version 2022.June

FIS SECURITY STATEMENT

1. Introduction

This Security Statement ("**Statement**") summarizes FIS' information security policies, procedures and standards including its technical and organizational measures for the security of data ("**FIS' Information Security Practices**") and forms an integral part of the agreement between Client or Client's affiliate(s) and FIS which incorporates this Statement by reference ("**Agreement**"). The Statement sets out FIS' obligations with respect to information security and data protection in relation to the Agreement. To the extent of any conflict or inconsistency between the provisions of this Statement and any provision of the Agreement, the provisions of this Statement prevail and take precedence over such conflicting or inconsistent provisions.

FIS' Information Security Practices are compliant with International Organization for Standardization ISO 27001:2013 and are designed to protect the security, confidentiality and integrity of Client Data and Client Personal Data processed or stored on FIS' systems pursuant to the Agreement.

Additional information on FIS' Information Security Practices is made available to Client under the Vendor Management Resource Center on the Client Portal (as defined below) or upon request. Such information is FIS' Confidential Information.

2. Organizational Practices

FIS' Information Security Department is responsible for developing and implementing FIS' Information Security Practices. FIS maintains safeguards designed to prevent the compromise or unauthorized disclosure of Client's Confidential Information, Client Data, and Personal Data, including loss, corruption, destruction or mis-transmission of Client's Confidential Information, Client Data, and Personal Data.

FIS maintains FIS' Information Security Practices designed to comply with (1) all applicable laws relating to the privacy, confidentiality and security of Client's Confidential Information, including Client Data and Client Personal Data to the extent applicable to FIS as a third-party service provider; (2) the requirements set forth in this Statement; and (3) all applicable provisions of FIS' related policies including but not limited to FIS' Information Security Policy. Client may review additional information concerning FIS' Information Security Practices in the Client Portal.

FIS' internal and external auditors regularly review FIS' Information Security Practices. FIS performs security assessment reviews to determine whether identified vulnerabilities, in particular as related to web and network environments have been remediated. Security assessment reviews include: diagnostic reviews of devices, internal and external penetration testing, assessments of applications that can access sensitive data and assessments of FIS' Information Security Practices.

FIS updates FIS' Information Security Practices from time to time in response to evolving information security threats. Such updates provide at least an equivalent or increased level of security compared to what is described in this Statement, and FIS will provide Client with a summary of any updates upon request.

FIS implements commercially reasonable administrative, technical, and physical safeguards designed to: (i) provide for the security and confidentiality of Client Data and Client Personal Data; (ii) protect against any anticipated threats or hazards to the security or integrity of Client Data and Client Personal Data; and (iii) protect against unauthorized access to or use of Client Data and Client Personal Data. FIS will review and test such safeguards on no less than an annual basis. FIS has processes for regularly testing, assessing and evaluating the effectiveness of its technical and organizational measures in order to verify the security of its processing. The measures are described throughout this Statement.

3. Security Controls

3.1. Access Control to Facilities

3.1.1. FIS Facility Restrictions

Access to FIS facilities is restricted using controls such as camera coverage and badge access. Badges and keys are only distributed in accordance with documented organizational procedures. Visitors are screened prior to admittance, are provided a visitor badge, and in sensitive areas require an escort in accordance with FIS' Information Security Policy. Alarm systems are in place to notify appropriate individuals of potential threats. FIS regularly tests its emergency procedure protocols.

Physical security measures implemented at FIS offices are designed to protect employees, visitors, and assets. Physical security consists of a combination of physical barriers, electronic access and monitoring systems, Security Officers and procedures for controlling access to buildings and sensitive or restricted areas. Security is staffed 24 hours a day, seven days a week, at FIS data center facilities. Secure shred bins are provided for the proper disposal of hard copy documentation and other small media thorough-out the campus.

An access control system utilizing individual badge identification, doors protected by an electronic badge reader or locked with limited access to the physical key, closed circuit camera monitoring, and onsite physical security guards stationed in strategic locations are utilized to provide facility physical security and protection. Physical access to FIS buildings, office spaces and certain secured areas within the facility are controlled by an electronic access control system. The system provides for real-time monitoring of all electronic badge accesses across the monitored facility, requires physical security officer acknowledgement of system identified error codes or issues, and is tied to centralized servers communicating the exact date and time stamp for each entry (utilizing network time protocol). Automated database backups are performed daily and are replicated on the secondary server.

For data centers, FIS maintains automatic early-warning sensors (e.g., fire, water, temperature and humidity), independent air conditioning systems and fire suppression systems. Mission-critical hardware is protected by an emergency power supply system with batteries and backup generators. Hazardous or combustible materials are kept at a safe distance from information assets.

