FIS Security Statement

1. INTRODUCTION

1.1 This Security Statement ("**Statement**") summarizes FIS cybersecurity policies, procedures, processes and standards including its technical and organizational measures regarding the availability, authenticity, integrity and confidentiality of all data ("**FIS Cybersecurity Practices**") and forms an integral part of the agreement between Client and FIS which incorporates this Statement by reference ("**Agreement**"). This Statement sets out FIS obligations with respect to cybersecurity 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.

1.2 FIS Cybersecurity Practices are compliant with International Organization for Standardization ISO 27001:2022, are aligned to the NIST and CIS frameworks, and are designed to protect the availability, authenticity, integrity and confidentiality of Client Data, including Client Personal Data. The FIS ISO 27001:2022 certification is available on the Vendor Management Resource Center on the Client Portal (as defined below) or upon request.

1.3 Additional information on FIS Cybersecurity Practices is made available to Client under the Vendor Management Resource Center on the Client Portal or upon request. All information about FIS Cybersecurity Practices on the Client Portal is FIS Confidential Information.

2. ORGANIZATIONAL PRACTICES

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

2.2 FIS Cybersecurity practices are designed to comply with (1) all applicable laws and industry standard practices relating to the privacy, confidentiality, availability, authenticity, integrity and security of Client 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 related FIS policies, including but not limited to the FIS Cybersecurity Standard.

2.3 FIS' internal and external auditors review FIS' global Cybersecurity Practices on at least an annual basis. Additionally, FIS internal and external auditors perform regular security assessments on FIS Cybersecurity Practices to determine whether identified vulnerabilities, in particular as related to web and network environments, have been remediated. Security assessments include: diagnostic reviews of devices, internal and external penetration testing, assessments of applications with access to sensitive data, assessments of various FIS systems, and reviews of FIS Cybersecurity Practices.

2.4 Periodic updates are made to FIS Cybersecurity Practices preempting and responding to evolving cybersecurity 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 material updates upon request. In no event shall FIS make any material changes to its Cybersecurity Practices that reduce, limit, or adversely affect Client's rights and/or FIS obligations under this Statement without the prior written consent of Client.

2.5 FIS implements reasonable (industry standard) administrative, technical, organizational and physical safeguards designed to: (i) provide for the security and confidentiality of Client Data, including Client Personal Data; (ii) protect against any anticipated threats or hazards to the security or integrity of Client Data, including Client Confidential Information and Client Personal Data; and (iii) protect against unauthorized access to or use of Client Data, including Client Confidential Information 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.

2.6 To enhance data management, reduce compliance risks, and improve security and operational efficiency, our data discovery and classification scanning platform performs scans to identify, classify and locate data, including Client Confidential Information and Client Personal Data, across its systems and databases. Securely designed scanners are

Classified as Public - This content can be shared with anyone.

hosted on-premises in FIS data centers, collecting only encrypted metadata governed by the principle of least privilege and enforced through role-based access control.

3. SECURITY CONTROLS

3.1 Access Control to Facilities

3.1.1 FIS Facility Restrictions

FIS uses a number of technological and operational approaches in its physical security program to mitigate security risks to the extent reasonably practicable. The FIS security team works closely with FIS facilities teams at each FIS facility to confirm appropriate measures are in place to prevent unauthorized persons from gaining access to systems within which data is processed. The FIS security team also continually monitors any changes to the physical infrastructure, business, and known threats which may impact the physical security of FIS work sites.

Access to FIS facilities is restricted and monitored using controls such as badge access, camera coverage, door alarms and guards. Badges and keys are only distributed in accordance with documented organizational procedures. Visitors' identities are verified prior to admittance, are provided a visitor badge, and in sensitive areas require an escort in accordance with the FIS Corporate 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 facilities are designed to protect employees, contractors, 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. Physical security is staffed 24 hours a day, seven days a week, at data center facilities used by FIS in the provision of the Solution. Secure shred bins or shredders are provided for the proper disposal of hard copy documentation and other small media at FIS facilities.

