Broadridge Information Security Annex

1. **Information Security Program**. Broadridge has in place a comprehensive information security program ("**Information Security Program**") consistent with one, or a combination of: (a) the Control Objectives for Information and Related Technology (COBIT) framework, (b) International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001, (c) various National Institute of Standards and Technology (NIST) standards, (d) NIST Cybersecurity Framework, (e) the Payment Card Industry (PCI) Data Security Standard; (f) The Health Insurance Portability and Accountability Act (HIPAA) or (g) the Health Information Trust Alliance (HITRUST). The Information Security Program includes administrative, technical and physical safeguards to protect against anticipated threats or hazards to the confidentiality, integrity and availability of Client's Confidential Information, including unauthorized use, access or disclosure. The Information Security Program is reviewed and assessed, no less than annually, for changing standards and anticipated threats and hazards. Based upon the results of that assessment, the Information Security Program and standards related thereto will be updated and approved by senior management. Broadridge will permit Client to review the Information Security Program documents and information during Client's Annual Security Assessment (defined below).

2. **Audit Reports and Certifications**. For those services where Broadridge deems it appropriate, Broadridge will engage an independent external auditor to conduct annual reviews of Broadridge's controls against appropriate controls framework, such as SSAE 18 (or its equivalent standard), ISO 27001, PCI, HIPAA or HITRUST, as applicable. Any material deficiencies noted on an assessment or audit will be promptly addressed with the development and implementation of a corrective action plan approved by Broadridge's management. Upon written request, Broadridge will provide an executive summary of such corrective action plan and provide confirmation of remediation to Client. Upon written request and where such external auditor reports exist, Broadridge will provide such reports or certifications to Client.

3. **Security Questionnaires**. To the extent available for a particular Service, up to once annually upon written request, Broadridge will provide to Client a completed BITS Standardized Information Gathering ("**SIG**") questionnaire, or in the case of Services hosted in the cloud, a Consensus Assessment Initiative Questionnaire ("**CAIQ**"). If a SIG or CAIQ is reviewed by Client and Client has reasonable questions or clarifications, Broadridge will use commercially reasonable efforts to reply promptly. Only in the event that a SIG or CAIQ is not available for a particular Service, Client may issue a vendor risk assessment questionnaire to Broadridge in lieu thereof and Broadridge will use commercially reasonable efforts to respond to such questionnaire within 60 days of receipt. If requested by Client and agreed by Broadridge, Broadridge will submit such questionnaire responses via Client's third party portal provider only if (i) Broadridge and such third party have an existing direct contractual relationship or enter into a new direct contractual relationship (which may require facilitation by Client), or (ii) in the absence of such direct contractual relationship, Client agrees or has previously agreed in writing to be fully liable for such third party.

4. **Security Assessments**. Broadridge will permit Client staff (including internal auditors) and/or its authorized representatives (including external auditors and regulators with regulatory jurisdiction over Client) to conduct an annual security assessment ("**Annual Security Assessment**") of the

Information Security Program, which will be limited in scope to those elements of the Information Security Program used to protect the Services. The Annual Security Assessment will occur at mutually agreeable times and shall not exceed two business days (unless otherwise agreed by the parties). Client must provide Broadridge reasonable written notice at least 90 days prior to any requested Annual Security Assessment, which notice must include the proposed agenda and scope, provided that the scope for licensed software will be limited to the software development program (e.g., secure development practices, security testing and vulnerability remediation). The Annual Security Assessment will include meetings with security, risk and technology professionals and a review of documentation, policies, procedures, and other evidence of a mature control environment. Mutually agreed upon control deficiencies identified as a result of an Annual Security Assessment will be remediated or otherwise mitigated by Broadridge on a reasonable schedule in collaboration with Client representatives. Broadridge will reasonably cooperate with Client in the event of any examination by a regulator by making all books, records, documentation, information, and access to personnel related to the Services Client receives available to Client and to the regulator upon reasonable advance written notice to Broadridge. Neither Client nor its representatives will be permitted to conduct security assessments directly on Broadridge's vendors, service providers or subcontractors. Upon request, Broadridge will provide Client with a summary of its assessment of any such third party that has access to Client Confidential Information and will discuss such summary with Client. For the avoidance of doubt, neither Client nor its representatives will be permitted to conduct any testing of Broadridge systems and networks or install any audit software, nor be permitted physical access to any locations where services are performed outside Broadridge owned or managed facilities ("**Broadridge Facilities**").

