SafeRent Solutions Access Security Requirements

The security requirements included in this document represent the minimum security requirements acceptable to SafeRent Solutions and are intended to ensure that an End User (i.e., any other organisation engaging with SafeRent Solutions) has appropriate controls in place to protect information and systems, including any information that it receives, processes, transfers, transmits, stores, delivers, and / or otherwise accesses on behalf of SafeRent Solutions.

DEFINITIONS

"Reseller Information" means SafeRent Solutions highly sensitive information whether property of SafeRent Solutions or another consumer reporting agency (e.g., Experian) and provided to End User, includes, 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 SafeRent Solutions' reputation, valuation, and / or provide a competitive disadvantage to Reseller or upstream consumer reporting agencies.

"Resource" means all End User devices, including but not limited to laptops, PCs, routers, servers, and other computer systems that store, process, transfer, transmit, deliver, or otherwise access the Reseller Information.

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 document.

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 unauthorised third-party.

5. Data Security

Third Party will use security measures, including encryption, to protect SafeRent Solutions provided data in storage and in transit to reduce the risk of exposure to unauthorised parties.

6. Remote Access Connection Authorisation

All remote access connections to End User internal networks and / or computer systems will require authorisation 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 SafeRent Solutions to SafeRent Solutions within twenty-four (24) hours of End User's confirmation of such violation or incident.

8.   Identification, Authentication and Authorisation
Each user of any Resource will 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. SafeRent Solutions' 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.