

Information security controls

Briefing for clients on Experian information security controls





Introduction

Security sits at the core of Experian's operations. The vast majority of modern organisations face a significant number of risks relating to loss of information and due to the nature of our business, Experian is no different.

In order to defend our data from such risks, Experian has developed a best of breed security framework based around ISO27001; the cornerstone of which is our information security policy.

As well as our commitment to ensuring that our staff continues to meet our high standards, we have also made a significant investment in establishing a Global Security function to ensure that security is embedded within our day to day activities across the world. The rest of this document is aimed at explaining this security framework in more detail and we hope will demonstrate the Experian commitment to maintaining the security of the data that we hold.

1. Information security policy

The Global Security Policy is owned by the Experian global risk management committee which is an executive level body, and which assumes ultimate responsibility for the Experian risk position. The Global Security Policy is available to all Experian employees on the Corporate Intranet.

The Global Security Policy is reviewed regularly to ensure they are consistent with, and properly address, the following concerns:

- Business needs and business environment;
- External technology environment;
- Internal technology environment;
- Legal, statutory, regulatory and contractual requirements; and
- Other requirements specific to new or unique circumstances

If required, security standards will be updated to include these controls.

2. Organisation and management

Experian has achieved and subsequently retained certification to ISO/IEC 27001, having successfully made the transition from BS 7799.

The Experian Global Risk Management Committee assumes ultimate responsibility and sponsorship for the Experian risk

posture at an executive level. The Global Security Steering Committee assumes operational ownership of the Experian information security policies and standards. The Global Chief Information Security Officer oversees and provides guidance to Experian for the overall development, implementation and coordination of security for systems and physical security. This role is supported by the Global Security Office staff and business unit information security officers. All information assets such as data, applications, software and hardware have a steward appointed who is responsible for ensuring the asset's security.

Management supports security through leadership statements, actions and endorsement of the security policy and implementation/improvement the controls specified in the policy.

Security roles are defined in the Global Security Policy. Each employee, whether permanent or temporary, is responsible for security. Specific business information security roles are also in place in lines of business, i.e. Information Security Officer and Information Stewards.



3. Security – training and awareness

Experian places a strong emphasis on training to ensure that employees are aware of the importance of security within the business environment in an ever changing and evolving risk landscape. All staff are required to comply with a comprehensive suite of security requirements and procedures to ensure they operate all systems in a secure manner.

The Global Security Office deploys a comprehensive awareness programme that targets employees generically and addresses specific areas of compliance for those areas that have specific information security responsibilities. All Experian employees receive mandatory Information Security and Data Protection training on being hired and subsequently on at least a yearly basis to ensure that they are aware of the security policies and their specific information security responsibilities, to ensure that they are properly equipped to perform their duties in maintaining the Experian security posture.

New starters are given training on information security and data protection principles and processes when they join Experian. This includes the use of an information security compulsory basic training module. The initial training is complemented by ongoing training and awareness campaigns.

Staff are subject to both on the job training, and where required, are also

subject to targeted security training programmes. Experian also has a training portal where users can receive training tailored specific to their interest, or needs.

4. Asset classification

Experian has a classification scheme for all information held by it. A security risk assessment determines the classification of each information asset. All information and information assets, including hardware, software, applications and licences are identified and this configuration information is held and maintained in a configuration management database. The assets in this inventory are classified into one of four categories through a risk assessment based on the sensitivity, value, criticality and impact or inherent risk of the asset.

Controls to protect the confidentiality, integrity and availability throughout the lifecycle of the information or information assets will then be applied in accordance with the classification.

5. Physical and environmental security

Physical and environmental security requirements are defined by regularly updated risk assessments carried out on all Experian buildings. Minimum requirements are determined and established within these risk assessments. All Experian employees have the responsibility to maintain the levels of security controls required for each Experian building.



Experian recognises the value of information, and that drives the controls required to adequately manage and secure it throughout its lifecycle.



6. Communications and operations management

Experian has detailed processes and procedures to ensure the confidentiality, integrity and availability of its systems. These include:

- System monitoring and logging
- Change management
- Intrusion detection, prevention and incident management
- Virus and malicious software defence
- Segregation of duties and environments
- Capacity planning
- Cryptographic controls
- Data and voice network security

Experian recognises the value of information and controls required to adequately manage and secure it throughout its lifecycle

All connections to the Experian network are approved, documented and tracked. They are designed to ensure security of architecture, segregation and adequate redundancy. Network components are securely deployed with unused services and components removed and default passwords changed. Physical security controls are in place to protect access to components, cabling, terminals and network ports.

