

# EXPERIAN INFORMATION SOLUTIONS

## Protecting Client Information

No matter where information travels or what form it takes, sufficient security mechanisms are absolutely essential to protect it from attack. Whether from intentional hacking or accidental disaster, once critical data has been compromised, your company's reputation can be quickly jeopardized.

Experian maintains a comprehensive information security program that contains administrative, technical, and physical safeguards that are appropriate to the sensitivity of the information. Such safeguards are designed to:

- Ensure the security and confidentiality of customer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access or use of information that could result in harm or inconvenience to any customer.

At Experian we take a managed approach to security to ensure that data is protected through the entire lifecycle, from creation, transformation and use, storage and destruction we are deploying the latest techniques and processes to provide the best possible protection. To protect your customer, your company's good name and Experian's corporate reputation we monitor our systems to ensure the utmost in customer information protection.

The common "defense-in-depth" security architecture is not enough in today's dynamic Internet world. Experian continually reassesses its security strategy and is moving to a resilient security enterprise that will be equipped with processes and people to anticipate new threats and mitigate exposures to the environment. The resilient security architecture is the equivalent to putting a turret on the military tank to quickly react to new and unanticipated threats.

### **People**

At Experian we believe our people are our most valuable asset. In information protection it takes the best, most well trained staff to meet the challenges of today's dynamic Internet world. We started by hiring a leading Chief Information Security Officer in the field and are developing a team of

[This document is a general description of security practices in Experian's various lines of business. Security controls are implemented as required to meet specific risk reduction objectives. Refer all detailed questions to Client Information Security.](#)

information protection specialists. They are implementing processes and technology that allow for cost-effective protection of information while balancing risk and expense. Our internal training capabilities are second to none allowing us to continually develop, educate and train our staff.

### **Network Security and Intrusion Detection**

Firewalls and intrusion detection devices protect entrance to Experian's network. The internal network is divided into "network security zones" providing additional protection layers in the network. Access to the production systems is granted on an as-needed basis, and is monitored for any possible abuse or unauthorized users.

Experian protects its telecommunications system and any computer system or network device that is used to provide services against the risk of infiltration and access penetration. We maintain state-of-the-art firewalls and provide general maintenance and monitoring of firewalls. We strictly monitor and approve all firewall rule set changes and provide monitoring of firewalls in order to identify attempted security violations.

### **Virus Protection**

Experian deploys, implements and maintains the most current commercially available computer virus detection/scanning program. We use three-tiered virus prevention architecture to prevent the infection and spread of computer viruses between parties, which access or exchange data or files through network connectivity.

### **Access Control**

Experian implements the latest measures to restrict electronic access to its Client's systems to only authorized personnel who are subject to nondisclosure agreements for the protection of Client information. We ensure that all personnel who access or submit material to its Client's systems are uniquely identified and authenticated. We enforce the principle of "least privilege," namely, that authorized personnel only have the level of access to our customer's systems required to perform their job functions in providing services to them.

In addition to application, database or operating system level access controls, we encrypt data as required by our Client using strong, industry standard encryption technology when not under the strict controls of our host systems.

[This document is a general description of security practices in Experian's various lines of business. Security controls are implemented as required to meet specific risk reduction objectives. Refer all detailed questions to Client Information Security.](#)

## **Data Integrity**

Experian safeguards the confidentiality and integrity of all our customer's data being transmitted over the data network. We implement and maintain strong, industry standard encryption techniques to protect Client's data when transmitted over open networks (for example, SSL for Web browser sessions, or PGP file encryption for bulk data transfers).

## **Background Check**

Experian performs background checks on all individuals that have access to sensitive information. The background checks include criminal background checks, financial checks, and reviews of previous employment references. Upon hiring, each Experian representative signs proprietary information, non-disclosure and invention agreements.

## **Separation of Duties**

Experian ensures that adequate separation of duties exist among the staff including access to systems and networks. Access is granted to only appropriate and approved individuals based upon business need. Duties are assigned in such a manner that a person does not have the opportunity to conceal their errors or irregularities.

## **Vulnerability and Threat Management**

In addition to Experian's three tiered virus protections, we periodically scan our network and systems for vulnerabilities. We have security standards for configuration of our systems devices that are maintained by our professional system administration staff.

## **Business Continuity and Disaster Recovery**

Experian currently has extensive plans in place for business continuation caused by natural disasters. This plan outlines Experian's ability to sustain normal business operations with its own power capabilities, water, and supplies. Experian has made a corporate commitment to maintaining an integrated Business Continuity Plan across all of our North American operations. We maintain and regularly test a comprehensive Business Continuity Plan for all products and services. Environmental controls are in place to protect against damage or disruption from water damage, power outages, and extreme temperatures. Uninterrupted Power Supply (UPS) systems and diesel backup generators are established to serve as power backup contingencies.

[This document is a general description of security practices in Experian's various lines of business. Security controls are implemented as required to meet specific risk reduction objectives. Refer all detailed questions to Client Information Security.](#)

## **Physical security**

The Experian Data Centers are protected by a 24x7 manned security operation. Security Officers patrol the site and ensure that all appropriate and established security measures are followed. Our Security Officers monitor and record closed circuit cameras 24 hours a day, seven days a week. The cameras provide surveillance of the interior, parking lots and all perimeter areas. Building access is controlled through the use of an electronically coded magnetic striped badge system. There are specific access levels controlling restricted areas that are approved only through senior management.

Access to secured areas such as data centers, telecommunications areas, etc. are restricted to authorized personnel on a need-to-access basis. These areas are protected with additional entry controls such as video surveillance, locks, magnetic swipe cards, and proximity card readers. An audit trail of access to these restricted areas are maintained and regularly reviewed.

This document is a general description of security practices in Experian's various lines of business. Security controls are implemented as required to meet specific risk reduction objectives. Refer all detailed questions to Client Information Security.