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 FIS facilities 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.

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 highly combustible materials are kept at a safe distance from information assets.

3.1.2 Client Policies and Client Location Access

FIS personnel, who will perform Professional Services at Client's site, will not sign any individual undertakings from Client. FIS remains responsible for its personnel's acts and/or omissions whilst at Client's site. If FIS personnel receive access cards or keys that provide them with access to Client's premises, FIS shall take reasonable measures designed to ensure that (a) such access cards and/or keys are only used for their intended purpose; (b) are protected from access by unauthorized third parties; (c) are promptly returned to Client once the Professional Services have been completed; and (d) any loss is reported to Client without undue delay.

FIS personnel, who will perform Professional Services using FIS devices, will not disable the FIS Virtual Private Network (VPN). FIS cannot permit the use of Client VPNs on or connection of FIS devices to Client networks.

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

Prior to onboarding, FIS conducts a background check for each FIS employee who is involved in the provision of the Solution and/or performing Professional Services. 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

Classified as Public - This content can be shared with anyone.

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 the onboarding location country, and may, in addition to the above, include credit checks. FIS complies with all applicable laws related to background checks, including required notices and applicable consents. FIS will not assign any employee to the provision of the Solution and/or Professional Services if his/her background check findings do not meet the standards established by FIS.

FIS assigns all employees mandatory security and privacy awareness training on an annual basis. FIS requires all employees with access to sensitive information to follow clean desk and clear screen standards to ensure such 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 is suspended upon termination.

3.2.2 Network Security

FIS employs a defensive in-depth model when building networks 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, protocols and services required for FIS to support, secure, monitor and provide the Solution.

FIS uses Network Intrusion Detection and/or Prevention Systems to monitor threats to the FIS environment. Where all, or part of, the Solution is provided using online services (i.e., accessible via the internet), FIS deploys a web application firewall (WAF) and controls designed to protect against distributed denial of service (DDoS) attacks. FIS requires the use of multi-factor authentication for its internal systems and networks. Privileged access to the internal FIS technology environment requires network access control (NAC) which evaluates the security posture of the connecting device.

FIS does not intentionally create back doors or similar programming that could be used to access the Client Data, including Client Confidential Information and Client Personal Data, without Client's permission.

Except as required by applicable law, FIS shall not create or change its business processes with the intention to facilitate access to Client Data, including Client Confidential Information and Client Personal Data, by any government without Client's permission.

FIS may from time to time in its reasonable discretion block attempted access to the Solution from technology of individuals, entities, or governments which FIS reasonably believes may pose a threat to the Solution, 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 the Solution. 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 the Solution, systems and clients. FIS will make information regarding this practice available to Client on the Client Portal or upon request.

3.2.3 System and Services Hardening

In respect of systems operated by or on behalf of FIS, FIS hardens its operating systems in accordance with industry security standards and procedures. FIS hardening standards are based on the Center for Internet Security (CIS) standards, National Institute of Standards and Technology (NIST), and/or Department of Defense (DoD) where applicable. For example, FIS requires that all default passwords are changed, unneeded functionality is disabled or removed, the concept of "least-privileged" access is adhered to, file permissions do not include world writeable ability, administrative or "root" access is limited, where possible, to the management console and those network ports that are necessary to provide the Solution 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.

3.2.4 Access Control

Access to FIS operating systems is limited to those individuals required to support the system including where privileged access is restricted and controlled. 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. Local administrative rights are not permitted on FIS end user computing devices.

3.2.5 Anti-virus, anti-malware, anti-spyware, PC controls

FIS requires that anti-virus, anti-malware, anti-spyware, and event detection and response (EDR) software is enabled on its operating systems at both the server and endpoint levels when they are available and supported by a commercially available solution. FIS PCs and laptops have industry standard controls including disk encryption, access management, whitelisting, anti-virus/anti-malware, and administrative controls.

3.2.6 Applications and Systems Development

Classified as Public - This content can be shared with anyone.

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 the 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 by Design).