The Experian customer access network is divided into three physically segregated layers. Customer access connections are attached to the access layer of the network.

Virtual application services are installed in the content switching layer of the network and actual application

servers and backend services are installed in the final application/service tier of the network architecture.

Each tier of the network is separated with a layer of firewall appliance from different vendors and is actively monitored by IDS and IPS systems. Firewalls are configured to only allow the network traffic required to conduct business. Routing controls are in place to segregate traffic and disallow unlimited network roaming.

All Experian servers and PCs are built to a documented secure standard, which if appropriate (for example on Microsoft Windows machines) will include anti-virus and malware defences. All information assets will have a defined patching schedule which is determined by the system's criticality and the level of threat the patch is mitigating.

Experian also actively monitors the threat environment and checks the effectiveness of current security controls by reviewing both free and paid for sources of threat information, including; public information, major vendor feeds and also receiving information from specialist closed group mailing lists. The overall process is also plugged into an automated patch and fix strategy which is underpinned with a technology infrastructure to deliver corrective updates.

7. System access

There is a formal user registration and de-registration procedure in place managed by the Access Control Group function which is certified to ISO 27001:2005. Each process involves gaining sign off from the person responsible for the system then actioning the request in a manner that is fully auditable. Regular reviews of user access rights are performed to identify and remove any invalid or inactive accounts. All Experian employees have to comply with stated security practices in the selection and use of passwords. They are also responsible for ensuring that unattended equipment is adequately protected

Each user is given a uniquely assigned user ID, for authentication and accountability. Upon change of requirement, e.g. a change in employment status, access rights are immediately revoked or re-assigned upon notification. Inactive accounts are monitored and disabled after set periods of time unless prior arrangements have been made to explain the inactivity.

Privileged and administrative accounts are reserved solely for performing system maintenance and related administrative duties. These are reviewed more frequently and are subject to tighter controls.

Experian uses authentication and authorisation mechanisms which are proportionate to the sensitivity of the data in the resource which they are protecting. For highly sensitive data Experian requires more than a single factor of authentication and may use location or time based controls to provide additional risk reductions. Experian has a two factor authentication solution in place to ensure all remote access is secure.

8. System development and maintenance

Experian has a framework in place to support management of risk at project level advocating that the process commences at project initiation; risks are initially identified via a formal workshop that includes the project stakeholders. The output from this is transferred onto a standard Risk Register

template and each risk is assessed in order to determine its impact, probability of occurrence and therefore its priority for attention. Risk mitigation activity is then considered, appropriate responses selected, and ownership agreed. Subsequent review of the project risks and progress of mitigation actions is the responsibility of the project manager, and is an iterative process undertaken at predetermined intervals for the duration of the project (agreed with project sponsors), with ongoing input from the stakeholders. A mechanism for escalation of significant risks is agreed with the Project Sponsors at project initiation, and implemented by the Project Manager. Above project-level, the risk review process is conducted via formal risk forums across the enterprise; these take place at quarterly intervals to coincide with the Group Audit Committee schedule.





All Experian staff are subject to screening prior to employment and also prior to promotion or transfer to roles with increased access to sensitive information assets.

9. Security compliance

Experian periodically measures compliance with the Experian Global Security Policy via the Global Security Office. Experian's global security office works with business units to assess their compliance with Experian security policies and standards. The results of these assessments are aggregated and reported to the Global Risk Management Committee.

10. Personnel and provisioning

All Experian staff are subject to screening prior to employment and also prior to promotion or transfer to roles with increased access to sensitive information assets. Screening processes are conducted to provide verification of identity and credentials, as well as to evaluate applicant integrity. Security considerations that support Experian security requirements are addressed through the hiring or contract initiation process and in descriptions

of staff job accountabilities and responsibilities or in statements of work to be performed.

All roles are shadowed by backup personnel. Also, process and procedure is a strong additional facet used to underpin and ensure that knowledge is shared to remove single points of failure/excellence.

All Experian staff are subject to confidentiality/non-disclosure agreements as part of standard contracts. The agreements are not confined to the period of employment with Experian.

11. Business continuity management

The purpose of Business Continuity Planning is to safeguard the interests of Experian's key stakeholders (both internal and external), to ensure our ability to comply with legislation, contracts, and other formal and informal commitments, and to protect our reputation, brand and value-creating activities. To enable this Experian has a framework for the development and maintenance of Business Continuity Plans based on regulatory, contractual client and financial requirements. The plans are based on risk assessments and business impact analysis which are underpinned by established Business Continuity policies and procedures.

