclosed and shall notify Treasury as soon as practicable and prior to such disclosure, unless such notification is prohibited by law.

iv. Data Backup. Where appropriate to protect the integrity and availability of Treasury Data, Contractor shall maintain (and cause any third-party hosting company that it uses to maintain) a means to backup and recover Treasury Data in the event that Treasury Data is lost, corrupted or improperly destroyed. Treasury shall have the right to establish its own backup security for Treasury Data and to keep such backup Treasury Data and Treasury Data files in its possession if it chooses. Contractor shall cooperate with Treasury in facilitating the establishment and maintenance of such alternative backup security. At no time may Contractor store Treasury Data outside of the United States.

v. Return of Treasury Data. Contractor shall ensure that, upon request, Treasury can access and retrieve Treasury Data in the event the Contractor is unable to continue providing the Services under the Agreement due to termination of the Agreement or otherwise. In the event of a termination for any reason and upon Treasury's request, the Contractor will provide Treasury Data in a standard format or other mutually acceptable format. Treasury will reimburse Contractor for any costs incurred by Contractor to provide Treasury Data in a non-standard format.

vi. Destruction of Treasury Data. Upon written request of Treasury, Contractor shall irrevocably erase or destroy in such a manner to render unrecoverable all Treasury Data in Contractor's possession that is no longer required for the performance of its duties under the Agreement. Upon Treasury's request, Contractor shall certify in writing that these actions have been completed within seven (7) days of Treasury's request.

vii. Effect of Termination. Unless directed otherwise by Treasury, upon termination of the Agreement for any reason, Contractor shall maintain Treasury Data and continue to extend the protections of the Agreement and this Addendum to such information for a period of six months at which point it shall return (or at Treasury's request destroy) all Treasury Data received from Treasury (or created or received by Contractor on behalf of Treasury) regardless of form, and shall retain no copies of Treasury Data except as required by law. If return or destruction of all Treasury Data is not feasible, or any Treasury Data is required to be retained by Contractor under applicable law, Contractor shall continue to extend the protections of the Agreement and this Addendum to such information and limit further use of

Treasury Data to those purposes that make the return or destruction of Treasury Data infeasible.

d. Contractor Security.

i. Information Security Program. For the term of the Agreement, Contractor agrees that it has and will maintain a formal information security program which is appropriate for the types of services that it provides. Treasury has adopted the Minimum Security Requirements set forth below (Parts (IV) through (XIII)) in order to outline the security requirements which apply to all third parties, service providers, processors, and contractors (including Contractor) (collectively, "Third Parties") that process Treasury Confidential Information or who have access to Treasury systems. Treasury has identified ISO 27001 Control Requirements; however, Third Parties may identify and rely upon other controls which meet the essence of the requirements.

ii. Contractor Personnel. Contractor agrees that it shall only use highly qualified and appropriately skilled and experienced personnel and contractors in performing the Agreement and, to the extent not prohibited by applicable law, shall require each to pass a background check.

iii. Acceptance of Acceptable Use Policy. Contractor shall ensure that all Contractor personnel, including employees and contractors, who access Treasury's network as a part of performing the Agreement, will agree to Treasury's Acceptable Use Policy as found in Management Directive 205.34, as it may be amended from time to time.

iv. Multi-Factor Authentication. For services exposed to the Internet, where sensitive information is stored, processed or transmitted, Contractor will provide Multi-Factor Authentication for user authentication to the web application via workstation and mobile browsers. If the service is provided via mobile application as well, that application must also be protected by Multi-Factor Authentication.

v. Security Awareness Training. Contractor shall ensure its personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with Commonwealth of Pennsylvania IT Policies. A comprehensive compilation of these policies can be found at https://www.oa.pa.gov/Policies/Pages/itp.aspx or by visiting the Pennsylvania Office of Administration's website and toggling to IT Policies under the "Policies."

e. Security Incident and Breach Notification.

i. Contractor agrees to notify Treasury upon learning of: (i) unauthorized access, loss, alteration, theft or corruption of Treasury's Confidential Information; (ii) any event that creates a substantial risk to the confidentiality, integrity or availability of Treasury Data; (iii) a breach of any of Contractor's security obligations under this Addendum; or (iv) any other event requiring notification under applicable law. In such an instance, Contractor agrees to:

a) Take such action as may be necessary to preserve forensic evidence and eliminate the cause of the risk or breach within Contractor's reasonable control. As soon as practicable after discovery, Contractor shall undertake a thorough forensic investigation of any compromise or improper use and provide Treasury all information necessary to enable Treasury to fully understand the nature and extent of the compromise or improper use to the extent known;
b) Notify Treasury by telephone at (717) 787-8726 and (717) 705-6428 and by e-mail at ITSecurity@patreasury.gov regarding such an event without undue delay and in any event within 24 hours of discovery; and
c) To the extent that the breach or incident was caused by Contractor's failure to comply with the requirements of the Agreement or this Addendum, or otherwise was caused by the fault of Contractor, assume the cost of informing all such affected individuals in accordance with applicable law, in addition to its other indemnification obligations under this Addendum.

ii. Security Incident Investigations.

