DTCC MINIMUM RISK MANAGEMENT AND INFORMATION SECURITY REQUIREMENTS

1. INTRODUCTION

1.1 These Minimum Risk Management and Information Security Requirements (the **Minimum Requirements**) describe certain technical and organisational measures regarding risk management and information security to which entities within the vendor group (each a **Service Provider**) will adhere in the delivery of relevant services using commercially reasonably efforts to accomplish the stated Minimum Requirement. The most up to date version of the Minimum Requirements can be found under the Frequently Asked Questions section of https://www.dtcc.com/vendor-management. These Minimum Requirements are stated in a general manner, in recognition that there may be multiple approaches to accomplish a particular requirement set out herein. These Minimum Requirements are not intended to replace a Service Provider's standard policies and procedures but are intended to address the minimum controls that the Service Provider will have in place in connection with the services to which these Minimum Requirements relate.

1.2 These Minimum Requirements apply where the Service Provider has access to information of its current customers (each a **Customer**) that is considered to be confidential under the existing agreement in place with the Customer or is otherwise defined by applicable law as personal information, personal data, or personal identifiable information (such information, **Customer's Confidential Information**) or uses Information Systems to provide the Customer with the services. The Service Provider provides in its agreements with those persons who perform some or all of the obligations of the Service Provider under the applicable agreement with the Customer (each, a **Subcontractor**) that such Subcontractors apply the Minimum Requirements (as if the Subcontractors were themselves the Service Provider) where the Subcontractors have, process, or otherwise have access to Customer's Confidential Information and/or Information Systems.

1.3 These Minimum Requirements do not limit a Service Provider's obligations under any agreement the Service Provider may have entered into or under applicable laws.

1.4 Each Service Provider will be able to reasonably show on request how it meets these Minimum Requirements through its technical, organisational and information security measures, controls, policies, procedures or practices. Where the stated Minimum Requirements do not apply to all services provided by a Service Provider, such Service Provider is able to reasonably show how the relevant requirement does not apply.

1.5 Any request for information made by a Customer in connection with these Minimum Requirements must be made in writing, with sufficient particularity and substantiation as to the basis of the request. The Service Provider as appropriate under the circumstances will reply to such requests within a reasonable timeframe. Unless otherwise provided in a Customer agreement or elsewhere in these Minimum Requirements, the number and frequency of such Customer requests should be reasonable and legitimate from a risk management perspective. All information provided by the Service Provider in response to such requests will constitute the Service Provider's confidential information and be subject to the confidentiality restrictions set out under the relevant Customer agreement.

2. DEFINITIONS FOR THESE MINIMUM REQUIREMENTS

2.1 **Assessment Information** means such information and assistance provided by the Service Provider as is reasonably necessary to enable the Customer to (i) assess the ongoing risk associated with the services the Customer is receiving in line with Industry Security Standards; and (ii) evaluate the Service Provider's

information security capability and controls; and (iii) assess any information security weaknesses identified by such information and the resolution of those weaknesses as determined by the Service Provider.

2.2 **Industry Security Standards** means a set of controls outlined in published materials for the purpose of protecting the digital infrastructure of an organisation, which are reasonably designed and consistent with global financial-sector information security and cybersecurity industry standards issued by a financial services regulatory authority in the jurisdiction in which the Service Provider operates or a widely recognised industry organisation.

2.3 **Information** means information processed, stored or transmitted in Information Assets, including the Customer's Confidential Information.

2.4 **Information Assets** means applications, services, information technology assets or other information handling components, which includes the operating environment and networks used to provide the Services.

2.5 **Information System** means a set of Information Assets processing, storing or transmitting Information.

2.6 **Major Security Incident** means a Security Incident that has or is reasonably anticipated to, for example, disrupt, degrade, cause a delay in, interrupt or otherwise alter the normal operation of an Information System, result in unauthorized access to an Information System; result in the loss of control of, disclosure of, or loss of Information; or cause a strain on, loss of, or overall threat to the resources, functions, security or operations.

2.7 **Penetration Testing** means a test methodology in accordance with Industry Security Standards in which assessors working under specific constraints attempt to circumvent or defeat the security features protecting Information, Information Assets or an Information System.

2.8 **Security Incident** means an event that compromises the security of an Information System and has an adverse impact on the availability, authenticity, integrity, or confidentiality of data or the services, whether resulting from malicious activity or not.

3. GOVERNANCE MEASURES

3.1 Technical and Organisational Measures.

(a) The Service Provider will implement appropriate technical and organisational measures to maintain a level of information security in line with Industry Security Standards based on the risk associated with the relevant service and the type of information the Service Provider is customarily given access to in connection with such services, as assessed reasonably by the Service Provider and as adequate for the type and scope of the services it provides.

(b) Such technical and organisational security measures include measures to ensure the security, availability, integrity, and confidentiality of Customer's Confidential Information and to protect against the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer's Confidential Information.