All business functions are incorporated within the Business Continuity Management (BCM) programme and are required to analyse their business requirements and clearly define their recovery time objectives to ensure their business criticality is known and understood. Business continuity plans are developed and appropriately maintained and exercised by their respective owners in response to changing circumstances and business risk profiles.

The Group BCM team undertakes periodic compliance reviews of individual BC plans and related documentation. In addition and in conjunction with the Group BCM team, Internal Audit may include the assessment of compliance with the Policy and Standards as part of their work programme.

Group BCM manages a global exception process for use where a non-conformance with the Policy and/or Standards is identified. All exceptions are documented and approved by local senior management and Group BCM. Policy exceptions are appropriately rated and the risks associated with each exception are documented and managed through the global risk management process.

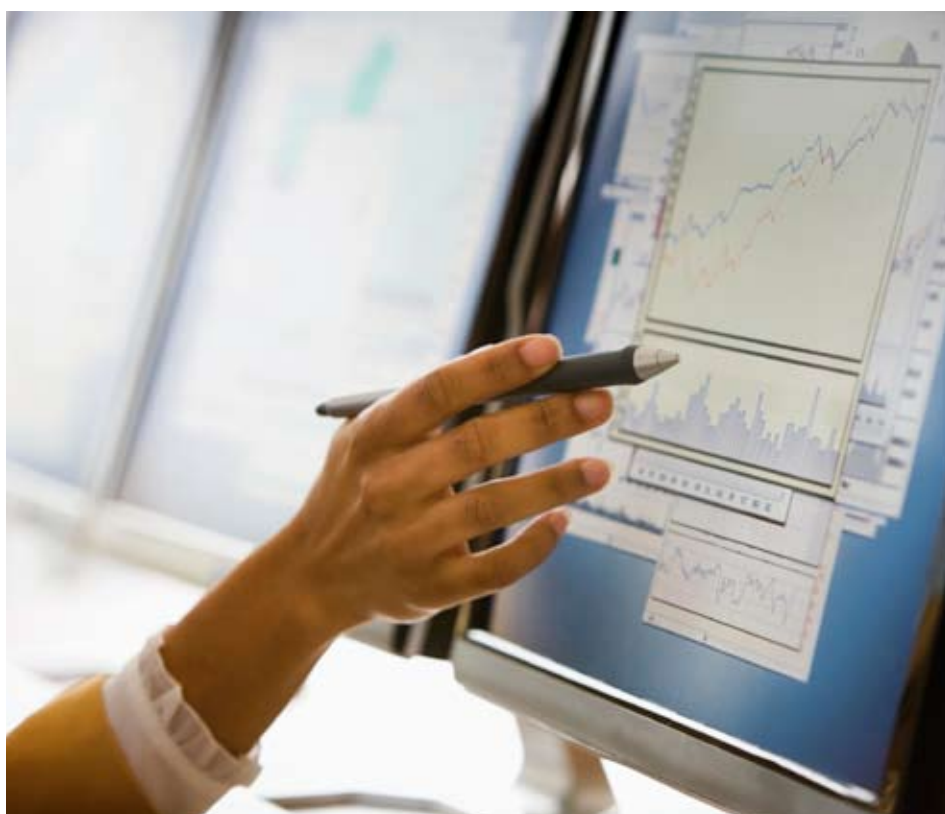
12. 3rd parties

The Experian Global Information Security Policy identifies numerous controls required for outsourcing any services or activities that could potentially impact the security of client data.

The following groups of information security controls and activities are deemed as key when outsourcing to an offshore partner:

- Third party risk identification and control
- Outsourcing contracts
- Governance

When third parties require access to Experian information systems and resources, this request is risk assessed based on the classification and sensitivity of the information that is being accessed, transferred or processed. Any risks that are identified by granting this access are identified and controlled. The third party must demonstrate that their security practices and procedures are consistent with the equivalent Experian standards. Access must be approved by a sponsoring manager and limited to that which is specifically covered by a written contractual agreement. The contract will document information security requirements as contractual terms. Third party access has a review date when third party access is reviewed for termination.





