BROWSER

Access Control Policy

Prepared by	James Blizzard, Technical Lead
Approved by	John Beck, Strategy Director
Last updated	14th February 2019

1. Introduction & Purpose

Browser London Limited implements access control across all services and IT infrastructure. This provides authorised, audited employee access and ensures compliance with the requirements as detailed in the Browser London Information Security Policy.

This policy document defines the correct usage and management of system access control within Browser London Limited.

2. Scope

The policy applies to all Browser London Limited networks, IT systems and data, as well as employees, employees of temporary employment agencies, business partners, and contractor personnel.

This applies to all Browser London Limited IT services and resources, including:

- Computer networks (LAN/WIFI)
- Computer hardware (e.g. servers, networking equipment, laptops, mobile phones)
- Externally hosted virtualized (cloud) services (e.g. web servers, database servers)
- Internally used commercial services (e.g. Google Apps)
- Business and customer data

3. Policy

3.1. Access control policy

Browser London Limited will provide all employees with user accounts in order to carry out their required responsibilities. Privileged/administrative accounts are not provided by default.

Granting of these permissions is authorised, managed and documented by the Information Security Manager.

Access control is granted on a basis of least privilege.

3.2. Employee access

All employee access (including temporary workers and contractors) is granted by the Information Security Manager. Any personnel changes need to be communicated by department heads to Information Security Manager.

At start of employment, all employees are assigned a unique email identifier, protected by both password and Time-based One-Time Passwords (TOTP).

Accounts are suspended, and access is revoked on termination of employment.

3.3. Employee responsibilities

Users are required to read and abide by Browser London Limited's policies, standards and guidelines for appropriate and acceptable usage of the networks and information systems and resources. These are provided at start of employment.

It is each employee's responsibility to notify the Information Security Manager of any event which may compromise the integrity of Browser London Limited's systems or services.

3.4. Network, infrastructure, and remote worker access

Office network and infrastructure access is granted by, managed and documented by the Information Security Manager.

All infrastructure access is provided through SSH key pairs, secured with passphrases.

3.5. Monitoring of system access

All accesses to Browser London Limited's information systems are logged, including user, date/time, and IP address.

Unsuccessful accesses are also logged.

3.6. Mobile computing

Portable devices provided to employees are required to implement full-disk encryption, which is overseen and verified by the Technical Lead.