Stretto Security Requirements Policy
Version 2022.1

The security requirements included in this document represent the minimum security requirements acceptable to Stretto, Inc. ("STRETTO") and are intended to ensure that any third party individual or organization engaging with STRETTO as an end user ("End User") has appropriate controls in place to protect information and systems, including any information the End User receives, processes, transfers, transmits, stores, delivers, and/or otherwise accesses on account of its business relationship with STRETTO.

End User hereby agrees to comply with the Stretto Security Requirements Policy. It is the End User's responsibility to implement these controls and to obtain the assistance of an outside service provider if needed. STRETTO reserves the right to make changes to these security requirements without prior notification and to post the most current version to its web site at www.stretto.com/legal-policies.

DEFINITIONS

"Consumer Data" means Experian Information, data from other credit bureaus and credit reporting agencies and consumer information from other sources contained in products and services sold by STRETTO.

"End User" means any third party customer which receives, processes, transfers, transmits, stores, delivers, and/or otherwise accesses Consumer Data through STRETTO's products or services.

"Experian Information" means Experian highly sensitive information including, by way of example and not limitation, data, databases, application software, software documentation, supporting process documents, operation process and procedures documentation, test plans, test cases, test scenarios, cyber incident reports, consumer information, financial records, employee records, and information about potential acquisitions, and such other information that is similar in nature or as mutually agreed in writing, the disclosure, alteration or destruction of which would cause serious damage to Experian's reputation, valuation, and / or provide a competitive disadvantage to Experian.

"Resource" means all systems and devices an End User uses to access, transmit, process, deliver or store Consumer Data, including but not limited to laptops, PCs, routers, servers, and other computer systems.

1. Information Security Policies and Governance

End User shall have Information Security policies and procedures in place that are consistent with the practices described in an industry standard, such as ISO 27002 and / or this Security Requirements policy, which is aligned to both STRETTO's and Experian's Information Security policies.

2. Vulnerability Management

Firewalls, routers, servers, PCs, and all other Resources managed by End User (including physical, on premise or cloud hosted infrastructure) will be kept current with appropriate security specific system patches. End User will perform regular penetration tests to further assess the security of systems and resources. End User will use end-point computer malware detection / scanning services and procedures.

3. Logging and Monitoring

Logging mechanisms will be in place sufficient to identify security incidents, establish individual accountability, and reconstruct events. Audit logs will be retained in a protected state (i.e., encrypted, or locked) with a process for periodic review.

4. Network Security

End User will use security measures, including anti-virus software, to protect communications systems and networks device to reduce the risk of infiltration, hacking, access penetration by, or exposure to, an unauthorized third-party.

5. Data Security

End User will use security measures, including encryption, to protect Consumer Data in storage and in transit to reduce the risk of exposure to unauthorized parties.

6. Remote Access Connection Authorization

All remote access connections to End User internal networks and / or computer systems will require authorization with access control at the point of entry using multi-factor authentication. Such access will use secure channels, such as a Virtual Private Network (VPN).

7. Incident Response

Processes and procedures will be established for responding to security violations and unusual or suspicious events and incidents. End User will report actual or suspected security violations or incidents that may affect Consumer Data to STRETTO within twenty-four (24) hours of End User's confirmation of such violation or incident.

8. Identification, Authentication and Authorization

End User will require each user of any Resource to have a uniquely assigned user ID to enable individual authentication and accountability. Access to privileged accounts will be restricted to those people who administer the Resource and individual accountability will be maintained. All default passwords (such as those from hardware or software vendors) will be changed immediately upon receipt.

9. User Passwords and Accounts

All passwords will remain confidential and use 'strong' passwords that expire after a maximum of 90 calendar days. Accounts will automatically lockout after five (5) consecutive failed login attempts.

10. Training and Awareness

End User shall require all End User personnel to participate in information security training and awareness sessions at least annually and establish proof of learning for all personnel.

11. Experian's Right to Audit

End User shall be subject to remote and / or onsite assessments of its information security controls and compliance with these Security Requirements.

12. Bulk Email Communications into Experian

End User will not "bulk email" communications to multiple STRETTO employees without the prior written approval of STRETTO. End User shall seek authorization via their STRETTO account manager in advance of any such campaign.