Experian Security Requirements

The security requirements included in this document represent the minimum security requirements acceptable to Experian and are intended to ensure that a Third Party (i.e., Supplier, Reseller, Service Provider or any other organisation engaging with Experian) 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 Experian.

DEFINITIONS

“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, where the disclosure, alteration or destruction thereof would cause serious damage to Experian’s reputation, valuation, and/or provide a competitive disadvantage to Experian.

“Experian Data” means all information created, held, used or otherwise processed by or on behalf of Experian, of any nature and in any form regardless of physical or electronic location. The term data is used interchangeably with the term information.

“Resource” means all Third Party devices, including but not limited to laptops, PCs, mobile devices, routers, servers, and other computer systems that store, process, transfer, transmit, deliver or otherwise access the Experian Information.

1. Information Security Policies and Governance

The Third Party shall maintain and disseminate information security policies, standards and procedures relevant to their operating environment and ensure that they are reviewed regularly and after significant changes to ensure effectiveness.

2. Training and Awareness

Third Party shall implement a security training program that defines security responsibilities, provides role-based training as needed, and requires annual confirmation of understanding and acceptance from all personnel. Training attendance shall be recorded.

3. Risk Management

The Third Party shall use a formal process to manage risk and shall conduct an annual assessment to identify and manage internal and external risks relevant to the organisational operating environment and information assets.

4. Acceptable Use

Acceptable and unacceptable rules of behaviour for the use of technologies shall be set, enforced, supported, and communicated to all personnel, including the consequences for unacceptable behaviour.

5. Personnel Security

The Third Party shall manage personnel security risk by screening individuals to a level commensurate with their intended role prior to employment and authorising access.

6. Access Control Management

Third Party shall proactively secure user access by requiring strong passwords, risk-based authentication, session management controls and manage a formal process for user access, including registration, recertification, and revocation, to ensure that only authorised individuals have access to appropriate data.

Third Party shall define and implement appropriate and effective Multi-Factor Authentication (MFA) requirements for access to networks, resources, and privileged access scenarios, based on the organisation’s defined protection requirements.

7. IT/Systems Security

Third Party shall protect end-user devices from web and email based threats by enforcing secure browser settings and email security controls.

8. Vulnerability Management

Third Party shall scan all applications and assets (internal and external) to identify vulnerabilities, cloud account misconfigurations and unnecessary open ports. Proactive software patching shall be conducted to a defined schedule from known trusted sources.

Any externally (internet) facing resources and/or applications involved in the delivery of services to Experian shall be tested at least annually by way of penetration test, in addition for all new applications and following any significant change.

9. Network Security

Third Party shall configure all firewall policies to deny all network connections by default and only permit explicitly approved connections. Approved connections must follow the principle of least privilege and have documented business justification.

Internet-facing applications involved in delivering services to Experian shall be protected against common web exploits through a Web Application Firewall operating in blocking mode or equivalent continuous application security measures.

10. Data Security

Third Party shall define, maintain and implement Data Loss Prevention (DLP) policies and controls to protect sensitive data from unauthorized access, use, or transmission.

11. Endpoint Security

Third Party shall install anti-malware software on all servers and end-user endpoint devices. Anti-malware software, signatures, and threat analysis engines shall be automatically updated from a trusted source. Third Party shall encrypt all end-user devices at the disk level and control removable media by requiring management approval for use and enforcing encryption.

12. Cryptography

Third Party shall encrypt all structured and unstructured Experian data at rest using AES 256-bit encryption and shall enforce encryption in transit using approved protocols, ensuring at least TLS 1.2, HTTPS, and SFTP are implemented.

13. Security Logging and Monitoring

The Third Party shall implement and review logging and monitoring to detect and respond to malicious activity.

14. Incident Management

Third Party shall establish and maintain an incident response plan with defined roles, responsibilities, and compliance requirements and be tested periodically to ensure the continuation of business operations. Timely and relevant reports (within 24 hours) shall be provided to Experian of incidents effecting Experian.

15. Physical Security

Third Party shall protect areas containing critical infrastructure or IT equipment using an access control system with role-based privileges to prevent and detect unauthorized access.

16. Management of Change

Changes to any systems, applications and infrastructure shall be authorised, planned, approved, tested and evaluated following a defined process or procedure.

17. Security Assessments

Third Party shall be subject to security assessments of their information security controls and compliance with these Security Requirements. Assessment shall be no more frequent than once every 12 months or in the event of a security incidence affecting Experian.