



Disaster Recovery Plan Overview for Customers

Sage ERP Online

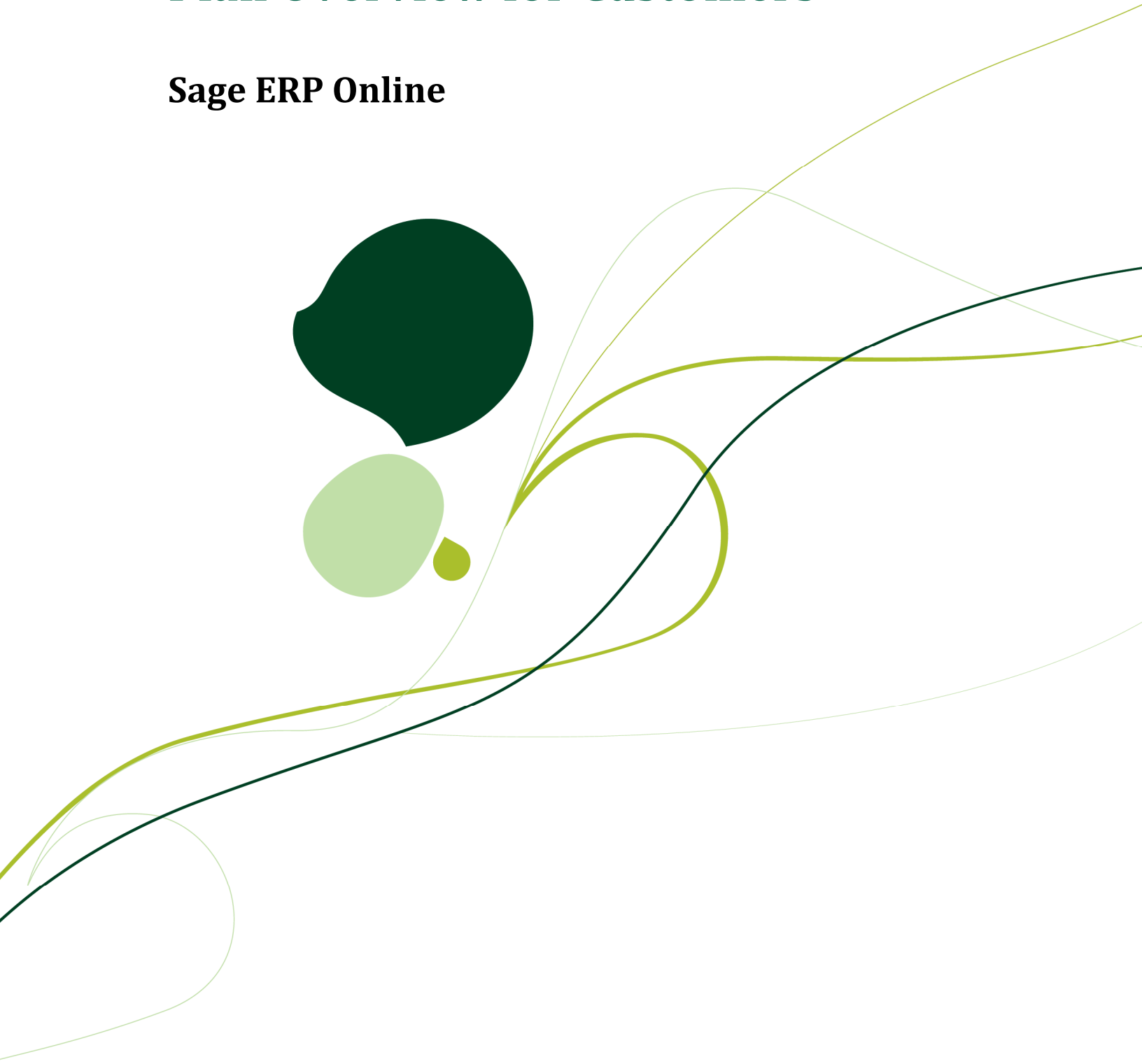


Table of Contents

1.0 Executive Summary	3
1.1 The Plan	3
1.2 Determining Factors.....	4
2.0 Disaster Recovery Strategy.....	5
2.1 Summary of the DRP Failover Process:	5
2.2 Infrastructure and Critical Systems.....	5
2.3 Infrastructure Security	5
2.4 Evaluation Criteria	5
2.5 Terms and Definitions.....	6
3.0 Post Disaster Recovery Back to Datacenter.....	6
3.1 Summary of the Post Disaster Recovery Process:	6
3.2 Infrastructure and Critical Systems.....	7
3.3 Firewall Security Policies	7
3.4 Evaluation Criteria	7
4.0 Conclusion	7

1.0 Executive Summary

This document details Sage's Disaster Recovery Plan (DRP) in terms of procedures and processes to fully recover from technology failure or man-made or natural disasters. This is a live document, and as such, contents detailed in this document may change from time to time. It neither replaces nor supersedes any language that is part of a legal and binding document between Sage and its customers.