3.2.7 Electronic Mail

FIS scans incoming emails, embedded links and attachments prior to allowing them into the FIS environment. FIS also uses industry standard software to control which files are allowed or blocked as attachments to protect against malicious executable files being delivered and/or opened. FIS configures email domains with industry standard anti-phishing technologies such as Sender Policy Framework (SPF) and Domain-based Message Authentication Reporting and Compliance (DMARC).

FIS follows financial services industry commercially reasonable practice to prevent Client Data, including Client Confidential Information and Client Personal Data, from leaving the FIS network, including using a Data Loss Prevention (DLP) solution to block data being sent, stored or copied to an unauthorized service or device.

3.2.8 Vulnerability & Patch Management

FIS employs reasonable efforts to identify and remediate or mitigate vulnerabilities in the Solution in accordance with the FIS Vulnerability Management Standard. This includes weekly network scanning of FIS public internet facing infrastructure and monthly network scanning of FIS non-public internet facing infrastructure. FIS, in its sole discretion, may pause or otherwise modify the scanning schedule to accommodate peak volume periods or resolve performance issues associated with scanning. FIS will perform scanning of FIS developed source code and related libraries for the presence of vulnerabilities in currently supported versions of the Solution. FIS undertakes reasonable efforts to immediately (no more than 14 days) remediate or mitigate critical vulnerabilities upon FIS becoming aware of the vulnerability. A critical vulnerability is defined as a public internet exposed vulnerability which has been validated by FIS as remotely exploitable and has a CVSS score >9. FIS will make reasonable efforts to meet the vulnerability remediation targets defined within FIS' Vulnerability Management Standard. In respect of Solutions not hosted by or on behalf of FIS but covered by ongoing support or maintenance services, FIS will remediate or mitigate by making patches available to the Client for their deployment and handling.

3.2.9 Bug Bounty Program

In respect of Hosted Solutions, FIS maintains a public bug bounty program to encourage responsible disclosure of discovered vulnerabilities in the Solution, which is the "FIS Bug Bounty Program"; participating in the FIS Bug Bounty Program shall be subject to conditions set forth by FIS at its discretion, to be updated from time to time. Subject to Client's participation in the FIS Bug Bounty Program as described at the following link: https://bugcrowd.com/fis, FIS will pay financial "bounties" to clients who identify and report vulnerabilities in accordance with the FIS Bug Bounty Program requirements.

3.2.10 Client Security Testing

FIS permits and encourages Clients to evaluate, test, and monitor the security of the Solution at Client's expense, only as set out below. Any testing not explicitly allowed by this Section is not permitted.

Scanning
Client may perform automated scanning of FIS public internet exposed Solutions. FIS may block or otherwise interfere with Client's scanning activity, as deemed appropriate and necessary by FIS in its sole discretion. FIS will not provide a response to Client's scan results although confirmed exploitable vulnerabilities identified via Client's scanning activity may be submitted to the FIS Bug Bounty Program as outlined in paragraph 3.2.9.

Ethical Hacking
Client may conduct ethical hacking of FIS public internet exposed Solutions subject to the terms of the FIS Bug Bounty Program. Vulnerabilities identified through such tests must be promptly submitted to FIS as documented in the FIS Bug Bounty Program. FIS may block or otherwise interfere with Client ethical hacking, as deemed appropriate and necessary by FIS in its sole discretion. FIS will not be liable for Client's inability to access its product or service as a result of Client's performance of security testing.

3.2.11 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 the FIS Cybersecurity Standard. User authentications (i.e., username and password) are bound to the respective user and may

Classified as Public - This content can be shared with anyone.

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.

3.2.12 Passwords

FIS requires the use of complex passwords. FIS password controls do not allow the previous ten (10) passwords to be used, and current passwords expire at regular intervals. Remote access to FIS systems requires the use of multi-factor authentication. 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.

3.2.13 Data Classification, Retention, and Controls

The FIS Information Classification Policy establishes a framework for classifying data based on its level of sensitivity. FIS aims to protect data from alteration, destruction, disclosure, and unauthorized access in alignment with business, legal, and regulatory requirements by classifying data appropriately.