5. **Background Checks**. Broadridge maintains background check policies and procedures for qualifying employees who are assigned to provide Services for Client. Such policies and procedures include work authorization verification, pre-employment drug testing and background checks of employees' employment history and criminal convictions, all to the extent permitted by applicable law and subject to Broadridge's local background check policy. Upon written request, Broadridge will make a copy of its then-current background check policy available to Client. As part of Broadridge's Third Party Risk Management Program (described below), Broadridge requires that its contractors that have access to Client Confidential Information employ a background check policy consistent with the Broadridge background check policy.

6. **Physical Security**. Broadridge maintains a secure environment in all work areas within Broadridge Facilities where Client Confidential Information is stored or accessed. A secure environment includes 24x7x365 security personnel or equivalent means of monitoring all relevant work areas within Broadridge Facilities and is physically restricted to authorized personnel only. Broadridge provides perimeter controls to detect unauthorized access to work areas within Broadridge Facilities and creates an audit trail of all access attempts, whether granted or refused. Once authorized, any visitor must be escorted by authorized personnel. The process for authorizing and validating access to Broadridge work areas within Broadridge Facilities is set out in Broadridge's Physical Security Policy, which may be reviewed during Client's Annual Security Assessment. Broadridge personnel are required to wear their photo ID badges when inside a work area within a Broadridge Facility and Broadridge provides temporary ID badges to any visitors in a work area within a Broadridge Facility. To the extent Services are performed outside Broadridge Facilities,

certain physical security controls are not applicable. It is Broadridge's policy that personnel must promptly report lost or stolen ID badges, access cards or keys and upon receipt of such report, Broadridge will promptly deactivate the impacted ID badge, access card or key. Broadridge will promptly (within 24 hours) deactivate any ID badge, access card or key of terminated personnel. Broadridge's policy dictates that co-location data centers must maintain physical and environmental security standards consistent with Broadridge standards. Broadridge will assess such locations on a regular basis to confirm compliance.

7. **Client Policies**. While present on site at a Client location, Broadridge personnel will comply with all laws, regulations and Client policies (including without limitation, those involving confidentiality, security measures, health and safety and dress code), to the extent to which each is applicable and has been communicated to such Broadridge personnel, and will act in accordance with commercially reasonable standards for professional etiquette and conduct.

8. **Training**. Broadridge provides regular (no less than annual) education and training regarding information security, confidentiality and non-disclosure duties under the Broadridge Information Security Policy, the Broadridge Global Privacy Policy and Broadridge Acceptable Use Policy (which may be reviewed during Client's Annual Security Assessment) to all Broadridge personnel, as relevant for their job function. In addition, Broadridge provides mandatory training to information security personnel and requires key information security personnel to stay abreast of changing cyber security threats and countermeasures. Broadridge logs and tracks all trainings of Broadridge personnel and certifications of Broadridge information security personnel.

9. **Penetration Testing and Remediation**. Client is prohibited from conducting any penetration testing on Broadridge systems and networks. On an annual basis, Broadridge engages an independent third party to conduct a network penetration test on Internet-facing IP addresses. If applicable and upon written request, Broadridge will provide Client with a high-level summary of the results of such testing including the scope and methodology of the test and confirmation that critical or high risk findings have been remediated, or a plan (including time frame) is in place to remediate.

