# IT Disaster Recovery Policy

| | |
|---|---|
| Document Type | Policy |
| Document owner | Jonas Bruun Jacobsen, Chief Technology Officer, BeCause ApS |
| Approved by | Management Board |
| Approval date | January 2022 |
| Review date | June 2022 |
| Version | 2.0 |
| Amendments | June 2022 |
| Related to | IT Security Policy |

## 1 Scope

This policy applies to all staff, contractors, students and interns at BeCause ApS. and all BeCause ApS Managed IT Services.

## 2. Purpose and overview

This policy provides a framework to define the ongoing process of planning, developing and implementing IT Disaster Recovery management for BeCause ApS.

It defines the current methods of management and mitigation of IT systems and services, including data on behalf of BeCause ApS.

It provides an overview of the system approach that should be taken in order to safeguard the critical technology and data managed by IT Services at BeCause ApS, and how that approach should be implemented.

## 3. Policy

### 3.1 Introduction

This policy provides a framework to define the ongoing processes of planning, developing, and implementing IT Disaster Recovery management for BeCause ApS. It defines the current methods of management and mitigation of IT systems and services, including data on behalf of BeCause ApS. A disaster is defined as a serious incident that cannot be managed within the scope of BeCause ApS's normal working operations.

### 3.2 Requirement for the Policy

This policy provides an overview of the systematic approach that should be taken in order to safeguard the critical technology and data managed by IT Services at BeCause ApS, and how that approach should be implemented.

### 3.3 Definitions

*Disaster Recovery Operations*

- All activities and steps necessary to restore systems services that are affected by a disaster.
- All activities concerned with management and user communications related to the disaster.
- All activities concerned with the mitigation of the impact of an ongoing disaster incident.
- All activities concerned with the follow-up to an incident

*Disaster Recovery Management*

- Identify critical and secondary systems based on risk assessment.
- Establish baseline recovery time capabilities and objectives.
- Maintain and test DR capabilities on an ongoing basis.
- Identify gaps between current and required capabilities for system recovery.

## 3.4 IT Disaster Recovery Policy Objectives

DR Management

This policy exists to minimize the impact of any significant incidents on BeCause ApS systems and services, to recover from the unavailability of those systems to an acceptable level, and to define the controls to do so (i.e. response and recovery controls)

In order to be able to achieve this there are 3 main objectives:

- Establish Operational Control of the Disaster (the War Room)
- Communicate with relevant parties impacted by the disaster (the Comms Plan)
- Activate a specific recovery plan(s) relevant to the situation (Run Books)

Disaster Recovery Planning

BeCause ApS IT Services shall conduct risk assessments and ensure scenarios, procedures and plans are developed and implemented for critical business systems to ensure timely resumption of essential services. These are known as Runbooks and should be made available to all technical IT that may need to be involved in service restoration (DR Teams) and will need to be regularly tested and updated as necessary. Copies of the Runbooks, and the Major Incident Plan should also be kept securely off-site and available out of hours.

Where critical services are outsourced, IT Services shall ensure that suppliers agree to have similar suitable plans and contingencies in place to meet the criteria for critical systems.

The provision of BeCause ApS IT infrastructure has to be a balance between affordability and availability, and it is therefore not possible to maintain fully redundant hardware in preparation for all or any potential disasters. BeCause ApS has their main data center in Microsoft Azure's EU West data center, located in the Netherlands. The Azure EU West datacenter is paired with the Azure EU North datacenter (located in Ireland) for cross data center resilience, where either data center has the capability to provide adequate operating services and redundancy in data in the case of the loss of a single data center. Disaster recovery is incorporated into the architecture of new systems that are deemed critical by the business, or so defined by their Service Level Agreement (SLA).

The recovery of a service is governed by the stated, agreed Recovery Time Objective (RTO) for each service, and the level of criticality of each system. A service is a collection of systems and devices that collectively support a business process. For all core BeCause ApS IT services the details for these are provided in the IT Services Catalogue section.

