Experian Client Security Requirements

The security requirements included in this document represent the minimum security requirements acceptable to Experian and are intended to ensure that a Client has appropriate controls in place to protect information and systems, including any information that it receives from Experian.

DEFINITIONS

"Experian Information" means Experian 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 Client managed information technology, systems, devices and applications that store, process, transfer, transmit or access Experian Information or are otherwise concerned with the contracted services from Experian.

1. Information Security Policies and Governance

The Client shall have, maintain and disseminate information security policies, standards and procedures relevant to their operating environment and ensure they are reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

2. Training and Awareness

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

3. Personnel Security

The Client shall manage Personnel security risk by screening individuals to a level commensurate with their intended role, prior to employment and authorizing access.

4. Identity and Access Management

Client shall proactively manage individual, group, system and application login accounts, ensuring a formal registration governs the creation of all accounts and assignment of access permissions. Privileged accounts shall be restricted to defined personnel or roles. All accounts, privileges and access permissions shall be periodically reviewed, validated and amended where necessary.

The Client shall define complexity, length and lifespan requirements to ensure strong criteria for password-based authentication and consistently implement the requirements across systems and applications. Multi-Factor Authentication (MFA) shall be used for access to networks, resources and privileged access scenarios based on organizationally defined requirements.

5. Vulnerability Management

Technical vulnerabilities shall be consistently identified, prioritised, tracked and remediated in all resources, systems, infrastructure and both hosted and developed applications. Proactive software patching shall be conducted to a defined schedule. Any externally (internet) facing resources and/or applications concerned with the contracted services from Experian, shall be tested at least annually by way of penetration or web-application security test.

6. Endpoint Security (Desktop PC's, Laptops)

Endpoint devices shall be managed to ensure consistent security configuration and only allowing authorised software to be installed. Anti-malware technologies shall be utilised to detect and eradicate malicious code on endpoint devices.

7. Cryptography

Cryptographic measures shall be used to protect the confidentiality of Experian Data in storage and in transit to prevent unauthorized disclosure.

8. Network Security

Client shall design and implement firewall and router configurations between untrusted and trusted networks based on the principle of least permissions and review at least annually. All remote access to resources and information assets shall be through managed network access control points.

9. Logging and Monitoring

Requirements for logging and monitoring shall be defined, prioritising monitoring of assets based on criticality and the sensitivity of the data they store and process. Event logs and alerts shall be reviewed on an ongoing basis and inappropriate or unusual activities that have actual or potential security incident implications shall be escalated in accordance with established timelines and procedures.

10. Security Incident Management

Processes to facilitate a response to potential or actual security-related incidents and data breaches shall be defined and tested periodically to ensure the continuation of business operations. Timely and relevant reports shall be provided to Experian of incidents effecting Experian.

11. Management of Change

Changes to any systems, applications and infrastructure shall be authorized, planned, approved, tested and evaluated following a defined process or procedure. Operational privileges for implementing change shall be restricted to authorised Personnel.

12. Experian’s Right to Audit

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

13. Bulk Email Communications into Experian

Client will not send “bulk email” communications to multiple Experian employees without the prior written approval of Experian. Client shall seek authorisation via their Experian Relationship Owner in advance of any such campaign.