Information Security
Suggested Best Practices

Transmission of Data

As a leading practice, sensitive data including: client, regulatory, or Personally Identifiable Information (PII), should be sent to Broadridge using a secure transmission method in order to protect the confidentiality and integrity of the data. Broadridge supports and encourages the use of secure data transmission methods between our clients systems and Broadridge systems (system to system) using available encryption protocols including, but not limited to: SFTP, FTPS (Secure File Transfer Protocol), PGP (Pretty Good Privacy), and NDM Secure + (IBM Connect Direct).

Email Encryption

Client sensitive information (Personally Identifiable Information-PII) should always be sent to Broadridge in an encrypted fashion to protect your proprietary information. Within the financial service industry, client sensitive information may include one or more of the following items:

1. National Identification number (i.e. Social Security #)
2. Shareholder first and last name
3. Shareholder complete address
4. Financial Account # or banking information
5. Shareholder email address
6. Shareholder telephone number
7. Vote instructions
8. Security Login IDs / Passwords
9. ePHI (medical for the HIPAA certified groups)
10. PCI-DSS (credit card information)
11. Other types of client sensitive Information

Broadridge strongly encourages all of our clients to submit their sensitive information to us in an encrypted fashion via Enforced TLS (Transport Layer Security) Encryption, a secured facility for sending email communications over the internet. If you have any questions on how to process or submit your client sensitive files to us via Enforced TLS Encryption or any other services, please contact your Broadridge Client Service Representative for assistance.

Clients should also consult their Information Security group before sending client sensitive information outside of their organization to Broadridge or to any other destination.

Data Security

Data security is a high priority at Broadridge. As we expand the technology in which we interface with our clients in sharing sensitive information or providing access to Broadridge systems, we have implemented a practice whereby we actively manage our data security interfaces. To further enhance our security controls, we ask that you designate a Data Security Administrator (DSA) to provide a technical relationship between your team and Broadridge. This will create a single channel to communicate all requests for systems/security access and file interfaces.

Information Security
Suggested Best Practices

Here are some recommended securities guidelines for your DSA:

- Submit access requests such as new user account creation, password resets, removal of Administrative suspends and terminations of users via email through your designated Broadridge Client Service Representative.
- Requests to terminate users having access to any Broadridge application are to be sent to your Broadridge Client Service Representative as soon as possible to deactivate their user IDs. This includes: ICS Online, MyService.broadridge.com, Campaign Manager, ICS Online Banks & Brokers, Proxy Edge, Post Edge, etc.
- Regularly, advise users with access to Broadridge applications that sharing of user IDs and passwords is not permitted. In the event the DSA is not available, the client should communicate contact information for a designated backup to Broadridge.
- Periodic review and recertification of users' access and entitlements is strongly recommended at a minimum quarterly.

ISO 27001:2013 Statement

The best measure of Broadridge's commitment to Information Security is our continued registration as an ISO 27001 certified company. ISO 27001- 2013 is an internationally recognized Information Security management standard that requires a company to maintain an Information Security Management System (ISMS) framework based on the ISO 27001:2013 standard.

In order to achieve registration as an ISO 27001 compliant company, Broadridge had to pass a rigorous certification audit by a third party registrar. Our current certification covers our ICS Proxy Services, Transfer Agency, Proxy Mailing, Proxy Voting and Tabulation Core Proxy Suite. Specific applications/processes include Proxy Vote, Telephone Proxy Voting, Proxy Edge, Global Proxy, Virtual Shareholder Meetings, ICS Online Banks & Brokers, Campaign Manager, ShareLink, Proxy Vote Processing and Vote Return Scanning, Advisor Mailbox, Investor Mailbox, Post Sale Suite of products, Post Edge, Mutual Fund Proxy Services, etc.

This International Standard preserves the confidentiality, integrity and availability of information within associated processes and applications. The information security controls and risk management processes give confidence and assurance to our clients and interested parties that risks are adequately managed.

Each certification is good for three years and requires a full re-certification audit and periodic surveillance audits from an accredited third party auditor to maintain certification. Since our initial certification in August 2008, ICS has passed all certification and surveillance audits. Our most recent re-certification was issued in June 2014 with a surveillance audit in Sept 2015. Our annual re-certification began in December 2016.