We group the criticality of each service into one of three different criticality levels with varying degrees of resilience and RTOs for the disaster recovery.

| | | |
|---|---|---|
| Tier 1 | A Tier 1 service is any critical system necessary to support the core operational delivery requirements of BeCause ApS. These services are defined by the management of BeCause, and supporting services are identified through further analysis by BeCause IT. | All Tier 1 services are resilient through redundancy across dual-data centers. Furthermore, they maintain their own copy of all data they require to ensure resilience, even if supporting services are failing. If any supporting service cannot be made non-critical for the Tier 1 service, the supporting service needs to be documented. The design recovery time objectives (RTO) for Tier 1 services are a maximum of 24 hours.<br>Significant changes associated with Tier 1 services must have documented and tested contingency plans - e.g. roll back plans, contingency services, extended change outage windows. |
| Tier 2 | A Tier 2 service is any other non-critical service operated or managed by IT Services as a production system for Company operations. | Tier 2 services have all their minimum essential services identified to ensure efficient recovery.<br>Tier 2 data shall be recoverable from backups.<br>Tier 2 services have a designed maximum recovery time objective (RTO) of 72 hours. |

| | | |
|---|---|---|
| | | Significant projects and changes associated with these services must have documented contingency plans. |
| Tier 3 | A Tier 3 service is one which the Service Owner defines as needing no resilience or failover, and which is not a critical supporting system. | These are services which are able to tolerate extended downtime of up to one week with no significant impact on operations.<br>They should be designed with manual workarounds where necessary via the provision of short term or temporary facilities to accommodate user requirements. |

The business criticality, infrastructure and supporting systems associated with each service should be identified and clearly defined to assign the correct criticality tier to the system. For each system, a Service Owner should be identified and recorded and the details of this responsibility documented. The Service Owner is listed in the IT Service Catalogue Section.

For each service, the following data shall be maintained by the Service Owner and approved by the CTO:

- Key service data: Service Owner, platform details, backup mechanism, recovery mechanism, service tier ranking.
- Key operational procedures for startup, shutdown and recovery of all systems associated with the service.
- Key contacts for suppliers, SLA details or maintenance contract details where relevant, and incident invocation and escalation procedures for the supplier.
- Documented testing and a full service test schedule.

The CTO shall be responsible for the collection, management and distribution of the DR Policy and Procedures. Service Owners and delegated systems administrators shall prepare and maintain procedures and plans as required under this policy.

Disaster Recovery Plan Testing
Where possible, disaster recovery documents, specifically this policy, the procedures and plans, shall be tested and updated to ensure that they are up to date and effective, especially following significant system changes.

System level testing, including the physical hardware when applicable is tested on a regular basis, to ensure that it operates as required and agreed with the service owner. Responsibility is assigned to Service Owners as identified by procedure to ensure that this is carried out in a correct manner.

Operational procedures shall be reviewed by Service Owners after significant or major changes to underlying systems, and testing of services shall coincide with planned major upgrades.

Test Frequency
BeCause ApS will perform the following DR testing (which is in addition to the testing requirements set out by each Service Owner for their individually owned services):

Full yearly DR scenario testing. The scenarios will be defined and agreed by BeCause IT Services and should be aligned to BeCause ApS' management as well.

### 3.5 Disaster Recovery Process

Disaster recovery management is incorporated in IT Services processes and structure:
The activities for disaster recovery management shall be coordinated by representatives from different parts of IT Services with relevant roles and job functions. This co-ordination involves the collaboration of several separate teams and is noted in detail in the IT Major Incident plan referenced above in the DR Management section.

## 4. IT Services Catalogue

| Service name or category | Criticality Tier | Service Owner |
|---|---|---|
| Customer-facing Bulk Search APIs | Tier 1 | Lasse Chris Aarøe |
| Customer-facing Widget and Widget APIs | Tier 1 | Jonas Bruun Jacobsen |
| Customer-facing Bulk Import APIs | Tier 1 | Lasse Chris Aarøe |
| Customer-facing Excel Bulk Import features | Tier 3 | Jonas Bruun Jacobsen |
| BeCause Sustainability Reporting features | Tier 2 | Rasmus Birkedal |
| BeCause Internal Statistics, Dashboards and Analytics features | Tier 3 | Rasmus Birkedal |
| BeCause remaining non-API platform features | Tier 2 | Jonas Bruun Jacobsen |

## 5. Contact Information

If you have any questions regarding our IT Disaster Recovery Policy, please find our contact details below:

BeCause ApS
Njalsgade 76
2300 Copenhagen S, Denmark
Corporate Identity Number: 39745267
Email address: privacy@because.eco