10. **Application Security Assessment and Remediation**. Client is prohibited from conducting any assessments of Broadridge applications. If agreed in writing by Client, at Client's expense, Broadridge will conduct a continuous application assessment by engaging Broadridge's preferred CREST certified third party. Broadridge will provide Client with a high-level summary of the results of such testing, including the scope and methodology of the test and confirmation that critical or high risk findings have been remediated, or a plan (including time frame) is in place to remediate.

11. **Vulnerability Testing, Software Testing and Patching**. Broadridge performs, either using its own personnel or a third party, monthly network security vulnerability tests against all systems that deliver hosted Services. Upon written request, Broadridge will provide a summary of such test results to Client and will discuss the details of such test results and any related remediation plans with Client. For the avoidance of doubt, Client is prohibited from conducting any vulnerability testing on Broadridge systems and networks. Broadridge will assign a severity rating to vulnerabilities in accordance with the most current version of the Common Vulnerability Scoring System (CVSS), the industry vulnerability scoring standard maintained by the Forum of Incident

Response and Security Teams (FIRST), promptly after each vulnerability becomes verified by Broadridge. Once a vulnerability is assigned a CVSS score, Broadridge will install security patches or take corrective action in accordance with its then current patching and vulnerability management criteria and schedule. As of the date hereof, hosted Services will be remediated or mitigated, and licensed software will be remediated or a workaround provided, in each case in accordance with the following remediation schedule: urgent and critical vulnerabilities (i.e., CVSS score of 10) within 15 days; high risk vulnerabilities (i.e., CVSS score of 7.0 to 9.9) within 45 days; medium vulnerabilities (i.e., CVSS score of 4.0 to 6.9) within 180 days; and low severity vulnerabilities (i.e., CVSS score less than 4.0) at the discretion of Broadridge. Broadridge will permit Clients receiving hosted Services to review its patch and vulnerability management policies during Client's Annual Security Assessment. For licensed software, Broadridge grants Client permission to conduct vulnerability testing of the software and Client shall provide any resulting vulnerability reports to Broadridge, which reports will be considered Broadridge Confidential Information.

12. **Software Programs**. Broadridge maintains secure development practices, based on industry standards (WASC Threat Classification 2.0, OWASP Top 10 or their successors), which are reasonably designed to ensure that all software applications written by or on behalf of Broadridge and utilized by Client are reasonably free of material security defects. At a minimum, all known urgent, critical and high risks will be addressed in accordance with Section 11 (Vulnerability Testing, Software Testing and Patching) before being sent to Client in the case of licensed software, and before being released into production in the case of hosted Services.

13. **Change Management**. Broadridge maintains a mature change management program, approved by senior management. Broadridge will ensure proper separation of duties for request, approval, implementation, backout and audit of changes and will maintain records for 12 months.

14. **Risk Assessments**. Risk assessments are not limited to vulnerability scanning and/or application assessments and will also include enterprise level risk assessments, conducted by the business and reported on to Broadridge senior management and the Board of Directors on no less than an annual basis. Broadridge will maintain a risk registry of such risks. For the avoidance of doubt, the risk registry and risk assessment reports are the property of the Broadridge Board of Directors and will not be shared with any third parties, including Client.

15. **Configuration Management**. Broadridge uses security configuration standards (such as the Center for Internet Security (CIS) Benchmarks) to secure systems that access, store, and process Client data. All build images are tested against the security configuration standards prior to deployment and periodic scans are conducted to detect deviations from the standard.

16. **Data Transmission, Storage and Encryption**. All electronic transmission or exchange of Client data that is being processed by Broadridge on behalf of Client is transmitted via a secure method (such as HTTPS or SFTP) across public networks and Private WAN Connections. "Private WAN Connections" means private telecommunications circuits between Broadridge Facilities but does not include those within Broadridge Facilities or between Broadridge and Client. Broadridge provides industry standard hardware, redundant firewalls, restrictive Internet protocols, strong authentication, and secure network connections between Client and Broadridge. Broadridge

agrees that all Client data that is being processed by Broadridge on behalf of Client will be stored, processed, and physically maintained solely on designated target devices and will be, at a minimum, logically separated from data of other Broadridge clients. Broadridge will encrypt such Client data in a manner that meets or exceeds the NIST guidelines for encrypting data while in motion over public networks or Private WAN Connections. Broadridge also encrypts such Client data stored on any mobile media such as laptops, thumb drives, smartphones and tablets. Broadridge will store such Client data that is backed up in accordance with its designated backup and recovery processes in encrypted form, using a commercially supported encryption solution. Encryption solutions will be deployed in compliance with FIPS 140-2 or its successors.

