Broadridge

Overview of Information Security and Global Privacy Programs

Ready for Next

Table of Contents

Information Security Mission and Strategy 2

Scope of Information Security Policy 3

Program Structure and Framework 3

Governance 4

Certifications and External Audits 5

Security Incident Response 6

Awareness, Training, and Engagement 6

Global Privacy Program and Policy 7

Records Retention 7

Last Revised: October 5, 2021

Information Security Mission and Strategy

Broadridge Financial Solutions, Inc. ("Broadridge" or the "Company") has a responsibility to protect all information with which it is entrusted and have an effective information security program. The security of the information created, processed and used by Broadridge as well as non-public client confidential information entrusted to Broadridge by its clients are among the Company's most important responsibilities. As a business, Broadridge must take the necessary steps to protect the confidentiality, integrity and availability of this information.

The purpose of Broadridge's Information Security Program (the "Program") is to manage Broadridge's information security efforts including securing our facilities and data centers, educating our associates and most importantly, protecting our clients' confidential information. The Program covers various facets, starting with the governance of the Program, and includes:

- Implementing appropriate technologies and processes
- Regularly monitoring and addressing threats and vulnerabilities
- Enhancing and expanding security initiatives
- Preparing and regular testing of response measures
- Ongoing training of our associates

In order to achieve these objectives, Broadridge employs the following:

- A layered defense approach to controls.
- A strategic and standards based approach to information technology risk management to aid decision-making, enhance outcomes, and increase accountability.
- A risk management approach to facilitate the identification of potential risks, implementation of approved controls, and integration of risk management processes with other planning processes and activities.

Scope of Information Security Policy

All personnel (Broadridge associates, majority owned ventures, contractors, consultants, and temporary employees) and organizations that are owned or managed by Broadridge as well as any external business partners and vendors that have access to Broadridge systems and information or processes information through or on behalf of Broadridge are required to comply with Broadridge's Information Security Policy.

Program Structure and Framework

Broadridge's Information Security Group ("BISG") is responsible for establishing, maintaining and monitoring the Program for Broadridge. This involves the creation, administration, and communication of policies and standards to ensure that correct controls are in place.

The Program has been designed to address the following:

- **Risk Assessment** - Identify/assess operational and application risks/vulnerabilities and propose recommendations for management through the utilization of appropriate information security controls.
- **Security Incidents** – Respond to any anticipated and actual threats and hazards to information resources.
- **Data Loss Prevention** - Establish controls to prevent loss or compromise of information resources.
- **Training and Awareness** - Promote information security awareness within the organization.
- **Entitlements Management** - Provide guidance on user and system access to ensure appropriateness for business functions.
- **Risk and Compliance** - Leverage control frameworks, including but not limited to, The International Organization for Standardization ("ISO"), Health Insurance Portability and Accountability Act ("HIPAA"), Payment Card Industry ("PCI"), National Institute of Standards and Technology ("NIST"), Statement on Standards for Attestation Engagements No. 18 ("SSAE-18"), gather evidence, and report to management the state of compliance with

information security frameworks relating to appropriate areas within the business.

- **Governance** - Govern the processes to ensure the proper management of information security controls that protect the Company's and clients' information.

Where applicable, the components of the Program are aligned with the following industry Standards/Frameworks:

- ISO27001:2013 - Information Security Management System requirements
- NIST - National Institute of Standards and Technology Information Security Handbook - Cyber Security Framework
- CSA CCM - Cloud Security Alliance's Cloud Controls Matrix
- PCI-Data Security Standard - Payment Card Industry Data Security Standard
- HIPAA
- HITRUST Common Security Framework ("HITRUST CSF")
- Federal Information Security Modernization Act of 2002 ("FISMA")

Governance

The Company's Information Security Management System ("ISMS") is part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The Chief Security Officer ("CSO") is responsible for overseeing the development, implementation, and maintenance of the ISMS. The Program is managed by the BISG and the Business Information Security Officers ("BISOs"). The BISG is responsible for maintaining security related metrics and information aligned to the Program and reporting to executive management and key stakeholders.

The BISG is responsible for providing bi-annual reporting to Broadridge's Risk Committee (the "Risk Committee"), which is comprised of members of executive management and other key stakeholders. The CSO and Chief Privacy Officer are members of the Risk Committee and the Company's Cybersecurity Council.

Management provides reports on its cybersecurity program to the Audit Committee of Broadridge's board of directors (the "Board") on a regular basis, including a quarterly report on the Program by an independent third-party cybersecurity services and consulting firm, and the full Board on an annual basis. Also, third-party cybersecurity experts present to the full Board on an annual basis. In addition, the Cybersecurity Council provides a summary of its activities to the full Board.

The Program also leverages external security ratings from BitSight for enhanced visibility to security risks.

Certifications and External Audits

Broadridge is audited or assessed for compliance with information security policy requirements on a frequency based on criticality of the business or product or where required by external audits. Audits or assessments in connection with ISO 27001, SSAE-18, Sarbanes-Oxley Act of 2002, Gramm-Leach Bliley Act ("GLBA")-Standards for Safeguarding Customer Information (Federal Trade Commission Safeguards), CSA, HIPAA, PCI-Data Security Standard, HITRUST, FISMA (NIST SP800-53) and other similar certificates are based on certification and regulatory requirements.