3.2. Logical Controls and Security

FIS has a dedicated group that is responsible for overseeing operational security, network security, host and server security, applications and system development, patch and vulnerability management, authentication and remote passwords, encryption, passwords and monitoring systems (collectively, "**Logical Controls and Security**"). FIS has documented protocols for all Logical Controls and Security including the following:

3.2.1 Employees

FIS performs (at the time of hire) a background check, as described herein, for each FIS employee that is performing any services under the Agreement. Currently, the background check in the United States of America consists of, at a minimum, verification of the highest level of education completed, verification of employment (as allowed by applicable law), social security number trace and validation, and a check of U.S. Government Specially Designated National (OFAC) and other export denial lists. Background checks outside of the United States consist of similar reviews to the extent allowed by local laws of each country. In addition, to the extent permitted by law, the background check may include a 9-panel drug test and credit and criminal record search. FIS complies with all applicable laws related to the background check, including required notices and applicable consents. FIS will not assign any employee to perform services for Client if his/her background check findings do not meet the standards established by FIS. FIS assigns all employees mandatory security awareness training on an annual basis. FIS requires all employees with access to sensitive information to follow a clean desk and clear screen standard such that the information is controlled and/or protected at all times. FIS has formal disciplinary procedures in place to address policy violations. A terminated employee's access to FIS facilities and FIS systems containing Client Data and Client Personal Data is suspended upon termination.

3.2.2 Network Security

FIS employs a defensive model when building networks (including firewalls) in a multi-tiered approach and uses separate layers of presentation, business logic and data when considered necessary. Connection between networks is limited to those ports and services required for FIS to support, secure, monitor and perform the services under the Agreement.

FIS uses Network Intrusion Detection and/or Prevention Systems to monitor threats to the FIS environment. FIS monitors these threats 24x7x365/366.

FIS may from time to time in its reasonable discretion block attempted access to FIS services from technology of individuals, entities, or governments FIS reasonably believes may pose a threat to FIS services, systems or clients (such technology, "Suspicious Technology"). Due to the unknown timing of cyber threats, FIS may not be able to provide Client prior notice of blocking the Suspicious Technology, and it may impact the availability of FIS services. If Client is adversely affected, FIS will make reasonable efforts to resolve any impacts to Client as long as FIS can reasonably prevent any ongoing threats to FIS services, systems and clients.

3.2.3 Host and Server Security

FIS hardens its operating systems in accordance with industry security standards and procedures. For example, FIS requires all default passwords are changed, unneeded functionality is disabled or removed, FIS adheres to the concept of "least-privileged" access, file permissions do not include world writeable ability, administrative or "root" access is limited to the console only, and only those network ports that are necessary to provide the services are opened. For database installations, FIS uses security at a table and row level, based upon the placement of a system and its role in the environment. FIS requires that anti-virus and anti-spyware software is enabled on its operating systems when they are available and supported by commercially available anti-virus solutions.

Access to FIS' operating systems is limited to those individuals required to support the system. FIS has implemented appropriate change management processes. Servers and workstations are enabled with auto-locking (password-protected) screensavers that activate after a period of inactivity. Installation of personal software is not allowed.

3.2.4 Applications and Systems Development

FIS uses System Development Lifecycle and system change procedures, which include requirements for code review and secure coding practices. Development and testing environments are segregated and firewalled from FIS' production environment. Version control software is utilized for the management and deployment of code through appropriate support groups. FIS applies measures for verifying system configuration, including default configuration. FIS considers data protection issues as part of the design and implementation of systems, services, products and business practices (Privacy bv Design).

3.2.5 Electronic Mail

FIS scans incoming emails and attachments prior to allowing them into the FIS environment. FIS also uses industry leading software to control what files are allowed or blocked as attachments to protect against malicious executable files being delivered and/or opened.

3.2.6 Patch and Vulnerability Management

FIS analyzes, tests, reviews and subsequently installs software updates on FIS systems and security patches as soon as reasonably possible after release. Critical security updates are promptly installed after testing is completed. FIS performs vulnerability scans, including scans on application and internal/external network infrastructure. Ethical hacking/penetration tests are performed by FIS on a periodic basis. FIS reviews, prioritizes and remediates known vulnerabilities based on identified risk factors.

