Information Technology Disaster Recovery Plan (IT DRP)

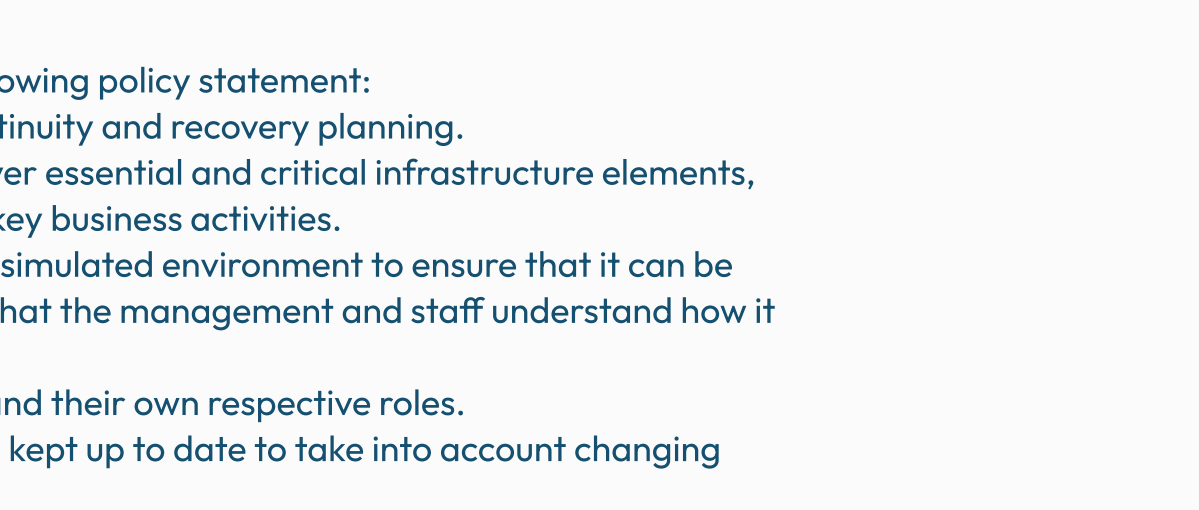
Jordan Ffolkes
Last reviewed & tested – 23/09/2025

Introduction

This document details the policies and procedures of Recognise Design Limited in the event of a disruption to critical IT services or damage to IT equipment or data. These processes will ensure that those assets are recoverable to the right level and within the right time frame to deliver a return to normal operations, with minimal impact on the business.
Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

Purpose of policy

Corporate management has approved the following policy statement:
- The company shall implement relevant continuity and recovery planning.
- All continuity and recovery plans should cover essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The plans should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the plans and their own respective roles.
- The continuity and recovery plans are to be kept up to date to take into account changing circumstances.



Business impact analysis

This business impact analysis to be used when doing the planning work for the first time.
The first section is about identifying important IT-services needed for the business including the business impact if interrupted. The second section helps when identifying the business needs regarding availability, recovery times, backup, data integrity and data confidentiality.

Business process/delivery	Supporting IT-service	Impact when interrupted, incl time when it becomes unacceptable
Finance	IT-system B	Will stop invoicing and reporting immediately, unacceptable after 24 hours.
HR	IT-system C IT-system B	Will mean use of prepared manual procedures, unacceptable after 48 hours.
All business staff	Email system	Will impact productivity immediately, unacceptable after 4 hours.

Business process/delivery	Business process/delivery				
	Availability	RTO	RPO	Data integrity	Data confidentiality
IT-system A	99,7%	4 h	10 min	Very high	Low
IT-system B	99,5%	24 h	24 h	Very high	High
IT-system C	99,5%	48 h	24 h	Very high	Very high
Email system	99,5%	4 h	12 h	Very high	Medium

The Recovery Time Objective (RTO) is the time frame agreed upon to get the business process/delivery operational again after an IT-interruption (including all IT recovery actions).
The Recovery Point Objective (RPO) is the acceptable amount of data you can lose in an incident without being able to recover it. Recover to a previous "point in time". Sets the demands on backup/restore/replication solutions.
Data integrity is the demand that information stays intact and isn't changed intentionally or unintentionally.
Data confidentiality is the demand that ensures that information is not made available or disclosed (intentionally or unintentionally) to others.