- Certain of Broadridge's products and services are examined at least annually against the SSAE-18 Service Organization Controls ("SOC") reporting standard by independent third-party auditors. These examinations cover controls for data security as applicable to in-scope trust service criteria for each service. Broadridge receives SOC 1 Type 2 and SOC 2 Type 2 reports covering these products and services.

- ISO 27001 assessments are conducted on an annual basis following the procedures laid out in the Security Compliance Assessment Process Procedure Manual

- CSA STAR Level 2 Certification (Cloud Security Alliance Security Trust Assurance and Risk)

- PCI-Data Security Standard Annual Certification

- HITRUST CSF Certification

- FISMA (NIST SP800-53) Certification

Security Incident Response

Our Security Incident Response ("SIRT") is the process of detecting, evaluating, and minimizing impact from internal or external events that put Broadridge assets at risk. Our SIRT plan is designed to efficiently manage security incidents in a manner that will effectively limit the risk to Broadridge and third party assets. Should our established safeguards (e.g., access controls, firewalls, and encryption) be circumvented, we rely on an effective SIRT program to quickly identify any compromises to our security posture, effectively restore system and data integrity, and meet legal and regulatory obligations.

In addition to our internal capabilities, we also leverage an external Managed Security Services Provider for enhanced threat monitoring and correlation.

Following NIST, our SIRT protocol includes seven key elements:

- Preparation
- Detection and Reporting
- Assessment
- Containment
- Eradication
- Recovery
- Postmortem Activity and Analysis (Lessons Learned)

Awareness, Training, and Engagement

The BISG in coordination with Broadridge's Human Resources department, makes available Information Security Awareness training materials for all Broadridge associates. All Broadridge associates are required to complete mandatory Information Security Awareness training offered by the BISG at least annually.

Non-compliance to the training and awareness requirement will result in escalation to an associate's management.

Employees have access to a library of information technology security knowledge and techniques including a dedicated intranet site and access to multiple online learning portals.

We also conduct quarterly phishing simulations and provide a phish alert report button for our associates to readily report suspicious emails for appropriate analysis and follow up.

Global Privacy Program and Policy

Broadridge is committed to respecting privacy. Our Global Privacy Program is designed to help ensure that we handle personal information appropriately and is intended to drive a consistent approach to privacy protection across Broadridge. The Global Privacy Policy specifies policy objectives for the collection, use, maintenance, security and disclosure of personal information by Broadridge. A copy of the Global Privacy Policy is available at broadridge-ir.com/governance/governance-documents.

Privacy is the responsibility of everyone at Broadridge. Senior management recognizes the importance of strong data privacy governance, and in particular data privacy and privacy compliance practices. Privacy governance within Broadridge is generally overseen by the CPO under the supervision of the Chief Legal Officer. Additionally, Broadridge's Data Use and Governance Committee reviews all new proposed uses of data, including personal information, to ensure compliance with the Global Privacy Program.

Broadridge's policies, in general, have been designed to either meet or exceed the regulatory requirements and standards set out within certain regulations, including for example, information security rules under GLBA and 201 Code of Massachusetts Regulation 17: Standards for the protection of personal information of residents of the Commonwealth.

For more information see broadridge.com/legal/privacy-statement-english.

Records Retention

Broadridge's records management program is intended for use by the Company, its subsidiaries, operating divisions, and staff departments and relates to all types of records, regardless of the media. All employees and independent contractors who create and use records and information are responsible for maintaining the Company's records according to Broadridge's Records Management Policy. Broadridge's Document Control and Records Management Procedure ("Records Procedure") implements such policy and applies to all electronic and non-electronic documents and data (both internal and external) required for the effective functioning of the ISMS. All records must be maintained in accordance with the requirements set forth in Broadridge's Records Management Policy.

Below are some aspects of the Records Management Policy and Records Procedure:

- All required documents generated by the Company will be identified with a title/name, contain a document and revision history, and require approvals

- The Company shall maintain Records Retention Schedules listing categories of records and the period for which the records must be retained

- Documents are required to be reviewed periodically, at a minimum annually, to ensure they remain accurate and will be updated as appropriate

- Any document, data, or information that does not constitute a record of the Company and the following documents, data, and information, generally, need not be retained once they serve their purpose and should be destroyed within 45 days of creation

- When the specified retention period ends, and after obtaining any necessary approvals, for any Company records should be disposed of or destroyed by means appropriate to their nature or level of confidentiality (e.g., shredding, recycling, deleting)

- Company employees are expected to regularly destroy convenience copies of records, drafts, duplicate copies of records, and transitory records

Our Record Management Governance Committee, which include members of the Legal Department and Compliance, meets at least annually. The responsibilities of this committee include, but are not be limited to, reviewing and modifying as appropriate the record management policies and procedures.

Any employee who becomes aware of a violation of the Records Management Policy or any other Company policy should promptly report any such violations to the Chief Legal Officer or other appropriate personnel. Reporting can also be carried out through the Ethics Hotline at ethics@broadridge.com or 1-800-669-0661.