1.1 The Plan

Sage operates two geographically separate data centers in the United States: a primary data center on the East Coast and a secondary data center on the West Coast. Production backups will be replicated to the secondary datacenter. In addition to traditional backups, real-time data will be constantly replicated to the secondary datacenter with a small amount of lag (typically less than one hour). In the event of a disaster we can enable the replicated systems in the secondary datacenter.

The secondary datacenter will then provide the infrastructure necessary to deliver Sage ERP Online services.

1.2 Determining Factors

The Sage ERP Online team has identified a number of key elements and procedures along with time-to-complete measures in the following defining qualities for an acceptable DRP:

- ✓ Data Security: Company databases will be stored offsite at secured locations which can be accessed at moment's notice. This offsite backup process must happen at least once a day.
- ✓ Recovered environment should mirror real time pre-disaster conditions in terms of usability and performance.
- ✓ The recovery time from failure must fall within (4) four hours from the time the DRP is put into motion.
- ✓ Once the primary site has returned to normalcy and an appropriate outage scheduled, returning the product to the primary datacenter must be within (4) four hours.
- ✓ All team members fully understand their duties in implementing such a plan.
- ✓ Operational policies must be adhered to within all planned activities.
- ✓ Proposed contingency arrangements should be cost-effective.
- ✓ Regular annual drills are required to ensure the DRP is current and valid.

2.0 Disaster Recovery Strategy

2.1 Summary of the DRP Failover Process:

	SUMMARY
1.	In the event of a disaster, the Sage ERP Online Team will communicate to our customer base through social media and other forms of communication, from the onset of any downtime. A further communication will then be sent immediately on the decision to invoke DR. This is at the (0 + 1hr) time.
2.	The Sage Disaster Recovery Plan Initiation Team gives the go-ahead for the DRP Plan.
3.	The Sage IS will then put into effect the failover process to the secondary datacenter.
4.	Once the failover process is complete, the Sage ERP Online Team will complete the necessary testing to confirm the integrity of the secondary environment.
5.	Once confirmed clients will be notified (by social media, telephone, and/or emails) that the failover site is up and running.

2.2 Infrastructure and Critical Systems

All key infrastructure and critical systems will be recovered in the secondary data center.

2.3 Infrastructure Security

All infrastructure security components present in the primary datacenter are replicated in the secondary datacenter. There is no reduction in any security aspect of the system when it is running in the secondary datacenter.

2.4 Evaluation Criteria

Clients have the ability to post and process transactions and carry out their day-to-day duties as per normal. There may be small variations in transaction times compared to the primary datacenter.

2.5 Terms and Definitions

Term	Definition
Sage ERP Online Team	Sage Hosted Services employees
Sage Disaster Recovery Plan Initiation Team	Sage Hosted Services Management Team

3.0 Post Disaster Recovery Back to Datacenter

Once the primary datacenter has been recovered, the Sage ERP Online team will test and confirm availability and functionality, after which we will then migrate back to our primary datacenter after appropriate customer notification. The post disaster recovery process, once put into effect, should be completed within (4) four hours and will be done during an appropriate maintenance window.

3.1 Summary of the Post Disaster Recovery Process:

SUMMARY	
1.	Once normalcy has resumed, the decision to restore Sage Accpac Online data back into the primary datacenter will be made by the Sage Disaster Recovery Plan initiation Team.
2.	The Sage ERP Online Team will then communicate out to all customers that the system will experience a maintenance outage to recover the offering to our primary datacenter. The Sage ERP Online team will attempt to align this with a scheduled maintenance window when appropriate.
3.	The Sage ERP Online team will then terminate all logged in connections and proceed to initiate the recovery of the Sage Accpac Online data back into the primary datacenter.
4.	The Sage IS Team will then put into effect the fall back process to the Primary datacenter on the East Coast.
5.	Once the fallback process is completed, the Sage ERP Online Team will proceed to test.
6.	Once the testing is deemed successful, The Sage ERP Online team will communicate out to all clients by social media, email and telephone that the offering is once again available

3.2 Infrastructure and Critical Systems

All key infrastructures recovered in the primary datacenter.

3.3 Firewall Security Policies

All security policies will revert to pre-disaster state.

3.4 Evaluation Criteria

Clients have the ability to post and process transactions carrying out their day-to-day duties as per normal.

4.0 Conclusion

While we strive for accuracy in this document, this document does not serve as a legal or a binding document. As market and industry conditions change, this document will be reviewed and updated at least yearly, after our annual Disaster Recovery tests. Sage reserves all rights to make changes to this document and its policies at its sole discretion.

Published: 7 October 2011