3.2.6.1 Penetration Tests.

FIS conducts a penetration test and security evaluation, which includes tests to detect vulnerabilities listed in the SANS Top-20 or OWASP or its successor current at the time of the penetration test and security evaluation. Upon written request from Client, FIS will provide a high level summary of the penetration test and security evaluation to the Client. Personnel performing the penetration test is independent of the controls being tested and do not report to the individuals who make the funding decisions for any noted vulnerabilities that require remediation.

3.2.6.2 Dynamic Application Scanning.

FIS conducts dynamic application scanning, which includes scanning for vulnerabilities listed in the SANS Top 20 or OWASP or its successor current at the time of the dynamic application scan. FIS will provide a summary of the dynamic application scan to Client upon request. The scan is performed using an industry standard tool and occurs no less than twice a year.

3.2.6.3 Static Application Security Testing.

FIS conducts static application security scanning, which include scanning for vulnerabilities listed in the SANS Top 20 or OWASP or its successor current at the time of the static application security scan. FIS will provide a summary of the static application security scan to Client upon request. The scan is performed using an industry standard tool.

3.2.6.4 Vulnerability Assessment.

FIS maintains a vulnerability management program based on industry standard practices that frequently assesses all FIS computing devices and systems (including without limitation all such devices and systems used by FIS to provide any services under the Agreement) and all software provided by FIS under the Agreement to verify that the applicable security controls are sound, and that mitigates or eliminates vulnerabilities. As part of such program, (i) FIS uses an industry standard tool to perform all vulnerability scans or engage, at its expense, an unrelated security firm to perform the assessment; and (ii) routine network, database and software scans are scheduled on a periodic basis;

3.2.6.5 Reporting and Remediation of Findings.

FIS provides to Client annually (or at such other more frequent intervals as requested by Client and mutually agreed upon by both parties) a summary which describes the results of the assessment. FIS will remediate any findings in accordance with FIS remediation timeframe policy based upon the CVSS scoring.

3.2.6.6 Client Security Testing.

FIS does not allow or consent to any form of direct security testing initiated by its clients or on behalf of its clients (including Client) in shared (multi-tenancy) FIS hosted environments, including but not limited to, vulnerability scanning, penetration testing, application code scanning, dynamic testing, installation of audit software, direct access to systems, or ethical hacking of FIS systems, applications, databases, or networks, except as may otherwise be agreed by the FIS Chief Information Security Officer and/or designee, as evidenced in writing signed by both FIS and Client.

If Client wishes to perform any form of security testing (i) in an FIS hosted environment dedicated to Client, then Client shall send, reasonably in advance, a written detailed request to the FIS Chief Information Security Officer and/or designee, await written confirmation from FIS and observe FIS scheduling instructions and other limitations communicated by FIS, in addition to the requirements set forth in the next paragraph; or (ii) in a Client hosted environment, the requirements set forth in the next paragraph will apply.

Any security testing initiated by Client shall be subject to the following conditions: (i) Client shall securely (e.g. encrypted) email, without undue delay, all potential vulnerabilities to: BugBounty@fisglobal.com and the relevant FIS relationship manager; and (ii) Client agrees to hold any such potential vulnerabilities and any testing results, reports or related information in strict confidence, and only disclose them to FIS as outlined in (i) in this paragraph. Once said potential vulnerabilities are communicated to FIS, FIS will perform security testing and work with Client to remediate confirmed vulnerabilities in accordance with FIS vulnerability management policies.

Client understands and agrees that, notwithstanding any other stipulation in this subsection 3.2.6.6, FIS will not acknowledge any results from any form of security testing that is not performed by FIS.

3.2.7 Authentication.

The level of authentication required to access a particular FIS environment is based on the type of data protected within that environment. FIS permits only authorized persons to access any FIS systems in accordance with FIS' Information Security Policy. User authentications (i.e. user name and password) are bound to the respective user and may not be shared. The use of an emergency user account must be documented and logged. Remote access to FIS' systems requires the use of multi-factor authentication.

3.2.8 Passwords

FIS requires the use of complex passwords. User accounts are locked after a defined number of abortive or unsuccessful logon attempts. If a password is possibly disclosed, it is changed without undue delay. Using a documented procedure, FIS employs processes to minimize the risk of unauthorized or no longer needed user accounts in the systems and audits user accounts to determine that access that is no longer required is revoked.

3.2.9 Data Classification, Retention, and Controls

FIS' Information Security Policy addresses the confidentiality, integrity, security, availability, retention and disposal of Client Data and any Client Personal Data. All FIS employees and vendors with access to Client Data or Client Personal Data are required to comply with secure deletion standards in alignment with the latest NIST *Guidelines for Media Sanitization*. FIS will store Client Data and Client Personal Data only for as long as necessary to achieve the purposes for which it was collected, for a contractually committed time period as set forth in the Agreement or in accordance with applicable laws.

