BROWSER

Security overview

Prepared by	James Blizzard, Technical Lead
Approved by	John Beck, Strategy Director
Last updated	23rd Nov 2017

BROWSER

1. Introduction

This document is intended to provide an overview of the policy and procedures that Browser London Ltd take in order to maintain alertness and response protocol in the event of a incident. For specific information that is applicable to your account please contact your account manager.

2. Staff training

We run security briefings for all new staff members, which are followed by routine updates throughout the course of their employment. We employ an education approach to updating key staff members on new security developments, through a range of applicable courses, events, and tutoring. We follow a protocol for onboarding new staff members and offboarding departing staff members.

Due to the ongoing nature of security, notably zero day vulnerabilities, we regularly update practices to mitigate against risk, these currently include:

- Regular password rotation
- A policy on passwords and their format
- Enforcing two-factor authentication across our network
- Encryption of password, files and messaging
    - Encryption of device hard drives (e.g. FileVault)
    - Encryption of external messaging data (e.g. Signal, Whatsapp, PGP)
    - Standard TLS encryption across internal chat and email clients
    - Using encryption services with vaults (e.g. 1password)
    - Using the company wide VPN (e.g. Express)
- Logging entry/exit within the office/building via key Guard
- Logging entry/exit within the building via CCTV
- Mobile device management via Google Device Management
- Log staff credentials, and verify (e.g. Passports, P45's)
- Running malware detection on a regular basis (e.g. MalwareBytes)
- Audit machines and devices (see Hardware)
- Auditing project access for the past 3 years (staff and their access level)
- Overall mindfulness of discussing sensitive information

BROWSER

2. Company hardware

We regularly update and replace hardware to maintain performance and industry standards. We do not loan or lease hardware from or to third party organisations. We are sensitive to the origin of hardware that is purchased, where and who we procure hardware from is based on a range of deciding factors that include: reputation, review, support, origin, legal position, legal location, 3rd party ownership. We also make records of the following for auditing and device management purposes:

- Desktops, laptops and tablets, mobile and desk phones
    - Serial numbers
    - IP addresses
    - mac address
    - Manufacturer
    - Model numbers
    - Value and date of purchase
- Servers and location
- Storage devices
- Mainframe computers

3. Company software

We use a range of 3rd party software and tools to in order to provide services to our clients. Please contact your account manager to request an inventory of the software and tools that have been used within your project lifecycle, these may include:

- Security and monitoring software
- Device operating software
- Email and messaging software
- CRM software
- Data management software
- Database management software
- Outsourced software development agreements
- Storage management software
- Web browsing software (e.g Chrome, Firefox)
- Open source software

BROWSER

5. Security and certification

We have a range of measures in place to mitigate against risk, these measures are tested on a regular basis in order to maintain alertness within the business. Please contact your account manager to request an inventory of the security and certification that is applicable to your project and business relationship, these may include:

- Intruder detection programmes
- Tests results for system vulnerability checks
- Information on previous security breaches
- Information security insurance and certificates
- Staff training programmes on security
- Network Firewall settings and maintenance
- Remote access software
- Policy on acceptable use for hardware and software
- Policy on remote working
- Information on which non-employees are granted access to important company data
- Policy on company passwords
- Plan for disaster recovery and security breaches
- Information on database record storage
- Vendor updates

6. Customer Support

Customer support is integral to the services we offer, in order to provide effective support to our customers we have a process for onboarding new clients and verification of the client representatives. An overview of your customer support package will be included within your SLA. Please contact your account manager if you wish to discuss the customer support process further. Additional information may include:

- How new clients are onboarded
- How clients access technical support
- How a client request are verified
- An outline of how authorised clients make requests
- An outline of who is responsible for actioning client requests

BROWSER

7. Operations and business continuity

Maintaining business continuity is key to maintaining an effective operation and providing services to our clients. To ensure business continuity we regularly assess our operational position, this may include:

- Listing staff, their roles and responsibilities
- Maintaining staff training programmes and knowledge sharing
- Reviewing confidentiality and intellectual property agreements for staff
- Documenting how knowledge sharing is approached and distributed
- Reviewing staff competency and review schedules
- Documenting organisational chart and project team
- Reviewing deployment and access levels
- Reviewing vacancies that are required
- Listing previous employees and their access levels for the last 3 years

8. Services rendered

The services that we provide cover consultancy, bespoke design, development, and support. We may use a range of services from 3rd party suppliers. Please contact your account manager to request an inventory of the the services and 3rd party suppliers that are applicable to your organisation, these may include:

- Security and anti-virus software
- Transactional email software (e.g. Postmark)
- CRM and integration software (e.g. Nutshell)
- Data management software
- Database and hosting management and monitoring
- Storage management (e.g. S3)
- Information on hosting environment (e.g. AWS)
- Storage backup systems (e.g.)
- Browser operating software (e.g. Chrome)
- Open source software (e.g. Drupal)
- Online payment gateways (e.g. Stripe)
- Information on software development processes
- Service level agreements

- Outsourcing software agreements
- Log of planned (and unplanned) network downtime over a set period
- A diagram of the network set-up