Robustness analysis

Contact the individual responsible for each IT-service in-scope for the planning work. Have an extensive discussion about the business need and what is covered in the service today.

Action	Description	Implementation plan
Change the backup solution	Identify new solution for IT-system A in order to meet the business need of Recovery Point Objective	Analysis done in 01/07/2022
RTO email system	Discuss the cost for a shorter Recovery Time Objective with the supplier	Discussion 01/07/2022
Secure erase of hard disks when replaced	Discuss a solution with tech team in order to erase all hard disks in a secure way when replaced (for all systems with high or very high confidentiality demand	Discussion 01/07/2022

Recovery planning section

This part of the business continuity plan covers preparations to handle IT-interruptions in an efficient way and reduce the impact on the business.

Key personal contact details

Name, Title	Contact option	Contact number
Jordan Ffolkes	Work	07791259731
	Mobile	07791259731
	Home	01920460168
	Email address	jordan@recognisedesign.com
Abel Beyene	Work	+44 7508 046656
	Mobile	+44 7508 046656
	Home	01920460168
	Email address	Abel.beyene@recognisedesign.com

Prepared DR procedures

Depending on the incident, one or more of the following disaster recovery procedures may be activated:

DR plan for Ransomware

Scenario	First aid equipment and first aid help, including accident/injuries logbook entries and RIDDOR reporting
Possible causes	Malware
IT services and data at risk	Storage systems and laptops
Impact	Lost or corrupted data
Prevention	• Identify potential weaknesses of our network and IT environment. • Implement the use of VPN connections for all mobile employees
Prevention	• Employees that service critical IT services should have the maximum access required to be able to complete their job. • Implement a backup and recovery plan for all vital data using the 3-2-1 Strategy: 3 - Retain a minimum of three copies of data. 2 - Store data on two different types of media. 1 - Secure one copy of your backups offsite. • Test backups regularly to ensure proper configuration, which will limit the impact of a data breach and accelerate the recovery process. • Isolate critical backups from the network (air gap) for maximum protection. • Implement copy-on-write file systems (NetApp WAFL – Linux ZFS) or WORM features in NAS systems or appliances. • Patch critical operating systems, antivirus, security, and backup software as soon as possible. • Establish ongoing cybersecurity training for users and admins to identify phishing emails.
Plan of action	• Disconnect all ransomware-affected systems from the network. • Never pay the ransom! Paying the criminals doesn't guarantee that you will get your data back. In many cases (and most definitely, if it is a "ranscam' or wiper malware) you will not get your data back, leaving you with no data. • Do not try to decrypt the data by yourself. Contact Abel Beyene for advice. • Check your backups. Even if your backup is missing after a ransomware attack, you should never rule out the possibility of recovery. Possible solutions depend on the type of media or storage system, and the type of ransomware. • Identify the issue, coordinate initial response. • Seek advice immediately by contacting Abel Beyene. • Follow the instructions in detail.
Key contacts	• Jordan Ffolkes • Abel Beyene

DR plan for virtualised systems

Scenario	Data loss situations in virtual systems
Possible causes	• Lack of time: Every second IT employee lacks the time to regularly document procedures and processes. • Continuing to work on an affected system after a data deletion has occurred. • Drive failures and RAID operating system issues. • Deleted or missing virtual machine/VMDK. • Corrupt VMFS Metadata or inaccessible Datastore. • Corruption inside Guest OS. • The data backup processes are outdated.
IT services and data at risk	Storage systems that support virtual machines
Impact	Lost or corrupted data
Plan of action	• Administer proper backup for all systems that contain virtual machines. • Never work on an affected system where an accidental data deletion has occurred. • Ensure all backup processes are up to date and have an emergency data recovery plan in place. • Restore lost data to a secondary system to protect against further data loss. • Do not run FSCK or CHKDSK file system repair tools on a virtual disk unless backups have been tested, by restoring to a secondary device. • Ensure that you have an updated contingency plan with best practise for data recovery, and contact details to trusted experts.
Key contacts	• Jordan Ffolkes • Abel Beyene

