[Client Company]

Disaster Recovery Plan Agreement

Prepared by [MSP NAME] on [DATE]

## The Plan

This is an agreement for your disaster recovery (DR) plan, policies, and procedures in the event of an outage or emergency. Keep this important document on hand and in a safe, accessible place if your network is down. This document is to be used as a reference for the outline of your backup strategy, recovery procedure by scenario, critical system details, and priority for recovery in the event of a disaster.

## Goals

Create a clear, concise, and up-to-date disaster recovery plan to ensure a swift and efficient recovery for your organization in the event of an unexpected disruption or outage to critical systems. This plan prioritizes uptime, data integrity, and availability to safeguard business continuity.

## Backup and Disaster Recovery (BDR) Terminology

[Partner Name] uses the following industry-leading technology to provide [Client Name] business continuity services: [INCLUDE ALL THAT APPLY]

* On-premises storage of data on a BDR appliance
* Direct to cloud data backup and a local cache for recovery acceleration
* Hybrid backup approach with a local appliance as the first point for restores and virtualizations and cloud storage for offsite redundancy and recovery as needed
* Workloads in the public cloud with third-party direct to a cloud backup of that data
* Chain-free technology for efficient and secure data backup.
* AirGap anti-deletion technology for immutable data
* Virtual Office for fast cloud virtualization
* Custom runbooks to quickly restore your specified applications and infrastructure
* Geo+ geographically redundant data replication
* Secure offsite cloud storage and virtualization in the Axcient Cloud
* AutoVerify automated backup data integrity verification to test backups and ensure recoverability
* End-to-end, always-on encryption to continually protect data at rest and in transit
* Recovery Time Objective (RTO): The maximum amount of time before restoring a network, application, or service after an unplanned disruption

## Backup Strategy

| System | Offsite Backup | Backup Retention | Backup Frequency |
| --- | --- | --- | --- |
| *e.g., System 1* | *√* | *3 year* | *Hourly* |
|  |  |  |  |
|  |  |  |  |

## Disaster Response Team

### [Partner Name] Contacts

If the client discovers the disaster, the following contacts should be notified in order of priority:

| Name | Role | Contact Info | DR Process ROLE | Priority |
| --- | --- | --- | --- | --- |
| *Example: Bob Smith* | *BDR System Admin* | *Phone: 123.456.7890**Email:* *bsmith@email.com* | *Data recovery* | *1* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### [Client Name] Contacts

If the managed services provider discovers the disaster, the following contacts should be notified in order of priority:

\*Note it is critical to include additional contact information, including alternative phone and non-company email, in case of a disaster and your systems are unavailable.

| Name | Role | Contact Info | DR Process ROLE | Priority |
| --- | --- | --- | --- | --- |
| *Example: Jane Doe* | *CEO* | *Cell Phone: 123.456.7890**Work email:* *bsmith@workemail.com**Alt email**bsmith@gmail.com* | *Technical staff notification* | *1* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Disaster Recovery Plan and Service Agreement

### Types of Recovery

There are varying recovery approaches that depend on the type of disaster. Here are the different types of recovery methods available for your IT environment: [INCLUDE ALL THAT APPLY]

* Local Virtualization – Boot the system to a local virtual environment.
* Cloud Virtualization – Boot the system in the cloud.
* Export as a virtual disk.
* BDR Appliance via Mount, FTPS Client, or iSCSI, as virtualization, exported as a virtual disk, or bare metal recovery to hardware.
* Private/Axcient Cloud Vault without Local Cache via Mount, FTPS Client, or Recovery Center as virtualization, exported as a virtual disk, or bare metal recovery to hardware.
* Private/Axcient Cloud Vault with Local Cache via Recovery Center as virtualization, exported as virtual disk, or bare metal recovery to hardware.
* Virtualize via Hypervisor – export an image and boot the system to a virtual environment.
* Bare Metal Restore—this method reformats the system from scratch and restores it to the existing or new physical or virtual system.

### Disaster Recovery (DR) Plan Potential Scenarios

Depending on the incident and potential impact, one or more of the following DR procedures will be activated. This is not an exhaustive list of all the possible incidents.

| Scenario | DR Plan |
| --- | --- |
| SCENARIO 1**Missing Files** *(Accidental deletion, malicious deletion)* | **Restoration**Any missing file will be restored from the appliance or the cloud to an alternative location.\*RTO up to 60 minutes |
| SCENARIO 2**Single Machine Corruption***(OS corruption; Ransomware; no hardware failure)* | **Failover*** Spin up a machine in Virtual Office or
* Direct virtualization on an appliance

\*RTO up to 60 minutes  |
| SCENARIO 3**Single Machine Failure***(hardware failure)* | **Local Appliance Virtualization and Bare-Metal Restore*** Rapid Recovery via Local Virtualization: During the initial outage, the affected machine will be provisioned as a virtual machine (VM) directly on the local appliance or in the cloud.