Client data retention and disposal are to be stipulated in the Agreement to meet business and legal requirements. All FIS employees and vendors with access to Client Data, including Client Confidential Information and 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, including Client Confidential Information and Client Personal Data, in its identifiable state 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 contract or in accordance with applicable laws and thereafter de-identify or delete it in accordance with applicable laws, the Agreement and secure deletion standards.

FIS takes reasonable steps to determine necessary access to Client Data. The 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 Data required to satisfy the user's job responsibilities. Where required, FIS will take adequate steps to keep Client Data relating to different clients or purposes separate.

FIS conducts regular appraisal of user access rights and initiates appropriate measures if any irregularities are detected.

3.2.14 AI Systems

Where FIS develops and/or uses Artificial Intelligence (AI), FIS will use AI in a transparent manner to responsibly and ethically drive innovation while prioritizing and maintaining the security and privacy of relevant parties, all as described in this Section. FIS follows a defined set of principles and a formal approval process in the development and use of AI systems and tools. FIS is committed to developing, maintaining and using AI systems and tools that are designed to:

- comply with applicable laws and regulations, including privacy, data protection, and AI laws;
- preserve the intellectual property rights of FIS and those of third parties;
- process data with a high degree of accuracy, quality, and integrity;
- meet the objectives of the AI system's or tool's intended use while minimizing errors;
- prevent unauthorized access to or use of the AI system or tool;
- provide required notifications and information to users of AI systems and tools regarding its use and oversight to enable the end user to understand and explain the AI system's functioning;
- be controlled and monitored by humans; and
- respect human dignity and personal autonomy, promote equal access, and avoid bias.

FIS shall not use Client Data, including Client Confidential Information and Client Personal Data, to train or operate any AI system that:

- exploits people's vulnerabilities (e.g., age, disability, circumstances);
- deploys subliminal or deceptive techniques to control a person's behavior; or
- uses biometric data to infer sensitive information (e.g., race, religion, political beliefs, sex life).

FIS will regularly review and assess its use of AI and its security controls to ensure ongoing compliance with this Section and industry standard practice.

3.2.15 Encryption

Classified as Public - This content can be shared with anyone.

The FIS Encryption Policy aligns with industry standards. FIS encrypts data at rest and in transit, based on FIS data classification policies and standards. If necessary or in accordance with FIS classification standards, FIS will use encryption key lengths that meet current NIST FIPS 140-2 standards and will only transmit Client Data, including Client Confidential Information and Client Personal Data, over the internet following industry-recognized encryption best practices. Specific algorithm and other minimum key lengths are specified within FIS policy.

This is done in combination with appropriate solutions for key management to mitigate the risk of unauthorized access to the encryption keys. FIS sets requirements for each phase of the lifecycle of cryptographic keys. These include generating, refreshing, storing, making back-ups, archiving, retrieving, transmitting, decommissioning, revoking and destroying keys.

3.2.16 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, 7 days a week, 365 days a year basis. FIS will perform reasonable logging, monitoring, or record keeping of user activity, including but not limited to where applicable administrator access, login attempts, hostnames/IP addresses of connections, date and time of connections where legally permissible and in accordance with applicable FIS information retention standards.

FIS operates a 24/7/365 security operations center which monitors and responds to security threats.

FIS shall securely collect, monitor and retain event logs so access to Confidential Information and systems can be traced. FIS shall provide mutually agreed upon logs to Client upon request. The summary will advise root cause of the incident and the mitigating actions taken to bring the incident to a satisfactory conclusion.

Security logs are retained for at least 365 days. Where technologically feasible, the log files contain at least the registration of user activities (failed log-in attempts or refused attempts to obtain access, violations of authorizations or unauthorized access to data), administrative activities, exceptions and cybersecurity events.