17. **Broadridge Internal Authentication and Access Controls**. Only authorized personnel approved by Broadridge management will be granted access to Client data that is being processed on behalf of Client. Privileges to access and handle (including printing and emailing) such Client data shall be granted on the principle of "least privilege required" to perform their respective job functions. If Broadridge electronically stores or transmits such Client data, its computers, including any wireless system, will have the following elements: (A) secure user authentication protocols, including: (i) control of user IDs and other identifiers; (ii) a reasonably secure method of assigning and selecting passwords or use of unique identifier technologies such as biometrics or token devices; (iii) control of encryption keys and certificates designed to ensure that such encryption keys and certificates are kept in a location and/or format that does not compromise the security of the data they protect; (iv) restricting access to active users and active user accounts only; and (v) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system; and (B) secure access control measures that: (i) restrict access to records and files containing such Client data only to those Broadridge personnel who need such information to perform the Services; and (ii) assign unique identifications plus passwords (which are not vendor supplied default passwords) that are reasonably designed to maintain the integrity of the security of the access controls to each person with computer access. Broadridge employs the following technical controls when connecting to Broadridge systems and networks remotely: encrypted VPN, multi-factor authentication, desktop firewall and off-network proxy. Broadridge maintains an accurate and up to date list of all personnel who have access to such Client data and will disable a terminated individual's remote and physical access within 24 hours in accordance with Section 6 (Physical Security) and all other access within 15 business days. Broadridge maintains password policies for applications hosted on behalf of Client that comply with NIST SP 800-63 or, at a minimum and where feasible based on the application, complex password format with (i) a minimum of eight characters, (ii) account lockout after three invalid attempts (remaining locked for 30 minutes unless unlocked earlier by an administrator), and (iii) inability to reuse the last five passwords.

18. **Asset Management**. Broadridge maintains an asset management program that includes an asset management policy, which is reviewed and approved by management on an annual basis. An inventory of all Broadridge production assets will be reconciled no less than quarterly. Such reconciliation will be in the form of discovery scans to validate that all assets in scope are accounted for. All assets used to store, process or directly access Client data will be owned or leased by Broadridge. In the case of mobile devices (e.g. smartphones, tablets), Broadridge maintains a Mobile Device Management (MDM) solution to secure Client Confidential Information on all Broadridge-owned mobile devices, which includes, but is not limited to, data

and access isolation, enforced encryption, removal of user ability to change settings as it pertains to the MDM solution, and isolation of all Broadridge applications that could contain any Client or Broadridge Confidential Information. Additionally, all Broadridge mobile devices are remote wipe enabled. BYOD is not permitted by Broadridge and non-Broadridge devices are unable to connect to or access any Broadridge application or network.

19. **Client Authentication**. With respect to access to any technology, products and services of Broadridge or its licensors ("**Broadridge Technology**") where Client controls authentication, including but not limited to a log-in identification and password, federated single sign-on capabilities (SAML), API access and certificate-based authentication protocols, Client shall be solely responsible for the provisioning and de-provisioning (except for those Services where Broadridge is explicitly responsible for provisioning and de-provisioning), distribution, selection, use and safeguarding of all identifying credentials in its control, and for the verification of the identity of each user or machine and its level of authorization to access any Broadridge Technology. Client will use any authentication feature only in accordance with the reasonable instructions established by Broadridge from time to time and communicated in writing to Client. Client will notify Broadridge immediately upon (but no more than 24 hours after) the occurrence of a security incident that compromises any identifying credentials (whether controlled by Client or provided by Broadridge), regardless of whether Client can determine if any credential has been used without authorization. Client shall be responsible and shall hold Broadridge harmless for any unauthorized access to or use of any Broadridge Technology in violation of this Section.

