



# DISASTER RECOVERY PLAN

INFIGO SOFTWARE

1<sup>st</sup> Floor, Suite 2, Belgrave House,  
Station Way, Crawley, RH10 1HU

[www.infigosoftware.com](http://www.infigosoftware.com)

EXTERNAL VERSION 1.1

13/10/2020



## TABLE OF CONTENTS

TABLE OF CONTENTS .....	2
1. High-Level Outline of Disaster Recovery Plan.....	3
2. Key Personnel and Contact Information .....	3
3. Recovery Plan.....	4
4. Recovery Plan Practice and Exercising.....	5



## 1. HIGH-LEVEL OUTLINE OF DISASTER RECOVERY PLAN

These are the major goals of the disaster recovery plan.

- Minimize interruptions of normal operations
- Limit extent of disruption and damage
- Minimize economic impact of the interruption
- Establish alternative means of operation if required
- Train personnel in emergency procedures
- Provide smooth and rapid restoration of service

Infigo operates various IT environments for the individual geographical areas and purposes. Main goal would be ensure the live environments are available, operational and uncompromised.

## 2. KEY PERSONNEL AND CONTACT INFORMATION

These are the key resources involved in the disaster recovery plan, including all key stakeholders and third-party resources.

NAME & TITLE	ROLE
Altaf Balotrawala	System Analyst
Michael Zauner	CTO
Alex Howell	Technical Operations Director
Roman Gherman	Moldova Head of Development
Pablo Cubillas	Development and Release Manager

### 3. RECOVERY PLAN

This is the relevant information needed to continue recovery plans

Recovery options depending on situation and severity:

Action	Data	Downtime	Time	Notes
Restore Backup	Lost up to last backup point	Optional	2 hours	Can be done for individual groups
Restore Data	Granular control what to restore	Optional	1-6 hours	Specific error cases
Redeploy	No data loss	No	40 minutes	Replaces Web/Application servers
Recreate environment except LB/GA	No data loss	Yes	4-6 hours	With extra backup
Recreate whole environment	No data loss	Yes	8 hours	With extra backup Client DNS would have to be reconfigured
Recreate whole environment with backup Except LB/GA	Lost up to last backup point	Yes	4-6 hours	
Recreate whole environment with backup	Lost up to last backup point	Yes	4-6 hours	Client DNS would have to be reconfigured
Recreate environment on new account	Depending on the backup option chosen, potentially no data loss	Yes	5-7 hours	Client DNS would have to be reconfigured

Optional we can perform the following actions:

- Disable a single platform
- Disable Loadbalancer to stop external access
- Setup IP restrictions for Platform/Environment
- Recycle application pools
- Restart server

#### 4. RECOVERY PLAN PRACTICE AND EXERCISING

This is the plan that should be carried out to practice and prepare for an emergency.

Action	Interval	Responsible
Restore Backup	Once a year	System Analyst
Restore Data	Once a year	System Analyst
Redeploy	Weekly	N/A
Recreate environment except LB/GA	Once a year	System Analyst
Recreate whole environment	Once a year	System Analyst
Recreate whole environment with backup Except LB/GA	Never	N/A
Recreate whole environment with backup	Never	N/A
Recreate environment on new account	Monthly	System Analyst