DR plan for RAID-systems

Scenario	Data loss situations in virtual systems
Possible causes	**Human error** • Whether by accident or carried out with malicious intent, data loss from reformatting, reinstalling, or overwriting volumes can be typically be overcome by expert data recovery engineers. **Power issues** • RAID systems can be affected by a loss of power, power cycling, and power surges, causing a loss of data. RAIDs running in a degraded state are especially vulnerable, as power issues can cause out of-sync drives to be reincorporated into the array **Mechanical issues and failed rebuilds** • RAID systems are built to withstand individual drive failures, but once a RAID is running in a degraded state, the workload of the remaining drives increases, and so does the risk of secondary drive failures. Additional drive failures can lead to a complete failure of the RAID. **Natural Disasters** • Fire, water, dirt, and other contaminants from natural disasters can destroy disks in an instant.
IT services and data at risk	RAID systems
Impact	Lost or corrupted data
Plan of action	**Do not run CHKDSK** • CHKDSK can be beneficial for single drive systems experiencing minor corruption, as it helps maintain file systems in a stable state. However, in most situations, inconsistencies found in volumes stored on RAID systems stem from issues at the RAID level, such as out-of-sync drives or problematic rebuilds. Therefore, executing CHKDSK in these cases may lead to harmful and irreversible alterations to the file system structures. **Never replace a failed drive with a drive that was part of a previous RAID system;** • always zero out the replacement drive before using. **If a drive is making unusual mechanical noises, turn it off immediately.** • A mechanically failing drive that is still in use can increase the severity of the data loss and reduce the chances of a full recovery.
Plan of action	• Verify backup copies of data before making hardware or software changes. • Label the drives with their position in a RAID array before removing them from your system. • If a RAID system fails in the middle of a rebuild process, do not run further rebuild attempts. • In a power loss situation with a RAID array, if the file system looks suspicious, is un-mountable, or the data is inaccessible after power is restored, do not run volume repair utilities.
Key contacts	• Jordan Ffolkes • Abel Beyene

DR plan for single HDD and SSD

Scenario	Data loss situations of single drives
Possible causes	**Mechanical failures** • If your hard drive is not working or is making clicking and/or grinding noises, it is likely experiencing a mechanical failure. This could be due to a head crash and/or motor failure. **Logical failures** • If your hard drive is working,but you cannot access some, or other files, then it is experiencing a logical issue. This could be due to a lost partition or accidental reformatting of the drive.
IT services and data at risk	User data stored locally on a single drive
Impact	Lost data
Plan of action	**Power off** • Turn off the power to the computer or storage device to prevent further damage. **Water damage** • DO NOT DRY IT OUT. Corrosion to the media begins with drying and increases loss of data. Place the hard drive in an airtight ziplock bag and send it as soon as possible to an Recognise Design office for hard drive data recovery services. **Strange noises** • Turn off the power. If your hard drive is making strange clicking or grinding noises, it could be a sign that your drive might have experienced a head crash and is not reading the data correctly. A head crash can result in permanent, unrecoverable damage to your files if the drive continues to run.
Plan of action	**Missing, reformatted or deleted files** • Whether it was an accidental deletion or if your files have gone missing, Recognise Design data recovery software might be your answer.
Key contacts	• Jordan Ffolkes • Abel Beyene

Revision history

Version	Date	Revision details
1	01/07/2022	N/A

www.recognisedesign.com
Company Number 08633423