Contractor agrees to cooperate with Treasury in investigating a security incident, as notified by Contractor under this Addendum or declared by Treasury, and provide the name and contact information, of at least two (2) security contacts who will respond to Treasury in a timely manner, dependent on criticality, in the event that Treasury must investigate a security incident. The current security contacts are as follows:
Contact Names: _____ _____
Phone Numbers: _____ _____
Email Addresses: _____ _____

f. Maintenance of Safeguards.

i. Contractor shall maintain and follow Industry Standards with respect to any of Treasury's Confidential Information in Contractor's possession or control and protect such information against any loss, alteration, theft or corruption.

ii. At Treasury's request, Contractor shall provide Treasury with copies of its information security policies, processes, and procedures made available by Contractor to third parties or otherwise requested by Treasury, subject to Contractor's reasonable requirements and restrictions to protect the security and confidentiality of such information. Contractor will notify Treasury of any changes to its policies, processes or procedures that relate to the security of Treasury's Confidential Information in Contractor's possession.

g. Information Security Audit.

i. Treasury shall have the right to review Contractor's information security program prior to the commencement of Services and from time to time during the Term of the Agreement. During the performance of the Services, on an ongoing basis annually and immediately in the event of a security incident, Treasury, including its professional advisors and auditors, at its own

expense, shall be entitled to perform, or to have performed, an on-site assessment of Contractor's information security program.

ii. Treasury shall have the right to review Contractor's information security program through Contractor's annual submission to Treasury of its current SOC2 report. The report must document an assessment conducted by a qualified, independent third party. Assessment scope must address the services provided to Treasury, including but not limited to related people, processes and technology.

iii. Upon Treasury's request, Contractor agrees to complete, within forty-five (45 days) of receipt of Treasury's request, an assessment questionnaire provided by Treasury regarding Contractor's information security program, including artifacts for a subset of controls.

h. Application Security.

In the event the Contractor conducts application software development for Treasury, Contractor will either make source code available for review by Treasury or will conduct source code scanning using a commercial security tool. Scans must be conducted annually and at any time significant code changes are made. Scan reports will be made available to Treasury within two weeks of execution. Contractor must disclose remediation timelines for high, medium and low risk security code defects. Scans must occur before code is implemented in production. High risk security code defects may not be implemented in production without written approval from Treasury's Chief Information Officer. Contractor shall not deliver any code that provides for back door access or otherwise would constitute a Disabling Device under this Addendum, except as specified and approved by Treasury. Contractor shall comply with the software development security requirements identified under Part (VII) below and inform Treasury of any code development internal requirements, procedures and/or policies that Contractor uses to establish and verify the quality and security of Contractor's code development services.

i. Compliance with Applicable State and Federal Law.

Contractor shall comply with all applicable federal, state, and local laws concerning data protection and privacy when performing the Services and storing, handling or transmitting Treasury Data.

j. Enforcing Compliance.

Contractor shall enforce and be responsible for compliance by all its personnel and contractors with the provisions of this Information Security Addendum and all other confidentiality obligations owed to Treasury.

k. Accommodation of Additional Protections.

Contractor agrees to comply with such additional protections as Treasury shall reasonably request.

l. Termination.

A breach by Contractor of any provision of this Addendum, as reasonably determined by Treasury, shall constitute a material breach of the Agreement and

shall provide grounds for immediate termination of the Agreement by Treasury pursuant to the Agreement.

m. Indemnification.

Contractor shall indemnify, hold harmless and defend Treasury from and against all claims, losses, liabilities, damages, judgments, costs and other expenses, including Treasury's costs and attorney fees, incurred as a result of, or arising directly or indirectly out of or in connection with (i) Contractor's failure to meet any of its obligations under this Addendum; (ii) any security breach or incident that was caused by Contractor's failure to comply with the requirements of the Agreement or this Addendum, or otherwise was caused by the fault of Contractor; and (iii) any claims, demands, awards, judgments, actions and proceedings made by any person or organization arising out of or in any way connected with Contractor's performance under this Addendum. Limitations on Contractor's liability, regardless of conflicting language elsewhere in the Agreement, shall not apply to claims related to Contractor's breach of the requirements of this Addendum.

n. Intellectual Property Infringement Indemnification.

Contractor shall indemnify, defend and hold Treasury harmless from any and all claims brought against Treasury alleging that the Services and/or Documentation or Treasury's use of the Services and/or Documentation, or use of any deliverables provided by Contractor, constitutes a misappropriation or infringement of intellectual property ("IP") of any Third Party. Contractor agrees to be responsible for all costs or expenses, to include reasonable attorneys' fees awarded or resulting from any claim. Treasury shall, after receiving notice of a claim, advise Contractor of such notification. Limitations on Contractor's liability, regardless of conflicting language elsewhere in any Agreement, shall not apply to claims related to Contractor's misappropriation or infringement of another's intellectual property.

o. Contractor Liability Insurance.

Treasury may require Contractor to procure, and maintain for the duration of the Agreement and a specified period thereafter, insurance against claims and damages which may arise from or in connection with the performance of its work to include IP infringement, professional liability, cybersecurity, and privacy or data breach coverage, with coverage amounts reasonably acceptable to Treasury.

p. Survival; Order of Precedence.

