HOUSERS
SMART INVESTMENT

Content

BUSINESS CONTINUITY POLICY

1. Introduction

The purpose of the IT Service Continuity Plan is to define precisely how HOUSERS will recover or continue the operation of IT services, applications, systems, or components at the level agreed in the business requirements.

This plan applies to all critical activities within the scope of the IT Service Continuity Management System.

The users of this document are all staff members, both internal and external, who have a role in IT service continuity.

2. Responsibility for the implementation of the Business Continuity Policy

The working teams, their activities and members are composed according to the following table:

Teams	Functions	Members
Team Manager	Lead activities during contingency and recovery. • Analysis of the situation. • Activation or not of the recovery plan. • Monitoring of the recovery process. • Damage assessment.	CTO (leader) Systems Manager
Recovery Team	Restore all core IT services which are: • MariaDB database service • API service • Front-end web service • Admin web service • Blogs web service	CTO (leader) Systems Manager (deputy) Software Development Assistants

	• Communication management microservice • Document management microservice • Payment microservice • Notifications microservice • Housers office file server	
Test Team	They will perform operational verification testing of core IT services. Each profile should have a verification test plan which should be submitted to the recovery team.	Head of Software Quality (CTO) Software Development Assistants

3. Incident identification

The risk assessment evaluates the level of the threat (i.e., disruptive incident) and the extent to which HOUSERS is vulnerable to that threat. The risk assessment is implemented through the Risk Assessment and Treatment Table. The risk assessment process is coordinated by the CTO and the risk assessment for individual services is performed by the service managers.

3.1. Levels of incident categorisation:

Insignificant consequence	1	The duration of the disruptive incident does not significantly affect the organization's finances, legal or contractual obligations or reputation.
Acceptable consequence	2	The duration of the disruptive incident causes damage to the organization's finances, legal or contractual obligations or reputation, but such damage is still acceptable considering its magnitude and specific circumstances.
Major consequence	3	The duration of the disruptive incident causes damage to the organization's finances, legal or contractual obligations or reputation, and that damage are not acceptable in its magnitude and specific circumstances.
Catastrophic consequence	4	The duration of the disruptive incident causes major damage to the organization's finances, legal or contractual obligations or reputation that will cause it to lose most of its capital and/or must permanently shut down its operations.

3.2. Types of alerts

1. Alerts derived from service monitoring
   a. Drop or slowdown of server response level due to a Denial-of-Service attack.
   b. No response from the server due to the failure of the isp connectivity.[1]

[1] **ISP details:** Amazon webservices (AWS) hosts the following services:
- API
- MariaDB
- Web front
- Web admin

c. Failure of API connectivity to LemnonWay
d. DB system crash

2. Alerts derived from active security monitoring
    a. Notifications from the early warning centre
    b. Alerts from periodic security audits
3. Alerts derived from the error in platform functionalities
    a. associated with the operation of investors
    b. associated with its administration panel

4. Procedure for reporting incidents

4.1. Active monitoring system

- Through the Teramonitor system activated with the deployment of the infrastructure on AWS, all events related to the operation of the infrastructure as well as its maintenance and backup are monitored in real-time.
- The monitoring service is located at Amazon Web Services' Paris node, while the Pro services are in Frankfurt and the development services in Ireland.

4.2. Alerts derived from service monitoring

a. Drop or slowdown of server response level due to Denial-of-Service attack; reports:
    a. Downtime alert by email to the Housers support account through an external monitoring system (Uptimerobot). The communication occurs at the time of the fall, it is immediate and automatic.
    b. In the case of slowdown, communication by users of the platform or Housers employees. The communication occurs when a user detects the drop in performance.
b. No response from the server due to isp connectivity down; reports:
    a. Downtime alert by email to the Housers support account through an external monitoring system (Uptimerobot). The

communication occurs at the time of the fall, it is immediate and automatic.

b. Downtime alert issued by the external systems department (provided by the company Teralevel) based on the alerts received from the Teramonitor monitoring system. This alert is issued either via e-mail or through the specific support channel that both companies share in Microsoft Teams.

c. API connectivity failure with LemnonWay; reports:
    a. Alert of connection failure with LemonWay via email to Housers support account sent by the API. The communication occurs at the time of the outage, it is immediate and automatic.

d. Blocking of the DB system; reports:
    a. DB connection failure alert via email to Housers support account sent by the API. The communication occurs at the time of the outage, it is immediate and automatic.
    b. Downtime alert issued by the external systems department (provided by the company Teralevel) based on the alerts received from the Teramonitor monitoring system. This alert is issued either by e-mail or through the specific support channel that both companies share in Microsoft Teams.