3.2.17 Security and Privacy Incident Response

The FIS Security Incident Response Team (FSIRT) is responsible for investigating and responding to confirmed security incidents impacting FIS technology. FSIRT is staffed 24/7/365 with cyber security response experts and is authorized to take the necessary actions to contain and respond to a cyber security incident. Client may review the FSIRT Security Incident Response Plan, which is available on the Client Portal or upon request. The FSIRT Security Incident Response Plan documents the processes and procedures of FSIRT. If Client becomes aware of a security incident impacting FIS technology and/or Solutions, Client should contact FSIRT at FSIRT@fisglobal.com.

The FIS Privacy Incident Response Team (PIRT) employs a coordinated incident response approach, leading a specialized form of data protection compliance protocols that respond to and investigate privacy incidents. Client may review the FIS Privacy Incident Response Plan, which is available on the Client Portal or upon request. By utilizing a coordinated approach, FIS mitigates, contains, and reduces the potential of any negative impact or risk associated with these incidents. PIRT is responsible for triaging and leading all investigations, as well as verifying documentation and facilitating communication amongst all stakeholders when potential and confirmed privacy incidents are identified. PIRT confirms FIS is timely in its identification, containment, and mitigation of privacy incidents as well as maintaining compliance with all applicable legal requirements. If Client becomes aware of a privacy incident impacting FIS technology and/or Solutions, Client should contact PIRT at PIRT@fisglobal.com.

Should FIS confirm a Data Breach, FIS shall provide Client with notification without undue delay, making all reasonable efforts to provide such notification within 24 hours of FIS confirmation of the described impact to Client Data, including Confidential Information or Client Personal Data. The notification shall summarize, in reasonable detail, to the extent possible and to the extent known, the nature and scope of the Data Breach and if known, the corrective action already taken or planned by FIS. FIS shall promptly take all reasonable and necessary actions to end the Data Breach, mitigate its impact, and prevent recurrence. FIS shall cooperate with Client in the investigation of the Data Breach and shall promptly respond to Client's reasonable inquiries about the Data Breach. FIS shall provide to Client regular updates regarding such Data Breach, and at the conclusion of the investigation, FIS shall provide to Client, to the extent possible and to the extent known, a report detailing the Data Breach, its impact, and the mitigation and/or remediation steps taken by FIS. Based on the nature of the incident, FIS will perform this investigation internally using the FSIRT/PIRT team or with a third-party forensic firm chosen by FIS. Client may request that a third party forensic firm perform a review, at Client's sole expense, and FIS will negotiate in good faith with Client to select a mutually agreeable third party firm and perform the related review.

For the avoidance of doubt, FIS will not give notice of unsuccessful security incidents, including, without limitation, pings and other broadcast attacks on FIS firewall, port scans, unsuccessful log-on attempts, unsuccessful denial of service

Classified as Public - This content can be shared with anyone.

attacks, unsuccessful exploit attempts, and any mix of the above, so long as no such incident results in unauthorized access, use or disclosure of Client Confidential Information.

FIS and Client shall mutually agree upon any external communications that specifically name Client in response to a Data Breach impacting Client systems or Client Data, including Client Confidential Information and Client Personal Data. Nothing in this Section shall prevent FIS from making any notifications or notifying third parties and/or regulators of any incident, cyber-attack, or Data Breach, which may be required under applicable laws, regulations, by such regulator, or in accordance with any client contracts. FIS will not inform any third party of a Data Breach naming Client without first obtaining Client's prior written consent, unless and to the extent FIS is otherwise required to provide notice by law and/or regulator.

FIS shall conduct forensic investigation following a Data Breach when FIS and Client mutually agree it is necessary and conduct any investigations in accordance with legal requirements for preserving evidence. Any forensic investigation will be conducted in a timely manner and will maintain the appropriate chain of custody**.**

3.2.18 Ransomware

FIS has robust controls in place to protect against ransomware. These controls are regularly tested and validated, providing FIS confidence that we have minimized the risk of a ransomware attack. FIS also regularly tests its ability and processes to respond to a ransomware attack. In the event of a ransomware attack, FIS will recover (rebuild) from trusted backups.