The provisions of this Addendum shall survive expiration or termination of the Agreement.

q. Entire Agreement.

The Agreement, including any exhibits and/or schedules thereto, and this Addendum contain the entire understanding of the parties with respect to the subject matter hereof and supersedes all prior agreements, oral or written, and all other communications between the parties relating to such subject matter.

IV. Minimum Security Requirements

The below requirements apply to all Third Parties (including Contractor) that process Treasury Confidential Information or PII on behalf of Treasury, or if they have a

direct connection to the Treasury network. While ISO 27001 controls are listed, equivalent controls from other frameworks may be used in accordance with those frameworks, if they meet the essence of the requirement.

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
5.1.1	Policies for information security	A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.
5.1.2	Review of the policies for information security	The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
6.1.1	Information security roles and responsibilities	All information security responsibilities should be defined and allocated.
7.2.2	Information Security Awareness, Education and Training	All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
8.1.1	Inventory of Assets	Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.
8.1.4	Return of Assets	All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement.
9.1.2	Access to Networks and Network Services	Users should only be provided with access to the network and network services that they have been specifically authorized to use.
9.2.1	User Registration and De-Registration	A formal user registration and de-registration process should be implemented to enable assignment of access rights.
9.2.2	User Access Provisioning	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.
9.2.3	Management of Privileged Access Rights	The allocation and use of privileged access rights should be restricted and controlled.
9.2.6	Removal or Adjustment of Access Rights	The access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.
9.4.1	Information Access Restriction	Access to information and application system functions should be restricted in accordance with the access control policy.

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
9.4.2	Secure Log-On Procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.
9.4.3	Password Management System	Password management systems should be interactive and should ensure quality passwords.
10.1.1	Policy on the Use of Cryptographic Controls	A policy on the use of cryptographic controls for protection of information should be developed and implemented.
11.1.1	Physical Security Perimeter	Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
11.1.2	Physical Entry Controls	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
11.1.3	Securing Offices, Rooms and Facilities	Physical security for offices, rooms and facilities should be designed and applied.
11.1.4	Protecting Against External and Environmental Threats	Physical protection against natural disasters, malicious attack or accidents should be designed and applied.
12.1.4	Separation of Development, Testing and Operational Environments	Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.
12.2.1	Controls Against Malware	Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.
12.4.1	Event Logging	Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.
12.4.3	Administrator and Operator Logs	System administrator and system operator activities should be logged, and the logs protected and regularly reviewed.
12.6.1	Management of Technical Vulnerabilities	Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
13.1.1	Network Controls	Networks should be managed and controlled to protect information in systems and applications.
13.1.3	Segregation in Networks	Information involved in electronic messaging should be appropriately protected.
14.1.3	Protecting Application Services Transactions	Information involved in application service transactions should be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
14.3.1	Protection of Test Data	Test data should be selected carefully, protected and controlled.
15.1.1	Information Security Policy for Supplier Relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.
15.2.1	Monitoring and Review of Supplier Services	Organizations should regularly monitor, review and audit supplier service delivery.
15.2.2	Managing Changes to Supplier Services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and reassessment of risks.
16.1.5	Response to Information Security Incidents	Information security incidents should be responded to in accordance with the documented procedures.
18.2.1	Independent Review of Information Security	The organization's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur.
Network and system vulnerability assessments shall be conducted on an annual basis, at a minimum. Critical vulnerabilities shall be tracked and remediated within 30 days of identification.		
Additional Requirements		
Local accounts shall be disabled if not required or used and shall not be used for privileged access.		
Third party shall notify Treasury of any separation or transfer of Third-Party Worker with Treasury credentials no later than the day of that event.		
Accounts shall be disabled after 90 days of inactivity, at a minimum.		
Treasury Confidential Information shall not be processed or stored on personal accounts or on personally owned computers, devices or media.		
Third-Party shall notify Treasury within a reasonable period, in no event to exceed five (5) business days after discovery, or shorter if required by applicable law or regulation, of any potential Cybersecurity Vulnerability. Third-party shall report all critical Cybersecurity Vulnerability that would have a significant adverse effect on Treasury and any Cybersecurity Vulnerability to Treasury at ITSecurity@patreasury.gov		
Security Incident Notification Requirements		
Third Party shall implement and maintain a written Incident Response Plan containing policies and procedures sufficient to comply with its breach notification obligations under this Agreement and applicable data protection and privacy Laws.		
Notification and Cooperation. Third Party shall:		

