iptor
A GENII COMPANY

IPTOR CLOUD MANAGED SERVICES | SEPTEMBER 2022

IPTOR.COM OPERATIONS POLICY

CONTENTS

SCOPE

This Iptor Operations Policy (the Policy) outlines standard operations in Iptor cloud managed services. General support including incident and service request management is described in Iptor Support Policy.

NB! This Policy does not constitute an agreement between Iptor and its customers. Major changes to this document will be communicated to Iptor customers through a bulletin or in another prominent way.

Iptor
P.O. Box 1350, Hemvärnsgatan 11 | SE-171 26 Solna, Sweden
T +46 8 627 2300 | iptor.ms@iptor.com | iptor.com

1. DEPLOYMENT OF IPTOR.COM (IDC)

Iptor.com is deployed on IBM cloud. IBM cloud has a word wide coverage. We have the possibility to deploy setup in different locations.

We have predefined three locations:

- Frankfurt
- Dallas
- Sydney

Each of these locations exist of three or more zones. A zone is a physical location. These zones are with a minimum of 10KM separated from each other.

The zones and locations are connected via the IBM network We have prepared all the necessary network setup to activate these locations.

2. IPTOR STANDARD BACKUP PROCEDURES

IDC has the following back-up

- Daily we run incremental back-ups with a retention of 7 days
- Weekly we run full back-up of the data drives with a retention of 7 days
- Monthly we run full back-up of the data drives with a retention of 370 days
- Yearly we run a full back-up the data drives with a retention of 370 days

Snapshots for quick recovery

- We do take snapshots daily with a retention of 3 days

The status of the back-up is checked daily.

3. IPTOR STANDARD MONITORING SERVICE

Iptor monitors IDC 24/7 and all logs are collected centrally.

4. IPTOR STANDARD UPGRADE POLICY

The system is as much as possible upgraded without impacting the customers.

- PowerVS ones a quarter (when a new PTF is release from IBM)
- Linux weekly
- Windows Weekly
- Openshift once a quarter
- Checkpoint when an update is released
    - Major updates when delivered and planned within a month

5. SYSTEM MANAGEMENT

- System shall be capable of operating 24 hours a day within the Availability Percentage commitment as set forth in the contract.
- Iptor is performing regular service and maintenance on the System as per this Policy unless other stated in the contract. Iptor will reserve at least one service window per Month to have a possibility to perform patching of the System, and Customer must accept service windows accordingly.

- Iptor plan the patching window, as far as possible, to be close to the respective vendors release date but with a decent delay added for planning and to ensure that proper change management processes can be followed.

- Iptor will strive to minimize both Scheduled Downtime and Unscheduled Downtime for the Customer's business. Regular maintenance is performed by Iptor with the goal to minimize overall downtime, interference with System Services, and security risks. The regular maintenance is carried out in planned service windows. When maintenance is performed within a service window, Scheduled Downtime can be needed during a certain time of the service window.

- Service windows for maintenance of common resources for all Iptor customers are scheduled annually by one point per month. Iptor plans for 10 shorter service windows, lasting up to 6 hours, and 2 longer service windows, lasting up to 36 hours. Iptor shall provide Customers with at least 6 days advance notice for the shorter service windows and 30 days prior notice for the longer service windows, informing if the service window will be used and any expected effect with respect to IDC (with estimated time of the Scheduled Downtime).

- Iptor strives to plan maintenance service windows so that Scheduled Downtime occurrences are limited. However, occasions may arise when Iptor proactively must perform maintenance in scheduled service windows but will not be able to announce such service window within 6 or 30 days in advance, in order to avoid critical situations for IDC. At these times, Iptor will provide at least one (1) weeks' notice to Customer that such maintenance should be done and how the Customer will be affected.

- In the case a third party vendor recommends installing a patch or fix for resolving an emerging critical incident and solution affects more services than the current incident does, Iptor will follow the recommendation if it is in reasonable proportion to the incident. This will be an emergency service window to solve an incident and Iptor will provide as much notice to Customer as possible. Iptor conducts maintenance in consultation with affected customers with service maintenance information to be provided to Customer as quickly as possible after.

6. SECURITY MANAGEMENT

IDC has multiple security layers in place. First of all we use a central place for authentication of all customer users. The IBM cloud is protected by the standard IBM firewalls in addition to this we have setup an additional layer of protection with Checkpoint firewalls end user protection on the systems. For entering the systems we use the Internet services (cloud flare) to protect the application against ddos and hackers. Within the IDC and IBM cloud we have deployed Hyper Protect Crypto Service.