FIS takes reasonable steps to determine access to Client Personal Data. FIS' Enterprise Identity and Access Management Policy is based on the "principle of least privilege," which calls for authorized users to access only the minimum level of Client Personal Data required to satisfy the user's job responsibilities.

3.2.10 Encryption

FIS has developed encryption key management policies and procedures in accordance with industry standards. FIS encrypts data at rest that is Client Data or Client Personal Data when and where FIS has implemented the ability to do so. Data is encrypted based on data classification policies and standards. FIS will use encryption key lengths that meet current NIST FIPS 140-2 standards. FIS policies require that FIS shall not transmit any unencrypted Client Data or Client Personal Data over the internet. Specific algorithm and other minimum key lengths are specified within FIS' policy.

3.2.11 Monitoring Systems and Procedures / Logging

FIS uses a real-time event management system to monitor its networks and servers via system logs, intrusion detection/prevention systems, data loss prevention, file integrity monitoring and firewall logs on a 24-hour per day basis. FIS will perform reasonable logging, monitoring, or record keeping of user activity where legally permissible and in accordance with FIS' applicable information retention standards.

4 Business Continuity and Disaster Recovery / Availability

FIS has a Global Business Resilience ("**GBR**") program and maintains recovery and response plans ("**Plans**") designed to minimize the risks associated with crisis events affecting FIS' ability to provide the services under the Agreement. Plans are designed to maintain a consistent provision of the Solution(s) in the event of a crisis incident affecting FIS' operations. FIS' GBR program meets the FFIEC business continuity guidelines and the PS-Prep / ISO 22301 business continuity international standards or similar equivalent standard.

FIS' collection of comprehensive and coordinated Plans are designed to address the agreed crisis response, continuity, and recovery needs for the Solution(s), including recovery time objective ("**RTO**") and recovery point objective ("**RPO**").

FIS provides a summary of the GBR program in the Client Portal or upon written request. FIS' RTO and RPO are as set forth in such summary. FIS maintains adequate backup procedures in order to recover Client Data to such RPO and within the RTO. FIS validates the efficacy and vialibity of its Plans at least annually to confirm viability and provide assurance of resilience capabilities as well as the readiness of Plans' participants. Recovery exercise results are provided via the Client Portal or upon request.

5 Vendor Management

FIS has an established Vendor Risk Management Program that uses subject matter experts from across the enterprise to determine FIS supplier's criticality and ability to meet business and control requirements throughout the lifecycle of the relationship.

FIS conducts a risk assessment for all third-party suppliers engaged in the provision of services under the Agreement to validate compliance with FIS' standards. FIS' risk assessment requires suppliers to confirm if they have appropriate contracts in place with their vendors that store, process, transmit, manage or access Client Data or Client Personal Data. FIS only allows such third-party suppliers to access, store, transmit, manage, or process Client Data and Client Personal Data, to the extent permissible under the Agreement and applicable laws.

Where required by law, FIS requires its suppliers to agree to data protection agreements to oblige such to comply with applicable data protection laws. Such suppliers shall as a minimum implement appropriate technical and organizational measures to verify a level of security appropriate to the risk. Upon FIS' request, FIS' suppliers shall provide a written description of their technical and organizational measures for processing Client Personal Data. FIS' suppliers must cooperate upon reasonable request in order to assist FIS with its compliance with applicable privacy laws.

FIS maintains a list of all third-party suppliers with access to Client Personal Data on the Client Portal (also available upon request).

6 Data Minimization

The Client is responsible for verifying the Client Data and Client Personal Data provided to FIS for processing or other purposes of the Agreement are accurate, current, adequate, of appropriate quality, relevant, minimal, and not excessive.

7 Defined Terms

As used in this Statement, the following terms have the following meanings:

"**Client Data**" means data introduced into the Solution by or on behalf of Client or Client's customers that is stored in or processed by the Solution.

"**Client Portal**" means a self-service portal made available to Client's designated representatives at Client's request at https://my.fisglobal.com/vendor-management offering specific Client resources to help better manage its relationship with FIS, including information about FIS' information security practices;

"**Confidential Information**" is all business or technical information disclosed by Client to FIS or by FIS to Client in connection with the Agreement. Confidential Information includes without limitation: (i) Client Data, Client Personal Data, information that is protected by applicable banking secrecy laws and the details of Client's computer operations; and (ii) details of the Solution(s).

"**Solution(s)**" means the software and/or services being provided by FIS to Client under the terms of the Agreement.