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
• Provide Treasury with the name and contact information for any employee of Third Party who shall serve as the Treasury's primary security contact and shall be available to assist Treasury twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a Security Incident; • Notify Treasury and Treasury's primary business contact within Third Party of a Security Incident as soon as practicable, but no later than twenty-four (24) hours after Third Party becomes aware of the Security Incident. Immediately following Third Party's notification to Treasury of a Security Incident, the parties shall coordinate with each other to investigate the Security Incident. Third Party agrees to fully cooperate with Treasury in the investigation of any Security Incident, including without limitation, by assisting with any investigation, making available all relevant records, logs, files, data reporting and other materials helpful to the investigation, and providing reasonable access to Third Party's facilities, systems, and personnel; • Maintain and preserve all documents, records and other data related to the Security Incident; • Fully cooperate, at its own expense, with Treasury in any litigation, investigation or other action deemed reasonably necessary by Treasury to protect its rights related to the Security Incident; and • Use its best efforts to prevent a recurrence of any such Security Incident.		
Expenses of Remediation. Third Party shall, at its own expense, use best efforts to immediately contain and remedy any Security Incident and prevent any further Security Incident, including, but not limited to, taking any and all action necessary to comply with Applicable Law. Third Party shall reimburse Treasury for all actual costs incurred by Treasury in responding to and mitigating damages caused by any Security Incident, including all costs of notice to third parties and remediation pursuant to the following section, including, but not limited to, costs incurred by Treasury relating to forensic investigators, legal counsel, telephone call centers, notification vendors, and business disruption.		
Disclosure to Third Parties. Third Party agrees that it shall not inform any third party of any Security Incident without first obtaining Treasury's prior written consent, other than to inform a complainant that the matter has been forwarded to Treasury's legal counsel. Further, Third Party agrees that Treasury shall have the sole right to determine: (i) whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in Treasury's discretion; and (ii) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.		

V. Physical Security Requirements

In addition to the Minimum Security Requirements regarding Physical Security defined above (11.1.1 – 11.1.4), the below requirements apply to all Third Parties (including Contractor) that process, access, or store (physically or logically) Treasury Confidential Information or PII on behalf of Treasury, or if they have a direct connection to the Treasury network. If Treasury data is only stored or processed in a cloud environment, the identified cloud provider must be

communicated to Treasury and the associated attestation reports (SOC 2 Type 1 & 2 Report, ISO 27001/2) must be provided to Treasury.

Physical Security Control Requirements
For all facilities used to access, process, transmit, and/or store Treasury Confidential Information or Personal Information, badge readers shall be used on all entry points to ensure physical access is restricted to authorized personnel.
All servers and network equipment used to store and/or access Treasury Confidential Information or Personal Information shall be kept in a secure room with the following controls: 1. Additional access control mechanisms (e.g., badge, biometrics, pin, etc.) on entry doors, 2. Rooms are located on the interior of the building with no windows, unless safeguards are in place to prevent shattering, and 3. Telecommunications equipment, cabling and relays receiving data or supporting services are hidden from view to deter interception or damage.
For all facilities used to access, process, transmit, and/or store Treasury Confidential Information or Personal Information, security cameras shall be implemented to monitor the perimeter, entry/exit points, and the interior of the facility.
Security camera recordings shall be retained for at least 30 days.
For all facilities used to access, process, transmit, and/or store Treasury Confidential Information or Personal Information, access shall be controlled by a security guard, mantrap, or other means when entering the facility.
Identification badges shall be issued to all employees, contractors, and visitors and worn always.
Identification badges shall delineate full time employees from contractors and visitors.
All physical documents that contain Treasury Confidential Information or Personal Information shall be kept in a locked office, cabinet, or other location which is locked, and access restricted to authorized personnel only.
Mechanisms shall be in place to notify, investigate, and address potential physical security incidents such as physical intrusion or a stolen asset.
If all facilities used to access, process, transmit, and/or store Treasury Confidential Information or Personal Information are not staffed 24x7x365, alarms shall be installed for off-hour access monitoring.
If facilities used to access, process, transmit, and/or store Treasury Confidential Information or Personal Information are shared with other occupants (e.g. co-located data center), protective mechanisms must be implemented between occupants to prevent unauthorized access to your organization's physical equipment (e.g. locked cage, badge access, etc.)
Physical access rights shall be reviewed on an annual basis (at a minimum) and updated as needed to ensure physical access to all facilities used to access, process, transmit, and/or store Treasury Confidential Information or Personal Information is restricted to authorized personnel.

VI. Security Requirements When Processing Sensitive / Regulated Data

In addition to the Minimum Security Requirements defined above, the below requirements apply to all Third Parties (including Contractor) that process Treasury PII), Sensitive Personal Information (SPI), Protected Health Information (PHI), Payment Card Information (PCI), Intellectual Property (IP) or supports Treasury mission critical business functions:

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
6.1.2	Segregation of duties	Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
7.1.1	Screening	Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
7.2.1	Management responsibilities	Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
8.3.1	Management of removable media	Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
8.3.2	Disposal of media	Media should be disposed of securely when no longer required, using formal procedures.
8.3.3	Physical media transfer	Media containing information should be protected against unauthorized access, misuse or corruption during transportation.
9.2.4	Management of secret authentication information of users	The allocation of secret authentication information should be controlled through a formal management process.
9.2.5	Review of user access rights	Asset owners should review users' access rights at regular intervals.
9.4.5	Access control to program source code	Access to program source code should be restricted.
11.2.7	Secure disposal or re-use of equipment	All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
12.1.1	Documented operating procedures	Operating procedures should be documented

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
		and made available to all users who need them.
12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.
12.4.2	Protection of log information	Logging facilities and log information should be protected against tampering and unauthorized access.
12.5.1	Installation of software on operational systems	Procedures should be implemented to control the installation of software on operational systems.
12.6.2	Restrictions on software installation	Rules governing the installation of software by users should be established and implemented.
12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes.
14.2.2	System change control procedures	Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.
16.1.1	Responsibilities and procedures	Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.
16.1.2	Reporting information security events	Information security events should be reported through appropriate management channels as quickly as possible.
16.1.4	Assessment of and decision on information security events	Information security events should be assessed, and it should be decided if they are to be classified as information security incidents.
16.1.6	Learning from information security incidents	Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable.

