BROWSER

Information Security Policy

Prepared by	James Blizzard, Technical Lead
Approved by	John Beck, Strategy Director
Last updated	13th February 2019

Browser London Limited recognises that information and the associated processes, systems and networks are valuable assets and that the management of personal data has important implications for individuals.

Through its security policies, procedures and structures, Browser London Limited will facilitate the secure and uninterrupted flow of information, both within Browser London Limited and in external communications. Browser London Limited believes that security is an integral part of the information sharing which is essential to academic and corporate endeavour and the policies outlined below are intended to support information security measures throughout Browser London Limited.

This policy is based on recommendations contained in ISO 27001.

Definition

For the purposes of this document, information security is defined as the preservation of: confidentiality: protecting information from unauthorised access and disclosure; integrity: safeguarding the accuracy and completeness of information and processing methods; and availability: ensuring that information and associated services are available to authorised users when required.

Information

Information exists in many forms. It may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Appropriate protection is

required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

Protection of Personal Data

Browser London Limited holds and processes information about employees, clients, and other data subjects for administrative and commercial purposes. When handling such information, Browser London Limited, and all staff or others who process or use any personal information, must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). Responsibilities under the 1998 Act are set out in the Data Protection Policy.

Information Security Responsibilities

Browser London Limited believes that information security is the responsibility of all members of staff. Every person handling information or using Company information systems is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at Browser London Limited.

This Policy is the responsibility of the Board; supervision of the Policy will be undertaken by the senior management. This policy may be supplemented by more detailed interpretation for specific sites, systems and services. Implementation of information security policy is managed through the Information Security Manager and other designated personnel with security responsibilities in specified areas of Browser London Limited.

Information Security Education and Training

Browser London Limited recognises the need for all staff and other users of Company systems to be aware of information security threats and concerns, and to be equipped to support Company security policy in the course of their normal work. The Information Security Officer shall implement a training programme for each class of users and, at the behest of Browser London Limited's departments, shall provide information and further training in information security matters to answer particular requirements.

Compliance with Legal and Contractual Requirements

Authorised Use

Company IT facilities must only be used for authorised purposes. Browser London Limited may from time to time monitor or investigate usage of IT facilities and any person found using IT facilities or systems for unauthorised purposes, or without authorised access, may be subject to disciplinary, and where appropriate, legal proceedings.

Monitoring of Operational Logs

Browser London Limited shall only permit the inspection and monitoring of operational logs by computer operations personnel and system administrators. Disclosure of information from such logs, to officers of the law or to support disciplinary proceedings, shall only occur (i) when required by and consistent with law; (ii) when there is reason to believe that a violation of law or of a Company policy has taken place; or (iii) when there are compelling circumstances.

Access to Company Records

In general, the privacy of users' files will be respected but Browser London Limited reserves the right to examine systems, directories, files and their contents, to ensure compliance with the law and with Company policies and regulations, and to determine which records are essential for Browser London Limited to function administratively or to meet its client obligations. Except in emergency circumstances, authorisation for access must be obtained from the Managing Director or their nominee, and shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

Protection of Software

To ensure that all software and licensed products used within Browser London Limited comply with the Copyright, Designs and Patents Act 1988 and subsequent Acts, Browser London Limited will carry out checks from time to time to ensure that only authorised products are being used, and will keep a record of the results of those audits. Unauthorised copying of software or use of unauthorised products by staff may be grounds for disciplinary, and where appropriate, legal proceedings.

Virus Control

Browser London Limited will maintain detection and prevention controls to protect against malicious software and unauthorised external access to networks and systems. All users of Company computers, including laptops, shall comply with best practice in order to ensure that up-to-date virus protection is maintained on their machines

Retention and Disposal of Information

Responsibility

All staff have a responsibility to consider security when disposing of information in the course of their work. Departments should establish procedures appropriate to the information held and processed by them, and ensure that all staff are aware of those procedures. Where appropriate data should be retained or disposed based on specific client requirements.

Reporting

All staff and other users should report immediately by e-mail to support@browserlondon.com or by telephone to the Technical Lead, Information Security Manager or Managing Director, any observed or suspected security incidents where a breach of Browser London Limited's security policies has occurred, any security weaknesses in, or threats to, systems or services.

Software Malfunctions

Software malfunctions should be reported to the Technical Lead.

Business Continuity

Browser London Limited will implement, and regularly update, a business continuity management process to counteract interruptions to normal Company activity and to protect critical processes from the effects of failures or damage to vital services or facilities.