(c) The Service Provider will implement appropriate security policies and procedures which govern the receipt, transmission, processing, storage, control, distribution, retrieval, access, presentation, and protection of Information Systems and Information Assets.

(d) The Service Provider will implement appropriate enterprise cybersecurity policies and procedures around managing Information Systems, Information Assets and Information to address change, configuration and release management, capacity management, technical vulnerability and patch management, and network management.

(e) The Service Provider will implement preventative monitoring and detection controls in line with Industry Security Standards.

(f) The Service Provider will implement appropriate policies and procedures to manage a secure systems development life cycle, including a procedure that results in timely resolution of all discovered high and medium risk vulnerabilities (using the common vulnerability scoring system, also known as CVSS), a security checkpoint in change management, and procedures to keep development, testing and production environments separate.

3.2 Management of Security Risks. The Service Provider will designate a qualified individual to be responsible for overseeing and implementing the Service Provider's cyber security risk management program and enforcing the Service Provider's cyber security policies.

3.3 Systems Connected to Service Provider's and its Affiliates' Infrastructure. Security controls over the communication network and standard configurations, using the principles of least functionality/privileges, will be established and security hardening demonstrated. Service Provider will take commercially reasonable measures to ensure that the connectivity between it and its affiliates systems, that are connected and sharing information required to support services delivered, is securely configured and hardened. The Service Provider will also take commercially reasonable measures to test such connectivity for identified weaknesses and common vulnerabilities in the relevant services industry in accordance with Service Provider's applicable policies and procedures.

3.4 Compliance.

(a) Service Provider will implement an information security policy documented and approved by its senior management that aligns with Industry Security Standards and covers the following areas:

- information security management;
- data governance and classification;
- asset inventory and device management;
- access controls and identity management;
- systems operations and availability controls;
- systems and network security and monitoring;
- systems and application development and quality assurance;
- physical security and environmental controls;
- data privacy and protection;
- vendor and subcontractor management; and

- risk assessment and incident response.

(b) Service Provider will review its security processes, procedures and controls at least annually. Service Provider will provide on request, a high-level overview of the Service Provider's relevant security policy addressing the particular area of concern expressed by Customer, provided such a request is made no more than once during any twelve (12) month period.

3.5 Ongoing Risk Assessments. Service Provider will periodically conduct a security risk assessment sufficient to ascertain that Service Provider's information security program meets its security requirements and reasonably takes into account technological developments and evolving threats. Service Provider will ensure that security risks are identified, assessed, and addressed and appropriate security controls are applied, based on the assessed risk from time to time. Service Provider will provide on request a standard suite of documentation that provide a high-level overview of the Service Provider's information security profile, provided such request is made no more than once during any twelve (12) month period.

3.6 Customer Information Security Reports. For relevant services, Service Provider will instruct its auditors to examine the controls placed in the operation and test the operating effectiveness of the relevant services on an appropriate and periodic basis. Service Provider will take appropriate steps to address material issues or to minimise risks identified by the auditors. Where the report is produced as part of the Service Provider's customary practices for the purpose of sharing with clients or is generally expected in line with Industry Security Standards from the Service Provider in connection with the type of services the Customer receives, a copy of such report will be provided to the Customer on request.

3.7 Customer Due Diligence and Security Questionnaires. The Service Provider will cooperate in the Customer's due diligence process conducted at the time of onboarding as is reasonably necessary for the Customer to be able to assess the risk associated with the Service Provider's services the Customer will be receiving in line with Industry Security Standards. Once the Customer is onboarded, the Service Provider will also respond to Customer's standard and reasonable security questionnaires in connection with its services to Customer and provide updated Assessment Information. The Customer may request such Assessment Information no more than once during any twelve (12) month period. However, this annual limit does not prohibit additional assessments if required by a regulatory authority. All information provided by the Service Provider in response to such requests will constitute the Service Provider's confidential information and be subject to the confidentiality restrictions set out under the relevant Customer agreement and applicable law.

3.8 Incident Response Preparation. The Service Provider will maintain, practice and comply with its written incident response plan designed to detect and respond to a Security Incident and promptly notify the Customer of any Major Security Incident and cooperate with the Customer to identify the root cause and resolve such Major Security Incident. The Customer can ask its Service Provider to provide a high-level overview of its incident response policy, provided the request is made no more than once during any twelve (12) month period.

3.9 Third Party Risk Management. The Service Provider's written information security program will include policies, procedures and controls addressing third party risk management and governance in line with Industry Security Standards.

4. PHYSICAL SECURITY AND BARRIERS

4.1 Secure Buildings and Premises. The buildings and premises the Service Provider uses to perform the relevant services are designed to be physically secure, to manage and monitor movement of persons into and out of facilities where the Information is processed, and to allow access only to authorised individuals.

A secure environment includes the availability of onsite security personnel on a 24 x 7 basis, alarms against unauthorised access and forced entry or equivalent means of monitoring locations supporting the delivery of the relevant services.

