Client Minimum Security Standards

Level Two

Version: 2.6

One Park Lane, Leeds LS3 1EP t. +44 (0) 113 388 4300 f. +44 (0) 113 388 4308 e. enquiries@TransUnion.co.uk
www.TransUnion.co.uk

Contents

1 DOCUMENT CONTROL

Description	Status
Version:	2.5
Date:	18th July 2018
Owner(s):	Group Security Director

Change History Log

Issue Number		
1.0	27 May 2011	Initial issue
2.2	03 November 2014	No changes
2.3	01 April 2015	No changes
2.4	20th January 2017	Updated and reviewed
2.5	18th July 2018	Rebrand and Reviewed
2.6	02nd May 2019	Rebrand and Contents Reviewed

2 INTRODUCTION

TransUnion recognises the importance of maintaining the highest levels of Information Security Management. Data can exist in many physical and logical forms, and can be subject to many types of human, physical and logical, in storage, processing and dissemination threat.

By providing our clients with access to data rich services, it is necessary to define a set of minimum security requirements which ensure the continued safe-custodianship of those assets.

This document describes the key areas we expect our clients to consider and provide the necessary controls, whether they are people, process or technology focused.

3 INFORMATION SECURITY MANAGEMENT

The client will employ operational and technological processes and procedures in line with good industry practice to protect against unauthorised use, access, loss, destruction, theft or disclosure of any information provided within the context of the service delivered by TransUnion Information Group.

It is expected that the client will be either registered to ISO27001, be able to demonstrate that they are working towards certification with agreed timescales or have control in place which are suitably aligned to the standard and demonstrable through onsite assessment.

The client will specifically ensure that the following requirements are met:

- The client acknowledges that it is critical to the interests of Customers and the reputation of TransUnion that all information be maintained in a secure manner at all times.
- An Organisational Security Policy exists, which has been endorsed at Board level, setting out commitment to comprehensive and ongoing security, including the physical, technological, logical, organisational and contractual measures set out in subsequent sections
- Clear allocation of responsibility to maintain and review the overall policy on an annual basis.
- Notification to TransUnion of the person, and alternate, with overall responsibility for Information Security, and the person/alternate (if different) to be used as the point of contact in the event of a security incident.
- Provision of sufficient resources, skills and facilities to meet all security responsibilities.
- Data must be classified as per its sensitivity.

- Guard against unauthorised or unlawful processing of Customer Personal Data and against accidental / deliberate corruption, loss or destruction of, or damage to, Customer Personal Data.
- In respect of portable and mobile devices used to store, transport and/or (as the case may be) Customer Personal Data (including paper records and magnetic and other electronic media) to store and transmit personal data (including laptop computers, mobile phones, memory sticks, PDAs, mobile phones, discs, external hard drives, and magnetic tapes) ("Mobile Media"), the loss of which could cause damage or distress to individuals, such measures will include the use of a Secure Medium and the encryption of all Customer Personal Data stored on, transported by or transmitted by such Mobile Media and/or (as the case may be) the encryption of such Mobile Media itself, in all instances:
- Asset disposal procedure is defined and followed to ensure all hard drives and media (e.g. tapes, CD's) are cleansed, degaussed or shredded after use so that no remnants of data still exist and / or are recoverable.
- The client will actively document and follow a clear desk procedure in line with best practice.

4 HUMAN RESOURCES SECURITY

The client will specifically ensure that the following requirements are met:

- Background and integrity checks (where appropriate in accordance with good industry practice) on employees or any other person having access to the output of the services ("staff") before their initial employment or subsequent move into a job function that would give them ability to access, use, alter, damage, destroy, copy or disclose any data provided by TransUnion.
- Adequate training and regular re-training of staff about their security responsibilities, Data Protection Act and legal obligations.
- Appropriate confidentiality provisions signed by staff as part of contract of employment or separate agreements.
- Rules and procedures to withdraw security access privileges for staff not complying with these Security Rules, Regulations and confidentiality provisions.
- Paper disposal procedures in place to ensure shredding of any printed materials items showing sensitive data.
- Guidelines issued to all employees to lock away any confidential items such as portable media or documents when not in use.
- Take reasonable steps to ensure the reliability of employees who have access to Customer Personal Data. Such steps to include employees undergoing training in data protection law and the care and handling of personal data as is deemed requisite and appropriate.

