SAP SuccessFactors Limited Disaster Recovery Overview

Enhanced Disaster Recovery option may be ordered for:
SAP SuccessFactors Performance & Goals
SAP SuccessFactors Succession & Development
SAP SuccessFactors Compensation
SAP SuccessFactors Learning
SAP SuccessFactors Validated Learning
SAP SuccessFactors Employee Central (included in subscription)

Eligible production data centers: DC2 (Amsterdam, the Netherlands); DC4 (Chandler, Arizona, USA);
DC8 (Ashburn, Virginia, USA) and DC12 (St. Leon-Rot, Germany).

SAP designs its service for high availability, security, and data integrity. All data centers are ANSI TIA/EIA-942
Tier III+ rated facilities. An N+1 engineering model helps ensure scalability and reliability for all critical systems
and components at the production site. System architecture requires a disaster recovery plan for a potential major
disruption in datacenter facilities and operations.

A disaster is only declared when there is a loss of utilities and services. A loss of electricity, including backup
power, would take a data center offline. A loss of connectivity to the Internet would also take a data center
offline. As long as the production site has power and is connected to the Internet, it will not be considered a
disaster. At the highest level, there are two possible scenarios that would require we invoke the disaster recovery
plan:

1. Natural Catastrophe:
   This is generally an unexpected occurrence with little or no lead time. Seasonal weather patterns and
geographic anomalies affect data centers in different ways, but regardless of the circumstances, the primary
site is left inoperable. SAP SuccessFactors takes a leadership role in monitoring risk, declaring a disaster
and invoking the Disaster Recovery plan – ensuring personnel in the “failover site” are prepared to support
production for a minimum of six months from handover. After the Disaster Recovery event has been
resolved and the data center rebuilt, SAP SuccessFactors makes the decision to reconstitute in the original
production site.

2. Man-made Incident:
   This, too, is an unplanned event which incapacitates infrastructure at the production site. Emergency
incidents are assessed by SAP SuccessFactors and SAP Corporate Infrastructure Services (CIS). A SAP
management member with proper authorization must officially declare a disaster in order to initiate a Disaster
Recovery plan. Operations from the secondary site could last anywhere from a few weeks to many months.
Initiation of the failback plan is at SAP’s sole discretion.

All SAP SuccessFactors products include, at a minimum, the following capabilities: (i) offsite database backups to
disk (i.e. weekly full / nightly incremental / archive logs multiple times daily to separate storage array); and (ii)
commercially reasonable efforts to restore service from backups as soon as possible in case of a disaster
resulting in loss of the production data center. Back-up data is retained for thirty (30) days. The Enhanced Disaster
Recovery option is available as described below.
<table>
<thead>
<tr>
<th>Disaster Recovery Option</th>
<th>Backups and Other Included Disaster Recovery Services</th>
<th>Current Enhanced Disaster Recovery Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Scenarios</td>
<td>Entire production data center is incapacitated and offline due to natural or man-made catastrophic event</td>
<td>Entire production data center is incapacitated and offline due to natural or man-made catastrophic event</td>
</tr>
<tr>
<td>Short Service Description</td>
<td>Restore replicated backups from disk at a remote location with an in-place network and security. SAP may temporarily re-allocate resources from other environments and backfill. SAP maintains an open purchase order for storage and replacement servers during emergencies.</td>
<td>Near real-time, asynchronous data replication and failover to a fully-functional, warm Disaster Recovery site with an in-place network, security, available storage and a complement of basic replacement servers.</td>
</tr>
<tr>
<td>Offsite Backups</td>
<td>Weekly full / Nightly incremental / Archive logs multiple times daily to separate storage array</td>
<td>Weekly full / Nightly incremental / Archive logs multiple times daily to separate storage array</td>
</tr>
<tr>
<td>RPO: Target age of data</td>
<td>None specified; likely 24 hours, but last full backup could be as much as 7 days old</td>
<td>Could be as little as one hour, but no more than of 24 hours of data loss</td>
</tr>
<tr>
<td>RTO: Data access and application functionality</td>
<td>Commercially reasonable efforts to restore service as soon as possible</td>
<td>48 hours to grant administrator access / service</td>
</tr>
<tr>
<td>RTO: Full pre-event compute capacity</td>
<td>Commercially reasonable efforts to restore 100% capacity as soon as possible</td>
<td>48 hours to restore 100% service capacity</td>
</tr>
<tr>
<td>Written Plan Document</td>
<td>No customer-specific written Disaster Recovery plan; only Global Disaster Recovery solution available upon request</td>
<td>Customer-specific, written Disaster Recovery Plan available upon request</td>
</tr>
<tr>
<td>Annual Disaster Recovery Test</td>
<td>Only SOC report evidence of annual Disaster Recovery test</td>
<td>Annual Cloud Disaster Recovery solution test with option for customer participation when in-region</td>
</tr>
<tr>
<td>Effective Dates and Restrictions</td>
<td>Applies to production environments for applications supporting both critical and non-critical business functions per customer contract</td>
<td>Applies to production environments for applications supporting only critical business functions listed above and effective at the time a Disaster Recovery event is declared</td>
</tr>
<tr>
<td>Annual Recurring Fee</td>
<td>Included with customer’s subscription; no additional charges.</td>
<td>Subscription surcharge for all modules listed above except EC</td>
</tr>
</tbody>
</table>

SAP retains the right to change (at any time in its sole discretion but subject to the terms of the Agreement) the Cloud Service, this specification sheet, and/or the location of the data center(s) from which a Cloud Service is hosted.