VII. Third Party Software Development

In addition to the Minimum Security Requirements defined above, the below requirements apply to all Third Parties (including Contractor) that develop software specific to Treasury's needs or host applications that Process Treasury Confidential Information or PII with no Trusted Third-Party Network connectivity to Treasury:

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
14.2.1	Secure development policy	Rules for the development of software and systems should be established and applied to developments within the organization.
14.2.6	Secure development environment	Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
14.2.7	Outsourced development	The organization should supervise and monitor the activity of outsourced system development.
14.2.8	System security testing	Testing of security functionality should be carried out during development.
14.2.9	System acceptance testing	Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.
Additional Requirements		
Third Party may not use offshore developers or outsourced developers without the written approval of the Treasury Chief Information Security Officer.		
Third Party shall provide all developers application security training.		
All confirmed critical/high vulnerabilities (mediums and low depending on impact) found during testing shall be remediated and retested within 30 days of identification and prior to moving code to production. A formal report including the scope and results of security testing (including any issues/exceptions) shall be provided to Treasury upon request.		

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
Any software developed for Treasury shall not contain any software (proprietary or open source) developed or sold by an entity other than Third Party unless approved by Treasury.		
All software delivered to Treasury shall be free of defects/vulnerabilities identified as "critical" or "high" risk. If software shall be delivered with critical or high-risk vulnerabilities, approval from the Treasury business application owner shall be obtained.		
Information security checkpoints shall be incorporated into the software development lifecycle including, but not limited to: • Risk assessment process • Documented security requirements • Secure coding guidelines and checklists • Secure design/architecture review • Source code review • Security testing		
If the Third-Party hosted application undergoes significant changes or enhancements, Treasury has the option to perform a technical penetration test (manual and/or automated) prior to the changes being implemented in production. In cases deemed acceptable by Treasury, a Third Party's penetration test results shall be leveraged if the report meets Treasury's quality standards and was conducted within the last 12 months.		
All Third-Party hosted applications shall be reassessed every two years. Reassessment includes but is not limited to a technical penetration test (manual and/or automated).		
Third Party Software Developer with Trusted Network Connectivity to Treasury		
Third Party shall have a designated application security representative that acts as the primary liaison between Third Party and Treasury in matters related to secure application development, ensuring that Third Party development teams meet all Treasury requirements for secure application development, and provides to Treasury, upon request, evidence of compliance with requirements listed in this section.		
Prior to the initiation of any project, Third Party shall request the application's risk classification (Critical vs. non-Critical) and network exposure designation (External or Internal facing) from the Treasury application owner. These risk factors shall be determined prior to the initiation of code development.		
Documented security requirements shall be formally defined for all new development of applications including projects involving significant changes to existing applications with the Treasury designation of "Critical" and/or "External facing". These requirements shall be developed in collaboration with the Treasury application owner and other key stakeholders as necessary. All secure design requirements shall be documented and maintained with the broader set of application requirements.		
Software development teams shall use Treasury-provided version control processes and tools.		
Application development shall take place in a secured development environment. The development environment shall incorporate the following controls: Access Control, Offsite backup, Logical separation between different development environments (e.g. development, staging, testing, etc.), change control for associated systems supporting development environments, approval process for code changes of the application prior to production		

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
release, specific permissions and logging of approvals associated with movement of code and test data into and out of the environment.		

VIII. Cloud Security

In addition to the Minimum Security Requirements defined above, the below requirements apply to all Third Parties (including Contractor) that host a cloud computing application (in a SaaS, PaaS, IaaS, or DRaaS environment) that Processes Treasury Confidential Information or PII), or the Third Party provides a cloud computing platform that allows Treasury to develop, run, and manage applications, or the Third Party is responsible for the management of virtual machine image and/or hypervisor on behalf of Treasury:

Cloud Security Requirements
Root/administrator access to the management console shall require multi-factor authentication.
Dedicated secure networks shall be separate from customer production infrastructure, leveraged to provide management access to the cloud infrastructure.
Third Party shall have the ability to provide logs which are specific to the instances used for Treasury or the Treasury engagement.
Third Party shall enable console and resource level logging across regions in the cloud infrastructure.
All logs in the cloud environment shall feed into a central log aggregation tool.
Third Party shall regularly back up application configuration, data within the application, database and configuration of systems within cloud infrastructure to ensure that data can be restored if needed.
Third Party shall retain the original structure and format of data residing within the cloud application for easy movement to another cloud solution / cloud service provider.
Third Party shall support federated authentication (e.g.: SAML) or standards-based identity protocols (e.g., OpenID Connect, OAuth2, etc.) leveraged for propagating and enforcing identity controls through the SaaS and API.
Third Party shall have cryptographic controls implemented to make sure that Treasury data at rest within cloud infrastructure is always encrypted (e.g.: AES-256).
Third Party shall have mechanisms in place to control encryption key generation, distribution, storage, access and destruction.
Third Party shall have access to management consoles and cloud application(s) restricted through Role Based Access Control & based on the least privilege principle.
If keys (e.g.: access key, secret key for cloud accounts or SSH keys used for managing cloud instances) are used for managing the cloud infrastructure; the Third Party shall keep in a protected vault with access controls.
Third Party shall have a cyber incident management program in place wherein the cyber events/incidents are evaluated, contained, remediated, and responded to.
Third Party shall have a patch management process for identifying and applying all relevant vendor patches and security updates within 30 days of release by vendor.
Third Party shall have the root/administrator account credentials vaulted.

