Huis Technologies IT Disaster Recovery Policy

Date: 30/08/2026

Review date: 30/08/2027

1. Purpose

The purpose of this policy is to establish a structured approach to ensure the swift recovery of critical IT systems, applications, and data in the event of a disaster or disruption. This policy sets out how we minimize downtime and data loss, ensuring continuity of operations. Huis Technologies Ltd is committed to maintaining a disaster recovery plan to ensure the availability, integrity, and security of IT systems and data. All employees and stakeholders must adhere to this policy and associated procedures.

This policy is reviewed and updated annually and when changes are made to our systems or devices. Policy updates are reviewed and implemented by the Managing Director and Technical Director. Dates for the next planned review are detailed at the top of this policy.

2. Scope

This policy applies to all IT systems, services, and data managed by Huis Technologies Ltd, as well as to all employees, contractors, and third-party vendors involved in maintaining these systems.

3. Definitions

3.1. Disaster: Any event causing significant disruption to IT systems, such as natural disasters, cyberattacks, hardware failures, or power outages.

3.2 Recovery Time Objective (RTO): The maximum acceptable downtime for a system or service.

3.3 Recovery Point Objective (RPO)**:** The maximum acceptable amount of data loss measured in time.

3.4 Critical Systems: IT systems deemed essential to organisational operations.

4. Roles and responsibilities

4.1 The Technical Director is responsible for the development, testing, and execution of the disaster recovery plan. The Technical Director is also responsible for identifying critical systems, setting RTO and RPO and for ensuring system documentation is maintained.

4.2 The Managing Director is responsible for ensuring that all employees are briefed on the contents of this policy and for ensuring transparent, prompt and efficient communication with relevant stakeholders/customers/users in the event of a disaster.

4.3 Huis Technologies Ltd employees are responsible for reporting incidents, cooperating during recovery efforts and maintaining system documentation where appropriate to their roles.

5. Risk Assessment and Business Impact Analysis

Huis Technologies Ltd conducts annual risk assessments to identify potential threats to IT systems. We perform a business impact analysis to prioritise critical systems based on RTO and RPO.

6. Disaster Recovery Plan (DRP)

Huis Technologies Ltd has developed and maintains a Disaster Recovery Plan with detailed recovery procedures for each critical system. The DRP includes contact information for customers and stakeholders as well as a list of risks specific to each.

Copies of the DRP are stored in multiple secure locations, including off-site and cloud-based repositories. Our DRP outlines the response times for each of three tiers [mission critical, business critical and important business] of services. The plan is tested quarterly in order to validate the response time for each tier. Failover tests are carried out as part of quarterly testing to ensure that failover times are below 60 seconds.

7. Backup Strategy

Huis Technologies Ltd ensures regular backups of all critical data and systems according to the RPO requirements. Daily point in time backups are made for 35 days, followed by weekly backups up to 12 months.

Backups are stored in a secure location via AWS Cloud Services in the UK and Republic of Ireland. Off site backups are stored in Frankfurt, Germany. Backup restoration procedures are tested quarterly to ensure data integrity.

8. Testing and Training

The Disaster Recovery Plan is tested annually to ensure effectiveness and identify areas for improvement. Regular training is provided to the Technical Director, Managing Director and relevant employees on disaster recovery procedures.

9. Incident Response

The IT Disaster Recovery Plan is activated immediately upon identification of an event likely to impact application service delivery. Events are categorised in three ways, each prompting a different response:

9.1 Mission critical: the disruption affects critical systems and impacts the ability of Huis Technologies Ltd to supply software services to its customers. This is the highest priority of disruption as it relates to critical tasks that must be performed by users of our software. Mission critical outages may threaten the immediate survival of a customers' organisation and are responded to with urgency.

9.2 Business critical: the disruption affects Huis Technologies Ltd's capacity to provide the level of service expected by its customers, but does not affect customers' capacity to access or use critical software services. Disruption may impact some customers' capacity to perform certain tasks, but does not threaten the immediate survival of a customers' organisation. Business critical outages are responded to as a matter of high priority.

9.3 Important business: the disruption affects a single non-critical element of the software rather than critical systems. Huis Technologies Ltd may risk reputational damage, but there is no immediate threat to the survival of a customer's organisation. Important business outages are responded to as medium priority.

9.4 Mission critical events are prioritized to ensure critical systems can be restored quickly and with as little disruption to customers as possible. The process for responding is outlined below.

All issues	
1.	Employees and.or users report an issue to the Technical Team and/or the Technical Director.
2.	The Technical Director takes steps to assess the extent of the issue & determine the nature and scope of the IT failure (e.g. network outage, cyberattack) and informs the Managing Director.
3.	The Technical Director evaluates the impact of the IT failure by assessing the affected systems, services, and users. The Technical Director prioritises based on criticality as outlined below:

Mission Critical	**Business Critical**	**Important Business**
4. The Managing Director informs stakeholders/ customers immediately. The support team contacts users to inform them of the issue and sets a schedule for updates.	4. The support team informs the individual users/stakeholders who are affected. The support team provides an estimate for a resolution of the issue.	4. The support team informs the stakeholder/customer and asks them to make any affected staff aware in the first instance.
5. The Technical Director takes steps to minimise disruption	5. The Technical Team begins resolving the issue and	5. The Technical Team begins resolving the issue and

by (for example, by disconnecting affected systems from the network, if necessary).	provides a workaround in the first instance where this allows users to continue to perform tasks. A workaround is usually provided within 1 working day.	provides a workaround in the first instance where this allows users to continue to perform tasks. A workaround is usually provided within 2 working days.
6. The Technical Director addresses immediate vulnerabilities (e.g., stop a cyberattack or apply patches).	6. The Technical Team provides an estimate for when the issue will be resolved fully and this is communicated to users/stakeholders via the support team. The issue is usually fully resolved within 5 working days.	6. The Technical Team provides an estimate for when the issue will be resolved fully and this is communicated to users/stakeholders via the support team. The issue is usually fully resolved within 10 working days.
7. The Technical Director ensures that evidence is preserved. For cyberattacks or compliance-related incidents, logs and evidence are preserved for analysis.	7. Once the issue is resolved, users and stakeholders are informed by the support team.	7. Once the issue is resolved, stakeholders/customers are informed by the support team and asked to update users within their organisation.
8. The Technical Director executes recovery procedures [retrieve data and applications from the most recent backups, rebuilds systems and tests to verify restored systems work as expected.		
9. Operations resume. Systems are brought back online incrementally to ensure stability, monitoring for performance issues, errors, or recurring problems.		
10. The Managing Director informs stakeholders/customers that systems are restored. The support team informs users.		

10. Incidents that require a disaster recovery plan response are recorded and reviewed post-recovery to improve future responses. A root cause analysis (RCA) takes place in order to fully investigate the cause of the failure to prevent recurrence. Records are kept of actions taken, timelines, and lessons learned and these inform changes to the IT Disaster Recovery Plan.

11. Vulnerabilities are addressed post-recovery from a mission critical or business critical incident including identification of systemic weaknesses. Where appropriate, additional system monitoring is deployed and staff training is reviewed and refreshed.

12. For mission critical events, a full investigation is carried out and copies of the report are sent to stakeholders. Where appropriate, the Technical Director and Managing Director may

also self-refer within 72 hours to the Information Commissioner's Office in the event of a suspected or actual data breach. The outcome of any ICO involvement is also communicated to stakeholders.