20. **Logging and Monitoring**. Broadridge collects security logs from operating systems, security devices and network devices and stores them in a central location for one year. Access to logs is limited to authorized personnel. Broadridge uses a Managed Security Service Provider (MSSP) that, 24x7x365, reviews the logs, correlates events and reports them to Broadridge's incident response team for investigation. Redacted samples of these logs pertaining to the Services for Client will reasonably be made available to Client for inspection as part of Client's Annual Security Assessment.

21. **Incident Management**. Broadridge maintains security incident management policies and procedures. Broadridge will promptly notify Client in the event Broadridge becomes aware of an actual or reasonably suspected breach of Client Confidential Information or material interference (e.g., a ransomware or DDOS attack) with Broadridge's networks, systems, databases, servers or electronic or other media on which Client Confidential Information is processed or stored (a "**Security Breach**"). Broadridge will investigate the Security Breach and, in its sole discretion, may leverage reputable third party firms to perform forensic examinations and provide other support and may also engage law enforcement. "Prompt", for the purposes of this paragraph, means soon after the event is identified and associated with information belonging to Client without impacting the necessary actions needed to contain and mitigate the continuation of the event; under most circumstances this will not exceed 24 hours.

22. **Broadridge Managed Cloud**. Broadridge provides certain of its Services within a public cloud environment that is Cloud Security Alliance (CSA) STAR certified or equivalent. Broadridge will leverage cloud capabilities provided and/or managed by third parties such as Amazon Web Services, or other reputable cloud providers. Broadridge maintains a program to actively manage

its cloud providers and assess how they secure and protect the information and data that Broadridge stores and processes in their respective clouds, including obtaining and reviewing each provider's most current applicable SOC report(s). To the extent applicable to any Services provided to Client, Broadridge will make such SOC report(s) available to Client, which may require Client to open an account with such cloud provider to view or request such report(s) directly.

23. **Data Destruction**. Client Confidential Information that is no longer required by Broadridge to perform under this Agreement will be securely erased or destroyed in such a manner that such Confidential Information is rendered unrecoverable, except for any copies reasonably required to maintain Broadridge's customary archives or computer back-up procedures and as otherwise required by applicable law, rule or regulation. As part of such requirement, any data processing equipment that is surplus to Broadridge's requirements and has held Client's Confidential Information (e.g. computer hard drives, photocopy machines) may only be re-used or disposed of following the secure erasure or destruction of all such Confidential Information, and where this occurs, it will be evidenced in writing. Broadridge shreds all paper waste in compliance with National Association of Information Destruction (NAID) standards and disposes of it in a secure and confidential manner to render all paper waste unreadable and non-recoverable.

24. **No Disabling Devices**. Broadridge installs, maintains, and runs up to date antivirus and anti-malware detection and eradication software at a minimum on all Windows and Linux-based systems, and performs antivirus and anti-malware signature updates not less than daily (to the extent a daily update is available from the applicable vendor). Provided that Client installs, maintains and runs up to date antivirus and anti-malware detection and eradication software and performs antivirus and anti-malware signature updates not less than daily (to the extent a daily update is available from the applicable vendor), Broadridge represents that Disabling Devices (defined below) are not contained within: (a) any electronically delivered Services, (b) any Broadridge website by which Client will access the Services, (c) any reports or other data furnished to Client, or (d) any Broadridge software delivered to Client (collectively, the "**Broadridge Electronic Services**"). "**Disabling Device**" means a program, routine, device, code, or instructions or other undisclosed feature, including, without limitation, a time bomb, virus, software lock, drop-dead device, malicious logic, worm, Trojan horse, spyware, or trap door, that is capable of (or has the effect of allowing any untrusted party or malicious user to be capable of) accessing, modifying, deleting, damaging, disabling, deactivating, interfering with, or otherwise harming the Broadridge Electronic Services or licensed software (as applicable) or Client's computers, networks, data, or other electronically stored information, or computer programs or systems, excluding in all cases any "0 day" vulnerabilities (i.e., a vulnerability within any third party software, operating system or network component that has not been released to the general public nor could be discovered by commercially reasonable due diligence by Broadridge).