A web application vulnerability assessment or penetration test shall be performed on the cloud application(s) hosting, storing, processing and/or transmitting Treasury data, in the last 12 months.
A network vulnerability assessment shall be performed on the cloud instances and systems (servers, databases, networking components/devices) which store, process, host, or transmit Treasury data within the last 12 months.
Third Party shall have application support for both single tenancy and multi-tenancy deployment.
Third Party shall support web application firewall (WAF) implementations which comply at minimum with the OWASP top 10 risks.
Third Party shall have controls in place to ensure non-public exposure of data, including but not limited to S3 buckets and Elasticsearch.
Third Party shall have audits to monitor for configuration drift.
Third Party shall have controls to automatically shut down publicly exposed data.

IX. Software as a Service (Saas) Security

In addition to the Minimum Security Requirements and the Cloud Security Requirements defined above, the below requirements apply to all Third Parties (including Contractor) that hosts a cloud computing application that Processes Treasury Confidential Information or PII on behalf of Treasury:

SaaS Security Requirements
SaaS provider is accountable for maintaining compliance with relevant regulations and legal requirements for its services.
SaaS provider shall provide documentation to tenants regarding the following: • Roles and responsibilities matrix between cloud service provider and Treasury for each platform/service offering (e.g., incident response, infrastructure support, access management, etc.). Methods for maintaining segregation of duties within the cloud service offering shall also be included. • Scenarios in which the cloud service provider may access tenant data and metadata. • Installation, configuration, and use of products/services/features. • Known issues with products/services of the cloud offering. • Transport routes of data between systems and governing procedures for data migration to and from cloud service offering(s). • How system (e.g., network, storage, memory, I/O, etc.) oversubscription is maintained and under what circumstances/scenarios. • List of Third Parties (sub processors or joint controllers) that have access to Treasury Confidential Information or manage aspects of the application, database, server operating system, etc.
Configuration of the SaaS shall adhere to a minimum baseline of security configuration settings for role, scope and location of the services.
SaaS provider that directly provides services to Treasury is solely accountable for the platform and infrastructure security. If the provider uses other cloud or Third-Party service vendors, the provider is accountable for ensuring the security arrangement meets Treasury contractual requirements.
Integration of the SaaS with Treasury resources shall leverage Treasury pre-approved integration architecture pattern(s).

All service endpoints shall be signed by a trust authority or there must be another mechanism of establishing trust available.
SaaS provider shall ensure data portability among different cloud services by supporting standardized file format, import/export functionality, etc.
SaaS provider shall support standard based identity protocols and enforcement such as OpenID Connect (OIDC), Security Assertion Markup Language (SAML) and OAuth2 for propagating and enforcing identity controls through SaaS and Application Programing Interfaces (API).
SaaS provider shall have the capability to support tenant-generated and stored encryption keys.
Access to management consoles for entitlement and policy management shall be secure and restricted through Role Based Access Control (RBAC) and be based on the least privilege principle. Credential(s) for privileged accounts, including root or administrator accounts, shall be vaulted and multi factor authentication shall be implemented.
Upon request, SaaS provider shall inform Treasury of application user access that has been provisioned and de-provisioned for the Treasury account.
SaaS provider shall have the capability to provide secure data disposal at Treasury's request and ensure data is not recoverable by any computer forensic means.
SaaS provider shall triage threats and security related events in multi-tenant environments on a global scale and ensure timely and thorough incident management.
SaaS providers shall demonstrate compliance with information security and confidentiality, service definitions, and service level agreements. SaaS provider reports, records, and services shall undergo audit and review at planned intervals to govern and maintain compliance with the service delivery agreements.
SaaS provider shall use dedicated secure networks to provide management access to cloud service infrastructure that is separate from the customer (tenant) production infrastructure.
SaaS provider shall permit tenants to perform independent vulnerability assessments of the customer (tenant) production infrastructure.
SaaS provider shall allow tenants to opt-out of having their data/metadata accessed via inspection technologies.
SaaS provider shall have an option for customers to opt-in or opt-out of specific features in SaaS releases.
SaaS provider shall have the capability to logically segment and recover data for a specific customer in the case of a failure or data loss.
SaaS provider logging and monitoring framework shall allow isolation of an incident to specific tenants. Upon request, SaaS provider shall provide Treasury with platform management logs, application logs, API activity logs.
Upon request, SaaS provider shall have the capability to restrict the storage of Treasury Data to specific countries or geographic locations.
A web application vulnerability assessment or penetration test shall be performed on the cloud application(s) in the last 12 months.