4.2 Physical Security of Media. The Service Provider maintains physical controls to protect software, computing devices, and networks from environmental hazards and unauthorised access, view, copy, alteration, removal or destruction.

4.3 Segregation. For relevant services, the Service Provider logically segregates the Customer's Confidential Information from the information and accounts of Service Provider's other customers, so that such information is not accessible by any such other customers or by any third parties accessing the information of such other customers. Access to the Customer's account on the services will be managed by the Customer's authorised users.

5. ACCESS, LOGGING AND MONITORING

5.1 Security-related Events Log. The Service Provider logs and monitors security-related events on all levels (e.g. operating system, database and application) in accordance with the Service Provider's applicable policies and procedures as required by Service Provider's legal and regulatory obligations.

5.2 Access Controls. The Service Provider maintains controls to limit access to any Information in the Information System to the Service Provider's personnel who have a legitimate need for such access to provide the relevant services and ensure any access is commensurate with a user's job responsibilities. The Service Provider's access controls are based on the security principles of "segregation of duties" and "least privilege" with respect to the Customer's Confidential Information and require proper Service Provider approval for any new user accounts. The access rights of the Service Provider's personnel and external party users to information and information processing facilities is adjusted upon a change of role and removed upon the termination of their employment, contract or agreement.

5.3 Remote Access Controls. The Service Provider maintains remote access controls to monitor and control access to Service Provider's systems or networks, including requiring multifactor authentication for Service Provider personnel accessing the Service Provider's network from an external system or network and other protections in line with the Service Provider's policies and procedures.

5.4 Customer and Subscriber Access. Only the Customer's authorised users will be able to access the Customer's account and the Customer's Confidential Information.

6. DATA HANDLING

6.1 Correctness and Integrity. The Service Provider implements effective controls to ensure appropriate collection, processing and protection of personal information in accordance with applicable laws. Apart from changes made by operation of relevant services, the Service Provider will not make changes to the Information unless requested to do so by the relevant Customer as part of the delivery of services. The Service Provider will notify the Customer of any event that may or will impact that the confidentiality, integrity or availability of personal information, including unauthorized intrusion into systems storing such personal information as defined by applicable law.

6.2 Encryption. The Service Provider encrypts all the Information in transit to/from and stored as part of the relevant services in accordance with Service Provider's data classification policies and procedures. Service Provider manages and stores all cryptographic keys in a secure manner.

6.3 Security Controls: The Service Provider maintains security controls with respect to the Information. Such controls are consistent with the Service Provider's applicable policies and procedures, including network security controls, confirmation and maintenance of software, computing devices and networks, and timely updates to software and firmware.

7. OPERATIONAL SECURITY

7.1 Malware Protection. The Service Provider implements measures to adequately protect against malicious code and apply up-to-date security patches as necessary in delivering the relevant services. The Service Provider regularly updates antivirus software, periodically scans for viruses (which includes real-time scanning) and protects the systems used to provide services to the Customer through properly configured firewalls and security devices which protect systems from unwanted access through the network.

7.2 Password Authentication and Management. In relation to relevant services, the Service Provider maintains password and authentication controls to establish, manage and control password and authentication requirements (e.g., password complexity and expiration, two-factor authentication, lockout after multiple login attempts, API keys) for all the Customer's accounts with access to such services. In relation to internal accounts used by the Service Provider's personnel, the Service Provider maintains password and authentication controls for all individuals with access to the Information in the Information System, whether direct or indirect.

8. PENETRATION TESTING

The Service Provider will periodically perform Penetration Testing in accordance with such relevant technical documentation made generally available electronically or in hard copy form by Service Provider to the Customers for the services. The Service Provider analyses the results of the Penetration Testing and, if it considers it necessary in light of the results, will make changes to the relevant services. The Customer can request, and Service Provider will provide, a summary of the results of the most recent Penetration Test, provided that the Customer must not make such request more than once during any twelve (12) month period or any other minimum period set out in the applicable agreement with the Customer.

9. SECURITY RISKS

9.1 Incident Detection and Management Processes. The Service Provider will implement a documented process around (i) the detection and analysis of anomalous events affecting the Information, Information Assets and Information Systems, (ii) the root cause analysis of incidents impacting the Information, Information Assets and Information Systems, with a view to implement permanent fixes and minimise the reoccurrences of incidents; and (iii) incident tracking, reporting, classification, prioritization, internal escalation, remediation, and preservation of data for all incidents impacting its Information and Information Systems. These processes will be reviewed on an annual basis.

9.2 Security Risks Communication. The Service Provider will respond to a query by the Customer that is triggered by an industry or government agency announcement, or the discovery of a high risk, zero-day technical vulnerability malware, or similar persistent threats which have the potential to have a broad industry-wide impact to the financial services industry or related industries, in a reasonable time period (which will not be longer than thirty (30) days).

10. QUALITY ASSURANCE

The Service Provider maintains a quality assurance program and validates that any software licensed in relation to relevant Services has undergone quality controls testing to identify and correct potential cybersecurity weaknesses and vulnerabilities.