BROWSER

Information Classification Policy

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

Browser London Limited provides digital services for a variety of clients worldwide. It is critical for Browser London Limited to ensure a high standard for the protection of information assets from unauthorised access and compromise or disclosure. Accordingly, Browser London Limited has adopted this information classification policy to help manage and protect its information assets.

All Browser London Limited associates share in the responsibility for ensuring that Browser London Limited information assets receive an appropriate level of protection by observing this Information Classification policy:

- Company Managers or information 'owners' shall be responsible for assigning classifications to information assets according to the standard information classification system presented below. ('Owners" have approved management responsibility. 'Owners' do not have property rights.)
- Where practicable, the information category shall be embedded in the information itself.
- All Company associates shall be guided by the information category in their security-related handling of Company information.

All Company information and all information entrusted to Company from third parties falls into one of four classifications in the table below, presented in order of increasing sensitivity.

Category	Description	Examples
Unclassified Public	Information is not confidential and can be made public without any implications for Company. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.	• Product brochures widely distributed • Information widely available in the public domain, • including publicly available Company web site areas • Sample downloads of Company software that is for sale • Financial reports required by regulatory authorities • Newsletters for external transmission • Any digital asset with an open licence
Proprietary	Information is restricted to management- approved internal access and protected from external access. Unauthorized access could influence Company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	• Passwords and information on corporate security procedure • Know-how used to process client information • Standard Operating Procedures used in all parts of Company's business • All Company-developed software code, whether used internally or sold to clients

Client Confidential Data	Information received from clients in any form for processing in production by Browser London Limited. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Client media • Electronic transmissions from clients • Product information generated for the client by Company production • Customer Data • User data from Twine or other Company services
Company Confidential Data	Information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Salaries and other personnel dat • Accounting data and internal financial repo • Confidential customer business data and confidential contracts • Non-disclosure agreements with clients/vendors • Company business plans

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.

BROWSER

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.

BROWSER

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.