X. Data Center Security

In addition to the Minimum Security Requirements defined above, the below requirements apply to all Third Parties (including Contractor) that provide data center facility services to Treasury:

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents should be designed and applied.
11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
11.2.1	Equipment siting and protection	Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
11.2.2	Supporting utilities	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.
11.2.4	Equipment maintenance	Equipment should be correctly maintained to ensure its continued availability and integrity.
17.2.1	Availability of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

Additional Requirements
Data center walls shall be resistant to fire or explosions.
Data centers with glass windows are not allowed unless shatter proof and impact resistant barriers are in place.
Physical data center access rights shall be reviewed at a minimum quarterly using a documented process.
All data centers shall have professionally installed intrusion alarm systems monitored by either a contracted security monitoring service or by members of the local security team within the building. All ingress points shall be alarmed and monitored. The alarm system shall be capable of continuous operation in the event of a loss of power.
Emergency doors shall have audible alarms and display appropriate signage.
Upon entrance to the data center, access shall be restricted to only the areas the person needs access to. Both ingress and egress points shall be controlled and monitored 24x7x365 to minimize tailgating and provide detailed location logging. Logs shall be retained for a

minimum one year from time of event or logging, except where prohibited or otherwise required by applicable laws and regulations. Logs relevant to pending or foreseeable litigation, investigation or audit (even when not subject to a formal document retention notice) shall be preserved as directed by Treasury. Visitors shall be escorted or observed at all times.
Closed-Circuit Television (CCTV) systems and appropriate signage shall be in place on the exterior and all datacenter floor entry points. Cameras shall be monitored during operational hours and be retained for a minimum 30 days.
Management of security alarms, entrance control, environmental controls, and CCTV systems shall be physically and logically restricted to staff responsible for these functions.
All entrances of the building containing the data center shall be designed to block entering the building interior or boarding elevators without first undergoing a manned identification check. The main entrance accessible to the public shall be manned 24/7. Multiple secured entrances shall exist between public and data center floor area.
Assets containing Treasury Confidential Information shall be caged off physically from the rest of the data center. The cage shall utilize the main security card access control system with multi factor authentication or a controlled key process. Cages shall be real floor to real ceiling to prevent unauthorized entry. Cages shall be designed to prevent intrusion or breach from outside of the cage. Finally, cages shall have a camera covering the entrance and be wired into the internal 24x7x365 CCTV system.
Anyone requiring badge access to any computer room shall follow a defined procedure approved by the third party including the badge holder's name, badge number, computer room location, reason access is needed, and termination date for a fixed duration. The Third-Party security office shall not configure any badge for computer room access without being authorized by the Third Party or designated team members.
The building exterior shall be periodically checked by scheduled security walk-throughs. Suspicious packages, activities, vehicles and/or people shall be investigated.
Data center parking area shall have physical obstacles in place to reduce risk of vehicle or car bomb penetrating exterior walls.
All data center workers shall be trained in control and storage of combustible materials (including paper and cardboard), and on the correct processes to follow when detecting a fire.
Server rooms shall not be used for storage and shall be clear of all unnecessary equipment and material not in use.
Detective monitoring and controls shall be implemented to mitigate the risk of overhead water sources impacting the IT equipment. Water detection shall be placed near air conditioners and any other water sources at the lowest level of the room.
Multiple methods of early fire detection shall be implemented and monitored 24X7x365 including smoke and temperature detection.
All data centers shall have a fire suppression system.
Loading bays and docks shall have CCTV coverage that provides a clear head-on view of the vehicle. This view shall be positioned to enable recognition of the driver, make of vehicle and registration number plate. The doors from the holding area into the data center shall conform to the interior security requirements for entrance to the data center. The movement, delivery or removal of any material or equipment into and out of the facility shall be recorded.
All switches and/or controls, which permit emergency shutdown of vital systems, shall have physical protection, audible alarm and signage to avoid accidental activation.