25. **Business Continuity Plan**. Broadridge maintains a business continuity plan (the "**BCP**") and implements the BCP in the event of any unplanned interruption of the Services. The BCP includes the pre-arranged recovery strategy of people, process and technology to continue mission critical functions until Services are restored. The BCP includes, but is broader than, the Disaster Recovery Plan, which includes activities and plans to restore the ongoing function of technology and infrastructure in the event of a disaster. Broadridge tests, reviews, and updates the BCP on at least an annual basis. Upon written request, Broadridge will provide Client with executive

summaries of all such updates and tests and, for those hosted Services that include disaster recovery, testing of the Disaster Recovery Plan. A current summary of each of the Business Continuity Program and the Technology Disaster Recovery Global Program can be found at https://www.broadridge.com/about/sustainability/business-continuity-planning.

26. **Third Party Risk Management Program**. Broadridge maintains an assessment program designed to validate that its third party vendors or service providers that have access to Client Confidential Information have a security program and control environment designed to protect Client Confidential Information. Client may review Broadridge's third party risk management program during Client's Annual Security Assessment.

27. **Broadridge India**. Broadridge performs certain functions of its Services through an affiliate and wholly owned subsidiary of Broadridge's parent located in India ("**Broadridge India**"). Broadridge India personnel may access Client Confidential Information in connection with the Services from Broadridge India locations or via secure remote access, but Client Confidential Information will not be stored in India. Broadridge India employees undergo a background check in accordance with Section 5 (Background Checks).

28. **Data Center Facilities**. Broadridge utilizes third party data center facilities to provide the Services. Personnel from these data centers do not have access to Broadridge systems or data. With respect to such provision of Services, Broadridge operates in compliance with data protection and privacy laws of the country where the data center is located.

29. **Kyndryl Facilities**. Broadridge utilizes Kyndryl Holdings, Inc. to provide technical and operational support of systems running in U.S., Canada and Europe based data centers. Kyndryl personnel operate under a set of security controls developed jointly by Broadridge and Kyndryl and administered by Broadridge, which may be reviewed during Client's Annual Security Assessment.

30. **Security Tools and Technology**. Broadridge employs security tools and technology such as firewalls (including DMZ implementation) and prohibits system administrative functions through direct remote internet access to any such tools and technology. Broadridge configures all security devices with a default deny-all policy. Firewall rules are audited on a periodic basis, but no less than annually, in compliance with applicable standards. Broadridge maintains intrusion detection/prevention systems, DDOS mitigation solutions at the internet perimeter, personnel and other resources to ascertain if a penetration attempt is being made against any part of Broadridge's network, mainframe, server or other infrastructure or facilities used by Broadridge to process, store or transport Client Confidential Information. Broadridge maintains secure VPNs and network admission control to protect remote access and validate that only Broadridge managed assets connect to our networks.

31. **Data Loss Prevention (DLP)**. Broadridge employs tools and has policies, standards, and processes that are designed to prevent unauthorized access, or disclosure of Client Confidential Information from systems that access, process or store such data. Broadridge employs DLP perimeter technology, deployed at the e-mail gateways and web proxies, based on pattern matching.

32. **Applicability to Licensed Software**. For Clients receiving licensed software only, this attachment does not apply, except for the following Sections: Security Questionnaires, Background Checks, Client Policies, Training, Change Management, Business Continuity Plan, Third Party Risk Management Program and as specified in the following Sections: Security Assessments, Vulnerability Testing, Software Testing and Patching, Software Programs and No Disabling Devices.