3.2.19 Working Remotely

FIS implements the following controls on employees working remotely:

- Working remote means working from a private, reasonably secure location, such as a home, apartment or flat. Working in a public location such as an internet café is not allowed.
- Workers must use FIS-owned and managed laptops that are imaged by FIS and have all of the standard controls including disk encryption, access management, whitelisting, anti-virus/anti-malware, and administrative controls.
- Workers must access FIS networks using multi-factor authentication, network access control, and VPN.
- Navigation of FIS networks must have the same or more stringent controls as from the office, such as the use of hardened intermediary devices to access highly sensitive environments.

In the case where workers are accessing client networks and assets, they must do so based on client connection requirements (for example, virtual desktop infrastructure) and strictly follow client protocols.

4. BUSINESS CONTINUITY AND DISASTER RECOVERY

4.1 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 Solution. Plans are designed to maintain a consistent provision of the Service(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.

4.2 FIS' collection of comprehensive and coordinated Plans are designed to address the agreed crisis response, continuity, and recovery needs for the Service(s), including recovery time objective ("**RTO**") and recovery point objective ("**RPO**"), and will vary based on the application platform. The maximum amount of acceptable data loss, measured in hours or minutes preceding a disruption shall be within the time period specified in the Application Recovery Appendix, available on the Client Portal.

4.3 FIS provides a summary of the GBR program in the Client Portal or upon request. FIS'RTO and RPO for the Solution are as set forth in such summary (or as set forth in the Agreement, with any RTO and RPO in the Agreement prevailing over 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 viability of its Plans at least annually to provide assurance of resilience capabilities as well as the readiness of the Plans' participants. Recovery exercise results are provided via the Client Portal or upon request.

5. PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

For FIS' products that require compliance with the then current version of the Payment Card Industry Data Security Standard ("**PCI DSS**"), FIS will maintain compliance with the then current version of the PCI DSS throughout the term

Classified as Public - This content can be shared with anyone.

of the Agreement and shall make available, via the Client Portal or upon request, evidence of certification of compliance to Client.

6. VENDOR MANAGEMENT

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

6.2 FIS conducts a risk assessment for all third-party suppliers engaged in the provision of the Solution 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, including Client Confidential Information and/or Client Personal Data. FIS only allows such third-party suppliers to access, store, transmit, manage, or process Client Data, including Client Confidential Information and Client Personal Data, to the extent permissible under the Agreement and applicable laws.

6.3 FIS requires its suppliers who process Client Data to agree to data protection agreements to oblige such suppliers to comply with applicable data protection laws. Such suppliers shall, at a minimum, implement appropriate technical and organizational measures to verify a level of security appropriate to the risk. FIS' suppliers must cooperate upon reasonable request in order to assist FIS with its compliance with applicable privacy laws.

6.4 FIS maintains a list of all third-party suppliers with access to Client Personal Data on the Client Portal.

7. DATA MINIMIZATION

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

8. DEFINED TERMS

As used in this Statement, the following terms have the following meaning and all other capitalized terms shall have the meaning as defined in the Agreement:

"**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 Personal Data"** means any Personal Data provided by Client to FIS, or on Client's behalf, for the purpose of FIS providing the Solution(s) to Client pursuant to the Agreement.

"**Client Portal**" means the FIS self-service portal (made available at Client's request) which enables Client's designated representatives to access resources on a variety of topics (such as cybersecurity, data privacy, business continuity and support practices) to help better manage Client's relationship with FIS.

"**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, including Client Personal Data, and the details of Client's computer operations; and (ii) details of the Solution(s).

"**Data Breach**" means a security incident or privacy incident that results in the loss of or unauthorized access to, use or disclosure of Client Data, including Client Confidential Information and Client Personal Data, in FIS possession or control.

"**Personal Data**" is any information relating to an identified or identifiable natural person.

"**Professional Services**" means programming, training, consulting, implementation and other professional services provided by FIS to Client.

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

Classified as Public - This content can be shared with anyone.