4.3. Alerts derived from active security monitoring

e. Notifications from the early warning centre; reports:
    a. Sending an email notification of vulnerability to Housers' support email. Automated and immediate sending upon detection of the fall.

f. Alerts derived from periodic security audits; reports:
    a. Sending the report derived from the security audits to the Housers CTO's email.

4.4. Alerts deriving from errors in platform functionalities

g. associated with investors' operations; reporting:

a. Failure alert via email to Housers support account sent by the API. The communication occurs at the time of the outage, it is immediate and automatic.

b. Direct notification through the web support form by Housers users or through the external support system (Freshdesk) communicated by Housers employees. Communication occurs when a user detects the problem.

h. associated with its administration panel; reports:

a. Failure alert via email to Housers support account sent by the API.

b. Direct notification through the external support system (Freshdesk) by Housers employees. Communication occurs when a user detects the problem.

5. Response to reported incidents

The CTO is responsible for ensuring continuity of operations.

5.1. Reaction times:

Type of incident	**severity**	**Reaction time**
Insignificant consequence	1	24-48 h.
Acceptable consequence	2	24-48 h
Major consequence	3	The immediate reaction after communication
Catastrophic consequence	4	The immediate reaction after communication

5.2. Information backup and recovery systems:

- The cluster of servers in Amazon Web Services Cloud environment:
    - Production services are deployed and distributed across the 3 AWS nodes located in Frankfurt. The backup and development services are deployed and distributed across the 3 AWS nodes located in Ireland. Finally, the monitoring and control services are deployed in the 3 AWS nodes located in Paris. In this way, the integrity and stability of the services are guaranteed, and if one of the nodes is down, the service can be recovered on any other node or even migrated to one of the other 2 zones.
    - Database system
        - The infrastructure has 2 environments: a production environment deployed in Frankfurt and a development environment deployed in Ireland.
        - Each of these environments has 2 database clusters: a MariaDB cluster with 3 nodes and a MongoDB cluster with another 3 nodes.

- Database backup:
    - Real-time synchronization between the nodes of the database cluster. This system prevents crashes on any of the 3 nodes on which it is implemented and allows operation even with only 1 of the 3 nodes.
    - A full copy of the database is made every day. Once the copy is made, it is mounted on the development database server, located in the Ireland node of Amazon and the integrity of the content is checked. Additionally, the backup is also sent to the Amazon S3 storage system (Frankfurt Node) and to the NAS located in Housers Madrid offices, which guarantees business continuity in case of any contingency.
    - The system has an uninterrupted daily copy history since the deployment of the infrastructure on AWS.

5.3. Banking information and user documentation

- The platform's transactional files (client and project documentation) are stored in Amazon's S3 service, which has all the data loss protection and information security systems that a giant like Amazon can provide. These files are in the Frankfurt node of S3, which in turn is made up of 3 nodes so that a fall in one of them does not affect the persistence or the normal operation of the system.
- In addition to the backup systems described above, all wallet and investor information is replicated in Lemonway's system, which in turn has its business continuity and backup systems.

5.4. Backup of source code

- The platform's source code is backed up in two layers: in each developer's local Git service and an external Git service.

5.5. The procedure of the response process:

  - Identification of the triggering event of the occurrence
  - Scope of impact analysis:
    - Identification of affected services
    - Identification of affected users: anonymous users, investors, platform administrators, ...
    - Affectation of data: data tables, historical data, logs, ...
    - Temporal impact: identification of problems arising from the impact before its detection.
    - Identification of possible vulnerabilities in the system.
  - Analysis of the proposed solution:
    - Analysis of the checkpoint from which the solution is proposed: the creation of a new branch for a hotfix and data backup.
    - Analysis of the code developed to solve the problem.
    - Analysis of the relationship of this code with the rest of the system services.
    - Analysis of the resulting data.

- Analysis of the security of the system once the solution has been applied.

- Evaluation of the response:
  - Proposal of actions to be taken to avoid the recurrence of the incident.
  - Proposal for refactoring the affected service if necessary.
  - Analysis of time and resources dedicated to the resolution.
  - Evaluation of the impact on the various departments: Customer Care, Marketing, Real State, Financial, Legal, Institutional.
  - Evaluation of the impact on the company-customer relationship.
  - Assessment of the impact on the reliability of the company.
  - Development of a complete report of the incident.

6. Follow-up and archiving

We have implemented an incident reporting and tracking system through Freshdesk. This system allows the declaration, monitoring and archiving of all incidents declared for subsequent review.
After the incident has been resolved, the causes that originated it and the possible preventive measures to be taken are analysed, as well as the possible updates that may be derived from these conclusions to be integrated into the response process.

7. Frequency of updates

The active monitoring system through Teramonitor enables real-time threat detection and the implementation of measures to prevent risks and correct vulnerabilities.