Supplier Information Security

Experian values its professional relationships with its suppliers and is committed to conducting business with companies that make Information Security the number one priority. Here at Experian, we ensure “Security First In Everything We Do…”, Experian therefore anticipates that all suppliers will meet Experian’s Supplier Security Requirements.

As part of the onboarding process and during the lifecycle of the contract, Experian will work with you to establish that you meet the appropriate level of Information Security required for the services you provide to us. Validation of your Information Security controls may include remote or onsite assessment. We expect suppliers to be able to demonstrate that Information Security is a “continual business as usual” activity. Exact Information Security requirements for each engagement will be established during contracting, however a summary of the typical Information Security controls we require our suppliers to meet is set forth below.

Experian Supplier Security Requirements (Summary)

The security requirements included on this page are intended to provide the potential supplier a summary of the key control areas which are expected to form the basis of the supplier’s “Information Security Program”. This programme shall be in effect to protect Experian Information the supplier receives, processes, transfers, transmits, stores, delivers, and / or otherwise accesses.

DEFINITIONS

"Experian Information" means Experian data files, databases, applications software (source code and object code), software documentation, supporting process documents, operational process and procedure documentation, test plans, test cases, test scenarios, cyber incident reports, consumer information, business information, and other data specifically classified by Experian as confidential or restricted.

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

INFORMATION SECURITY PROGRAM

Supplier will maintain a comprehensive Information Security Program that contains administrative, technical, and physical safeguards appropriate to the complexity, nature, and scope of its activities, and the sensitivity of its information assets. Such safeguards will include the elements set forth below and will be reasonably designed to:
(1) achieve the security and confidentiality of Experian Information;
(2) protect against any anticipated threats or hazards to the security or integrity of Experian Information;
(3) protect against unauthorised access to or use of Experian Information that could result in substantial harm or inconvenience to Experian, its clients and / or consumers, and
(4) provide assurances to Experian of the ongoing effectiveness of controls.

If Supplier receives, stores, processes, or transmits cardholder data (CHD; specifically, the primary account number) or sensitive authentication data (SAD)*, it must comply with the most current Payment Card Industry Data Security Standard (PCI DSS) as it relates to the processing of such data as a service provider to Experian.
*For further definition see PCI Data Security Standard as published on https://www.pcisecuritystandards.org/

SECURITY REQUIREMENTS

1. Information Security Policies and Governance

Supplier’s Information Security Program will be consistent with the practices described in an industry standard such as ISO 27002 and the Experian Suuplier Security Requirements Document that is aligned to the Experian Information Security policy.

2. Confidentiality and Integrity

Supplier will utilise a managed approach to security to ensure that Experian Information is protected through the entire life cycle, from creation, transformation and use, storage and destruction regardless of the storage media e.g. tape, disk, paper, etc.

3. Information Stewardship

Supplier will designate information stewards who are responsible for information assets under their control which store, process or transmit Experian Information.

4. Data Loss Protection

Data Loss Prevention (DLP) solutions are to be utilised to identify, monitor and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through content inspection and with a centralised management framework.

5. Vulnerability Management

Firewalls, routers, servers, PCs, and all other Resource(s) utilised in the provision of services to Experian will be kept current with appropriate security specific system patches. Supplier will perform regular penetration tests (including automatic and manual methods) to be completed by independent third parties to further assess the Resources.

6. Physical Security

A security function will exist to grant, adjust, and revoke physical access to facilities where Experian Information resides or can be accessed. All Supplier sites and access to information will reside within the contractually agreed location unless otherwise approved in writing by Experian.

7. Change Management

Modifications and improvements to Resource(s) must be managed through a controlled change management process. A designated 'owner' should be identified for all change requests and changes should be approved by a Change Management Group.

8. Logging and Monitoring

Logging mechanisms must be in place for all systems that process, transmit, or store Experian information. Logging is needed to identify security incidents, establish individual accountability, and reconstruct events. Audit logs will be retained in a protected state (i.e., encrypted or locked) and processes in place to review periodically to detect intrusions, unauthorised access, unintended activities, malicious software, or attempts of these or other actions that could compromise the security of systems processing Experian data. They will be retained for a minimum of 90 days.

9. Intrusion Prevention Systems

Supplier will use security measures (including IPS and IDS) to protect the Supplier telecommunications system(s) and any computer system or network device that Supplier uses to provide services to Experian to reduce the risk of infiltration, hacking, access penetration by or exposure to a third-party.

