BROWSER

Incident Management Policy

Prepared by	James Blizzard, Technical Lead
Approved by	John Beck, Strategy Director
Last updated	3rd January 2019

1. About this plan

1.1 Introduction

This manual was developed for Browser London Limited, herein referred to as Browser, and it is classified as the confidential property of that entity. Due to the sensitive nature of the information contained herein, this manual is available only to those persons who play a role in incident response and recovery processes.

This document may be shared with clients if approved by the Managing Director.

1.2 Overview and objectives

This incident management plan establishes the recommended organisation, actions, and procedures needed to

- Recognise and respond to an incident;
- Assess the situation quickly and effectively;
- Notify the appropriate individuals and organisations about the incident within 24 hours;
- Organise the company's response activities;
- Escalate the company's response efforts based on the severity of the incident; and
- Support the business recovery efforts being made in the aftermath of the incident.

This plan is designed to minimise operational and financial impacts of such a disaster, and will be activated when a local Incident Manager (or, in his/her absence, one of his/her alternates) determines that a disaster has occurred.

1.3 Scope

This document covers critical Infrastructure defined as follows:

- The public Amazon Web Services (AWS) platform hosting client services.
- Any third party hosting area where we have accepted responsibility.

This incident management plan includes initial actions and procedures to respond to events that could impact critical business activities at Browser London Limited and where appropriate, it's clients. This plan is designed to minimise the operational and financial impacts of disasters.

BROWSER

2. Incident response

2.1 Immediate action

Upon discovering a security incident or critical fault the following steps must be taken, in order:

1. Ensure data integrity and security by taking immediate snapshots.
2. If the service or part thereof is unavailable, attempt to restore service providing that this action does not impact on data integrity and security.
3. Restore backups where appropriate.
4. Secure and duplicate any evidence required for a root cause analysis of the incident.
5. Inform the affected clients and provide an ETA to resolution.
6. Refer the issue to the development lead and assist management to perform a full root cause analysis.
7. Generate change request entries to resolve any outstanding issues.

2.2 Security incidents

ISO 27001 Sections 13.01.01, 13.02.01, 13.02.03

In the event of a security related incident a certified outside auditor may be used to verify system integrity and provide a detailed analysis of the evidence and root cause of the incident.

These steps are aimed at our own AWS based infrastructure, where a third party supplier is supplying hosting they should be notified as quickly as possible (within 24 hours) so that their own plan can be implemented. Continue to follow the steps below as best as possible without hindering the third party host in their work.

Where data and evidence integrity must be secured the following steps must be taken immediately.

- Create a manual database snapshot to preserve data integrity and for evidential purposes.
- Verify that the AWS management platform has not been compromised, take immediate action to change credentials of all privileged users if a security breach is suspected [AWS Only].
- Take snapshots of all running instances for evidential and backup purposes.
- Take action to secure any running instances.
- Inform the development lead and then product team as a whole.
- If appropriate notify the Amazon Web Services security team - http://aws.amazon.com/security/

- Check all Security Groups, ACLs and IAM Roles for any unauthorised entries if required [AWS Only].
- Engage an outside auditor to review the platform if required.

Where practical clients must be kept informed by management.

2.3 Documenting incidents

ISO 27001 Sections 13.02.01

Where an incident of any kind has occurred it should, in addition to the steps described above, be fully documented. In the immediate term the person making the discovery or accepting the report of the discovery should create a helpdesk ticket describing:

- The description of the incident.
- The services impacted and their severity.
- How the issue was discovered.
- Any relevant details such as error messages or log entries.
- Immediate steps taken to resolve the issue and secure any evidence.

This information will later be used as part of the root cause analysis of the incident.
Unless the issues calls for more urgent action the issues will be discussed with the product team at the next morning stand-up and appropriate decisions and subsequent actions described in the ticket. The issue will only be marked closed once resolved and any required root cause analysis has been completed and documented.

2.4 Incident review and discussion

ISO 27001 Sections 13.02.02

Significant issues shall be raised during the daily morning standup meeting as part of the normal helpdesk ticket review. A decision will then be made as to the scale of the review required and the planning of any remedial work outstanding.

3. Disaster (data) recovery [AWS Only]

3.1 Overview

This section is aimed at the AWS based infrastructure. Where a third party host is involved they will typically be responsible for disaster recovery and will have their own processes to follow.

3.2 Target data

Data considered to be critical from a disaster recovery point of view includes:

- Critical: Database (data store) content for each user stored in Amazon RDS.
- Important: Original file or image data for each client stored in Amazon S3.

Nearly all other resources, including codebase and search indices, can be recovered by re-running our normal deployment procedures.

Be sure to identify these items in detail as it may vary from project to project.

3.3 Database backups (Amazon RDS)

ISO 27001 Sections 10.05.01

- Amazon RDS instances are configured as Multi-Zone instances for near-instant failover should an instance fail.
- Amazon's automated backup tool is used to provide incremental backups for the database service.
- The backup process takes a daily snapshot of the data and also records transaction logs to retain point-in-time recovery support.
- The RDS backup process is explained in more detail at http://aws.amazon.com/rds/faqs/#23
- Snapshots are retained for 7 days.
- Backups are tested for viability at least once annually by a member of the development team in addition to AWS' own compliance testing requirements.

3.4 Object backups (Amazon S3)

ISO 27001 Sections 10.05.01

- Amazon's S3 service provides versioning support to revert any changes or deletions to objects store within.
- More information is available under the Data Protection heading at http://aws.amazon.com/s3/faqs/