\*RTO up to 60 minutes* Non-Disruptive Bare-Metal Restore Test (Optional): Once hardware repairs are complete, we can leverage the ongoing VM instance for a non-intrusive test of the bare-metal restore process.
	+ Scheduled Downtime for Final Bare-Metal Restore: Following a successful test (if applicable), a designated window will be established for the final bare-metal restore. The VM will be stopped during this planned downtime, and the actual restore process will commence.

\*RTO up to x hours |
| SCENARIO 4**Multiple Machines Down***(Power failure)* | **Tiered recovery plan designed to minimize downtime and restore functionality as swiftly as possible.*** **Local Appliance Virtualization (Expeditious Restoration):** In a limited outage, we will leverage on-site resources by creating a running instance of the affected machines as virtual machines (VMs) directly on the local appliance. This maintains network connectivity and facilitates a rapid restoration for most scenarios.
* **Cloud Virtualization (For Extensive Outages):** If the local appliance's capacity proves insufficient to accommodate the workload of all affected machines, we will initiate a seamless migration to our cloud virtualization environment. It is imperative to ensure that all desktops have a functional and active VPN client installed, as this will be the primary method for establishing remote access to these machines.
* **Hardware Repair and Bare-Metal Restore/Resuming direct to cloud backups** [DETAIL PLAN HERE]

Your data will continue to be backed up to the cloud during this process while we get a new backup on your restored appliance.\*RTO up to x hours |
| SCENARIO 5**Site Down***(full-site outage; hardware failure/power outage/natural disaster)* | **Failover:*** **Triage workstations and servers to prioritize for recovery**
* **Determine hardware/performance requirements**
	+ How much RAM?
	+ CPU cores?
	+ Other:
* **Identify Networking information:**
	+ Gateway IP
	+ System IP addresses
	+ System subnets
* **Determine the best option for network connectivity with DR site and local site**
	+ SSL VPN
	+ Site-to-site VPN (IPSEC or OpenVPN)
	+ Remote desktop (RDP)
* **Virtualize desired systems in Axcient Cloud/Virtual Office**
	+ **Virtualize with runbooks, or**
	+ **Allocate appropriate VM resources**
		- Virtualize manually
			* **Step A – once machine(s) are turned on, configure Virtual Office settings including:**
				+ Gateway
				+ Subnet mask
				+ VPN preference - SSL VPN or Site-to-site VPN (IPSEC or OpenVPN)
				+ Port forwarding
				+ DHCP if not virtualizing active directory server
			* **Step B – Assigning static IP to each virtual machine, if needed**
				+ Log in to each VM console and configure static IP as you would normally in Windows
* **Credentials and access distribution:**
	+ Relay user login credentials (determined by the network connection option in Step 4)
	+ If using SSL VPN, must remote into each end user's machine to install VPN client

\*RTO: up to x hours |
| Failback | Once the failback site is rebuilt and the hardware is back in commission and running normally:**Appliance failbacks:** Incremental vault restore down to the new appliance Once the failback site is rebuilt and the hardware is back in commission and running normally.**Complete all appliance or cloud failbacks**: by **c**onducting bare metal restore operations |

***\*Recovery Time Objective (RTO): Recovery times are a good faith estimate and are dependent on a multitude of factors, including but not limited to site replication time, physical server health, and recovery scenario(s).***

## System Information

| System Name | Machine Role | Priority (1=high; 3=low) | Dependent Machine(s) |
| --- | --- | --- | --- |
| *e.g., System 1* | *Terminal Server* | *2* | *Active Directory Server* |
|  |  |  |  |
|  |  |  |  |

## Ongoing Review & Testing

Your data is tested [FREQUENCY] through an automated process known as AutoVerify. Additionally, your managed service provider has created runbooks to be used to virtualize your environment as a Virtual Office in the event of a disaster. These cloud failover capabilities support fast disaster recovery as well as disaster recovery plan testing.

The disaster recovery process and incident response will be tested yearly to ensure complete preparedness for a real disaster scenario. Additionally, both parties will review the disaster recovery plan annually during a Quarterly Business Review or as needed by any shifting threats or precipitating event.

### Disaster Recovery Plan Revision History

| Version | Date | Revision Details |
| --- | --- | --- |
| *e.g., Version 1.0* | *Jan. 1, 2024* | *Initial plan drafted for approval* |
|  |  |  |
|  |  |  |

By signing below, I certify that I have read the above information and approve this disaster recovery plan.

### [PARTNER NAME] REPRESENTATIVE

**Name:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### [CLIENT NAME] REPRESENTATIVE

**Name:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_