10. Incident Response

Processes and procedures will be established for responding to security violations and unusual or suspicious events and incidents to limit further damage to information assets and to permit identification and prosecution of violators. Supplier will report actual or suspected security violations or incidents that impact Experian to Experian within twenty-four (24) hours of Supplier's knowledge of such violation or incident

11. Malware Defense

Supplier will use computer malware detection / scanning services and procedures.

12. Segregation of Duties and Envionments

Supplier maintains controls designed to provide adequate segregation of duties among Supplier personnel, including access to systems and networks. Duties are assigned in such a manner that a person will not have conflicting duties that may result in accidental or deliberate compromise of information, systems or processes nor have the opportunity to conceal their errors or irregularities.

13. Encryption and PKI

All Experian Information will be encrypted in line with FIPS 140 requirements when in storage (at rest), unless Experian approved compensating controls are implemented. Laptop computers will not store Experian Information unless Experian agrees there is a business need for such storage, and if agreement is reached, Experian Information on laptops will be encrypted.

14. Network Security

Supplier will provide the following data communication security services:

a) safeguard the confidentiality and integrity of all data being transmitted over any form of data network; and
b) implement and maintain strong current industry best practise standard encryption techniques for all cases in which data identified as Experian Information is transmitted over any public data network. A minimum of 128-bit key encryption is required.

15. Identification, Authentication and Authorisation

Each user of any Resource will have a uniquely assigned user ID to enable individual authentication and accountability. Resources will authenticate each user prior to granting every authorised access. The level of authentication required for access to any Resource is proportionate to the sensitivity of the data housed on the Resource.

Access to privileged accounts will be restricted to only those people who administer the Resource; individual accountability will be maintained. All default passwords (such as those from hardware or software vendors) will be changed immediately upon receipt.

16. User Passwords and Accounts

User passwords will:

a) remain confidential and will not be shared, posted, or otherwise divulged in any manner;
b) consist of a minimum of eight (8) characters for standard user accounts (ten character for privileged user accounts);
c) contain at least three of the following
    i. uppercase characters (A through S)
    ii. lowercase characters (a through s)
    iii. numeric characters (0 through 9)
    iv. non-alphabetic characters (for example, !, $, #, %)
d) not contain the account name or account ID or other easily guessed values;
e) not allow the previous thirteen passwords to be reused; and
f) be encrypted in storage and transmission

User accounts will:

a) automatically lockout after five (5) consecutive incorrect attempts; and
b) expire after a maximum of 90 calendar days (30 days if privileged account user)

17. Remote Access Connection Authorisation

All remote access connections to Supplier internal networks and / or computer systems will require authorisation and will provide an approved means of access control at the "point of entry" to the Supplier computing or communication resources through multi-factor authentication. Such access will use secure access channels, such as a Virtual Private Network (VPN).

18. Secure System Development

Applications developed by Supplier for Experian will follow a methodology that allows for: (i) defining security requirements as part of the requirements definition phase; (ii) using a design model that incorporates best practices in security; (iii) developing code in ways that minimise security vulnerabilities (such as cross-site scripting, SQL injection, buffer overflows, etc.); (iv) testing the code through static and dynamic assessments; and (v) deploying the application in a secure production environment.

19. Personnel Security

All Supplier personnel and subcontractors, if any, who will: (a) have access to an Experian network; (b) have access to, or the capability to view or use Experian information; or (c) be on Experian premises for more than one day and issued an access badge (Individuals who are issued visitor badges and are escorted onsite by an Experian staff member for the entirety of their visit do not fall under this criterion) must pass a criminal background check, and general background investigation. Supplier shall not be required to screen any individual where it is prohibited by law.

20. Training and Awareness

Supplier shall require all Supplier personnel to participate in information security training and awareness sessions at least annually and establish proof of learning for all personnel. Where Supplier has direct access to Experian systems and / or network, Supplier personnel may be mandated to complete Experian training and awareness programs.

21. Business Continuity

Supplier will implement and maintain a Business Continuity program that includes documented recovery strategies, plans and procedures, to ensure the Supplier can continue to deliver its products and services to Experian within the contractual recovery time objective.

22. Experian's Right to Audit

Experian may conduct audits and onsite security risk assessments to assess Supplier Information Security Program and Supplier's compliance with Experian Supplier Security Requirements.

23. Third Party Relationships

Supplier will not provide or commence work with any third party that impacts Experian Information without the prior written approval of Experian. Supplier will not use offshore resources without the prior written approval of Experian.
Supplier will conduct security risk assessments of any third-party service providers with access to Experian Information.