5 PHYSICAL AND ENVIRONMENTAL SECURITY

The clients work premises should ensure the following:

- Current and tested premises intrusion detection and notification systems with assigned and documented alarm procedure.
- Appropriate strength doors, windows and locks.
- Issue of keys and codes restricted only to those who need it, with supporting documentation.
- Issue of appropriate passes to visitors and escort procedures; appropriate restrictions on visitor movement, especially to those areas with direct access to printed, screen, physical or logical versions of sensitive information.
- Distinct physical room or rooms for server and communications equipment; issue of keys and codes restricted only to those who need it, documentation of their issue.

6 ACCESS CONTROL

- Access and type of access to all data/databases/networks/devices enforced on the basis of defined, individual staff/user permissions requiring username and password logon.
- All access permissions set at least privilege and based on a need to know basis.
- Password/logon controls including complexity, expiry, uniqueness and lockout to meet best practice standards.
- Procedures to grant/rescind user permissions in line with changes in responsibilities, including termination.
- Hardened servers, including ongoing security patching, as appropriate.
- Screensaver non-activity lockouts on all servers and workstations in place and as per best practice.
- Display of appropriate security notices as part of the individual user logon process.
- Appropriate levels of activity logging, storage and review to provide abuse deterrence and to enable forensics in the event of a security breach.
- Distinct logon accounts for individual users of TransUnion Services.
- Specific responsibility assigned to person or persons to administer user logon accounts, including change of privilege and withdrawal of privilege in the event of user security breach or termination.

7 COMMUNICATIONS AND OPERATIONS MANAGEMENT

The client will specifically ensure that the following requirements are met:

- Protection of all external Internet gateways with appropriate firewalls and current security patches.
- Appropriate timely vulnerability scanning shall be conducted on external Internet gateways and significant findings remediated accordingly.
- Protection of other external communications access routes (e.g. out of band internet or remote access) with appropriate measures in line with best practice.
- Change control procedures governing amendments to firewall rule bases and other network changes relating to TransUnion data or assets.
- Restrictions to remote user access including appropriate user authentication and session encryption.
- Restrictions and procedures to ensure transfer and storage of sensitive information outside of the logical security perimeter of the client network is protected with a minimum of 256-bit digital encryption/authentication and/or a complex password.
- Appropriate and current antivirus protection measures are in place.

8 INFORMATION SECURITY INCIDENT MANAGEMENT

The client will specifically ensure that the following requirements are met:

- Implement technology and processes necessary to log all appropriate security event information.
- Adequate separation of duties must be in place to maintain the security event information.
- Monitoring of own environment, applications and processes for actual or potential security intrusions or violations.
- The Client will notify TransUnion by secure medium of any occurrence of a breach of information security immediately upon becoming aware of any such incident or immediately upon becoming aware of circumstances which are reasonably likely to lead to such an incident with sufficient detail as to allow TransUnion to ascertain in reasonable detail the magnitude and likely consequences of the Information Security Breach.
- The Client will co-operate with TransUnion and any appropriate third party in respect of an Information Security Breach.

9 BUSINESS CONTINUITY MANAGEMENT

The client will specifically ensure that the following requirements are met:

- It is expected that the Client will have an appropriate Business Continuity Management System (including Disaster Recovery) in place that will include a documented Business Continuity Plan and Policy and a documented Disaster Recovery Pan and Policy. There

should also be a named individual in place who is responsible for the day to day management of Business Continuity.

10 RIGHT TO AUDIT

- TransUnion reserves the right to visit the Client's offices to carry out checks as it deems necessary to ensure that the Client is properly fulfilling its obligation to this standard and may request sight of records and documents held by the Client in respect of such obligations.

11 PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

- If the Client is provided with access to Primary Account Numbers or are a Service Provider (as defined by the Payment Card Industry Security Standards Council), they will ensure that their environment and any subsequent services are provided in a manner which is compliant with the latest version of the Data Security Standard ("PCI DSS").

12 API ENCRYPTION REQUIREMENT

If the Client is provided with access to a TransUnion API service, it will be required to ensure that its communication with the API is encrypted to a suitable standard in line with best practice.

13 APPLICATION TO THIRD PARTIES

The Client must only make the Relevant Data available to those third parties to whom it is expressly authorised to supply the Relevant Data under the written agreement between TransUnion and the Client **("Third Party Recipients").**

The Client must ensure that any Third Party Recipients who receive Relevant Data comply with the Minimum Security Standards set out in this document. For this purpose, references in this document to the **"Client"** should be taken to include a reference to the relevant Third Party Recipients.

The Client must take appropriate steps to satisfy itself that the Third Party Recipients can and do comply with the Minimum Security Standards.