Third Party shall ensure that all computer devices are connected to surge protectors to protect them against spikes and surges in the electrical power supply.
Third Party shall ensure that backup power supply is available in the form of local generator(s).
Third Party shall ensure that all electrical and mechanical infrastructures are maintained per manufacturer specifications.
Emergency lighting, powered by a supply other than the main power, shall be implemented throughout the data center in accordance with local fire and health and safety regulations. Emergency lighting shall be activated when the fire alarm is raised, or when a degradation of power prevents the standard lights from operating.
The data center shall have systems in place to control and monitor temperature and humidity, air conditioning system to control air quality and minimize contamination. Server room temperature shall be controlled and monitored. Server room humidity shall be controlled and monitored within the range of 40-60% relative humidity.
The data center shall have air conditioning systems with separate zones for standard working areas, and areas containing equipment such as server rooms.
The air conditioning system supporting server rooms shall have dust filtration systems in place and shall be reviewed periodically to ensure air quality does not degrade / contamination increases.
Server rooms shall have positive pressurization to minimize contaminants entering these areas.
A process shall be in place for scheduled testing and maintenance of all critical data center infrastructure including security, power and environmental systems. Repairs or modification to facility security components (e.g., doors, locks, walls, hardware) shall be documented.
Critical data center infrastructure including power and environmental systems shall be engineered to function through an operational interruption. IT equipment with multiple power supplies shall leverage the redundant power infrastructure.
The data center access control system, and doors, shall be designed to maintain operation during scenarios such as: The failure of the access control application or hardware platform and a utility power outage.
All Treasury equipment shall be properly mounted in appropriately sized racks which are ground and/or ceiling mounted in accordance with local earthquake guidelines. Racks shall be labeled. Equipment in racks as well as cables into racks shall also have labels.
New equipment shall be stored in a secured area. Third Party personnel shall inspect the box for tampering before opening. Movement of used equipment containing Treasury data shall be done under the supervision of third-party personnel via a security approved process.
Third party shall have a documented equipment or media delivery or handling process.
Data centers shall have a disaster recovery plan for the facility and environmental that at least identifies and mitigates risks to Treasury services in the event of a disaster. The plan shall provide for contingencies to restore facility service if a disaster occurs, such as identified alternate data center sites. The plan shall be shared with Treasury to ensure Treasury can coordinate with its own DRP.
Data centers shall conduct an electrical blackout test, at least annually, to validate continue functionality through an operational interruption. Additionally, the data center shall participate and support Treasury DRP and associated testing.
All Treasury equipment shall be completely network segregated from non-Treasury parts of the data center.

XI. Direct, Trusted, Network Connection to Treasury

In addition to the Minimum Security Requirements defined above, the below requirements apply to all Third Parties (including Contractor) that have a direct, trusted network connection to Treasury:

Direct, Trusted, Network Connection Requirements
Third party shall use only Treasury managed devices or sessions, a Treasury Virtual Private Network (VPN) with two-factor authentication, or Virtual Desktop Infrastructure (VDI) with two-factor authentication to directly connect to Treasury resources.
Treasury conducts periodic scans on all Treasury owned IP addresses. If Treasury notifies the third party of any confirmed high or critical vulnerability found, the third party shall remediate the confirmed vulnerability within 30 days.
Remote access to a trusted Third-Party network is only allowed through the Treasury Virtual Private Network (VPN) with two-factor authentication.

XII. System and Data Availability

In addition to the Minimum Security Requirements defined above, the below requirements apply to all Third Parties (including Contractor) that manage, support, maintain systems or process, access, or store data that has high availability requirements, or the Third Party's service / application has high availability requirements as defined by Treasury:

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
12.1.1	Documented operating procedures	Operating procedures should be documented and made available to all users who need them.
12.1.3	Capacity management	The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
12.3.1	Information backup	Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.
17.1.1	Planning information security continuity	The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g., during a crisis or disaster.
17.1.2	Implementing information security continuity	The organization should establish, document, implement and maintain processes, procedures and controls to

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
		ensure the required level of continuity for information security during an adverse situation.
17.1.3	Verify, review and evaluate information security continuity	The organization should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

Additional Requirements
Third Party shall maintain a Disaster Recovery Plan (DRP) for all locations and applications used to provide services to Treasury. The DRP shall include the following elements: • Documented critical business functions, applications and supporting technologies. • Document what factors trigger a disaster, who is authorized to declare a disaster, and the communication plan, including notification to Treasury. • Identify alternate locations with the necessary infrastructure to support the recovery needs. • Document the management and membership of the disaster response and recovery teams. • Document service level, RTO's and RPO's. • Document the required recovery actions, identify and ensure the availability of required resources, and compile this information as the recovery plan. • Identify critical technology service provider dependencies and recovery support capability.
If Third Party provides a SaaS service, Third Party shall provide Treasury with geographically resilient hosting options. Third Party shall have more than one provider for each service for which there is a service delivery dependency
The disaster recovery plan must be reviewed and signed off every 12 months. Lessons learned should be captured as part of the disaster recovery exercise.
All data retention requirements should be documented and approved by Treasury.

XIII. PaaS Security

In addition to the Minimum Security Requirements and the Cloud Security Requirements defined above, the below requirements apply to all Third Parties (including Contractor) that provide a cloud computing platform to Treasury to develop, run, and manage applications:

PaaS Requirements
Maintain effective policies, guidelines, and processes to govern and control Virtual Machine (VM) lifecycle management, including self-service and automated scripts / DevOps tools.
Control the creation, storage, use, retirement and destruction of VM images with a formal change management process and tools and approve additions only when necessary.

Keep a small number of known-good and timely patched images of a guest operating system separately and use them for fast recovery and restoration of systems to the desired baseline.
Discover virtual systems, including dormant VMs and the applications running on them, regularly.
Use virtualization products with management solutions to examine, patch, and apply security configuration changes to VMs.
Maintain policies to restrict storage of VM images and snapshots. If it is necessary to store images and snapshots, proper authorization, such as secondary level of approval, shall be obtained and corresponding monitoring and control processes shall be established.
Control the backup, archiving, distribution, and restart of VMs with effective policies, guidelines, and processes such as suitably tagging the VM based on sensitivity / risk level.
Create a controlled environment to apply security patches and control policies to an offline or dormant VM.
Regularly monitor virtual appliances that provide critical infrastructure, management, and security services.
Ensure proper hardening and protection of VM instances through VM guest hardening.