12.1. Third party risk identification and control

Where access to Experian information systems and resources is required by external parties, including business partners, the risks of granting such access are identified and controlled. The following controls address the majority of the risks:

- Experian has a Classification Scheme for all information that falls within Experian responsibility. A security risk assessment determines the classification of each information asset. Controls, such as handling, transfer and destruction, to protect the confidentiality, integrity and availability of the information are consistently applied with the assigned Experian classification
- Information security policies, standards and practices, including security roles and responsibilities are in defined, documented, agreed and implemented
- Recruitment standards and procedures are implemented

to ensure business partner employees and contractors (if used) are screened, inducted, trained and managed according to Experian Global Security Policy

- Planning and management controls required in delivering services to Experian are implemented, approved and maintained, including segregation of duties
- Dependent on the technical and network connectivity, technical security controls are implemented to ensure security vulnerabilities are identified and managed, and approved technical and security configurations are implemented and maintained
- Change management standards and processes are implemented
- Contracts are drawn up which explicitly state the required security controls and requirements
- Physical and environmental controls are implemented, tested and maintained
- Incident management processes and controls are implemented
- Access control requirements

are identified, agreed and established to approve correct levels of user access to Experian information systems

- Controls associated with processes deployed to deliver outsourced services to Experian, including Systems and Software Development lifecycle
- Legal and regulatory requirements, including Data Protection and client contractual requirements
- Business continuity management and IT disaster recovery planning controls, including backup and retention

There could be other specific information security risks arising from the outsourcing of particular services that would have a set of unique controls, i.e. Customer Service Centre; Business Processing.

12.2. Outsourcing contracts

A standard approach to identifying and applying information security controls within contracts is used, although this is adapted according to the type of outsourced service. The following contractual arrangements are generic throughout:

- Definitions and Interpretations
- Scope of agreement
- Transition and acceptance
- Experian's assets and premises
- How the services are to be provided
- Retention of documentation and audit
- Correction plans, fraud, conflict of interest and Escrow
- Additional obligations of the parties and liability
- Intellectual property and confidentiality
- Escalation and dispute resolution
- Suspension and termination
- Compliance with legislation and policies
- Security
- Guarantees

12.3. Governance

The process of establishing an agreed approach to information security includes some key activities, namely:

1. Due diligence and business partner selection
2. Security risk identification, assessment and controls
3. Contracting
4. Technical connectivity
5. Offshore transition
6. Compliance review
7. Contractual, service and change management
8. Ongoing audits and reviews

From an Information Security perspective actions required to implement and monitor agreed controls based on the identified security risks are managed through ongoing reviews with the service provider.

13. Incident management

Experian has a formally documented risk-based incident management process to respond to security violations, unusual or suspicious events and incidents. This process is

coordinated by the Experian Global Security Office and is owned by the Executive. The purpose of this process is to limit further damage to information assets, identify root cause, and execute corrective actions. Incident communication is tightly controlled to ensure a 'need to know' principle while allowing the correct investigation and escalation to occur. Post incident reviews are held to analyse the effectiveness of the incident response and operational processes in order to continually improve them. The Experian incident response processes are periodically audited and tested to ensure their currency and effectiveness.

Trends and patterns of security incidents are reviewed and examined to determine enterprise issues or implications to the larger business. The incident management process feeds into other functional areas of the company including training and Awareness, risk management and business continuity.

All third party and partner staff must complete on a yearly basis a mandatory computer based information security training which covers recognising and reporting security incidents. This training is backed up with targeted awareness activities such as presentations, intranet articles and specialised training for staff in key positions on how to identify role specific incidents.

14. Data transfer standards

As a global provider of information solutions we continuously assess information threats and industry trends based upon The Experian Global Security Policy and we have identified a need to clearly define the controls and standards required for information exchanges between Experian, our clients, and other third party organisations.

This identifies the mechanisms currently approved for information exchange between our clients and Experian.



14.1. Data transfer security requirements

The principles of information security management define the requirements for effective information protection and these include;

- Non-repudiation – When transferring any information the system must ensure that the sender and recipient are confident that any other party is known and trusted and there is evidence to prove this
- Confidentiality/Integrity – Both parties in such an exchange require assurance that information is stored, transmitted and processed in a secure manner
- Audit – For the assurance of information integrity all information transfer must be suitably recorded to ensure that key events from any transfer can be evaluated in a timely manner

By applying these principles secure transfer of data can be achieved by either sending the data through an encrypted network communication channel or by encrypting the data file before sending along an unencrypted channel. All network communication types including the Internet can be provided with suitable encryption solutions to allow for data transfer.

14.2. Data classification

Any data that is to be transferred or exchanged must be classified according to its value and importance. Each classification attracts specific controls to adequately manage and secure it.

For all data being transferred or exchanged between Experian and our clients (i.e. Experian to Client/Client to Experian), we regard that data to be confidential.



As a global provider of information solutions we continuously assess information threats and industry trends

Experian Limited
Landmark House
Experian Way
Nottingham
NG80 1ZZ
www.experian.co.uk



© Experian 2009.

The word "EXPERIAN" and the graphical device are trade marks of Experian and/or its associated companies and may be registered in the EU, USA and other countries. The graphical device is a registered Community design in the EU.

All rights reserved.