PERIMATICS

13701 NE Bel-Red Rd, Suite 103
Bellevue, WA 98005
https://www.perimatics.com

DISASTER RECOVERY POLICY

1. OVERVIEW

Perimatics solutions are implemented at hospital sites with the goal of aiding surgeries with AI, data science and decision support. Our solution architecture is such that all processing takes place at the customer site. Disasters at our work facilities are unlikely to impact customer site performance.

We are putting the disaster recovery policy to ensure that it covers basic disasters in infrastructure and physical facilities. This is a living document that will evolve as our solutions evolve.

2. PURPOSE

This document details the policies and procedures of Perimatics 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 timeframe to deliver a return to normal operations, with minimal impact on the business.

3. TARGET ASSETS

- Development infrastructure: This includes source code, test data, versioning information.
- Customer information and documents: Contract documents and contacts.
- Communications within the company and with customers: Email and related documents attached to emails.
- Network access to Internet

4. RECOVERY POLICY

The table below summarizes the need for recovery of each of the assets and how it will be accomplished:

Disaster related failure in	**Need for recovery**	**Process for recovery**	**Owner**

Development infrastructure	Development assets are stored in the cloud (GitHub) and benefit from geo-distributed backups. Facility disasters at our office will not affect this.	Redownload source code and other development assets from GitHub	Dev Lead
Customer Information	Contracts are contact information are backed up offsite.	Use backups from the offsite facility.	COO
Communications	Communications within the company and with customers is primarily done over email. Our email infrastructure is Office365 with offline copy of all email being stored on individual computers by the email owners.	Recover email from Office365. Continue communications from backup machines. If Office365 service is hit by the disaster, use other communication mechanisms such as phone and other email accounts.	All
Network Access	Network access to Internet is currently through CenturyLink Business infrastructure.	Use alternative connection facilities such as mobile hotspots and network infrastructure available at team members' homes.	All
Physical facility	Place for the team to work	Until the disaster passes, team members will work from alternative facilities like their homes.	All

5. Testing schedule

- The disaster recovery plan will be tested in its entirety once every 12 months

6. PLAN REVIEW

- The plan will be formally reviewed once every 12 months and in response to regular testing and evolving needs.

7. POLICY VERSION HISTORY

Version	Date	Description	Approved By
1.0	5/1/2018	Initial Policy Drafted	COO