ORIGINAL CREATION DATE:

BUSINESS NAME:

EMERGENCY DATA RECOVERY PLAN

Advanced preparation for ransomware infection can save valuable time in a situation where seconds count. By clearly laying out your priorities for getting business up and running, you create a clear path forward, and enable your team to take fast action. Once the primary systems are back online and employees are back to work, less critical elements of the infrastructure may be addressed and reactivated.

This template is designed to help get your **Emergency Recovery Plan** laid out clearly, printed, and secured within your organization for access by your Emergency Response Team.

DOCUMENT SUMMARY:

PREPARED BY:		**TITLE:**		**DATE:**
APPROVED BY:		**TITLE:**		**DATE:**

VERSION HISTORY

	VERSION:	APPROVED BY:	DATE:	CHANGES MADE:	AUTHOR:
1.					
2.					
3.					
4.					

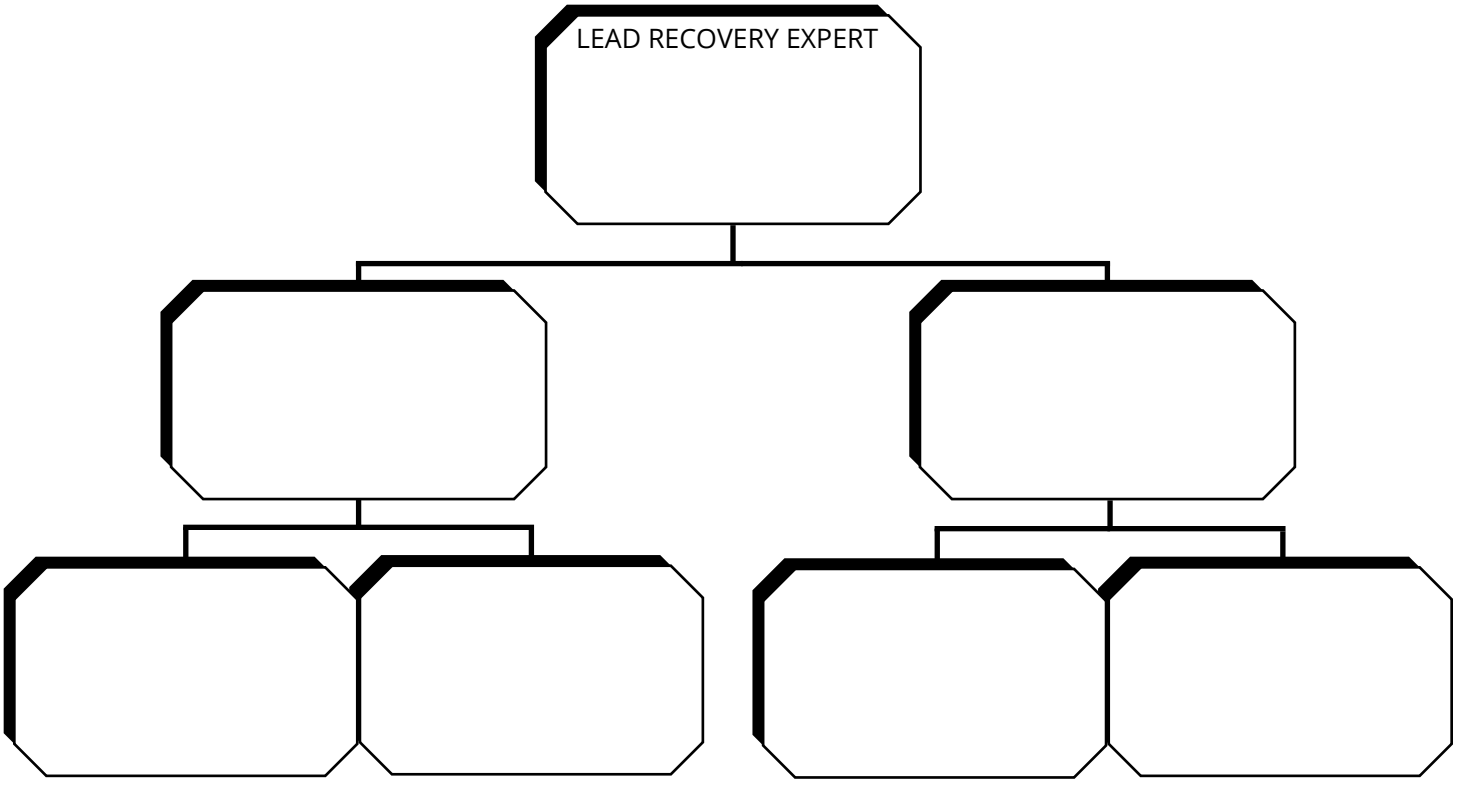
© 2022 NovaBACKUP. All Rights Reserved.

	VERSION:	APPROVED BY:	DATE:	CHANGES MADE:	AUTHOR:
5.					
6.					
7.					
8.					

4. EMERGENCY RESPONSE TEAM

	NAME:	TITLE:	ROLE:	PHONE:	EMAIL:
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					

5. NOTIFICATION TREE



© 2022 NovaBACKUP. All Rights Reserved.

1. OBJECTIVE - WHAT IS THE PRIMARY GOAL OF THIS RECOVERY PLAN?

This statement should include return to business goals, RTOs and RPOs, and expectations of impact.

2. OVERVIEW - WHAT ARE THE PRIMARY COMPONENTS OF THIS PLAN?

This should include major procedures, steps to be taken and tools required to meet recovery goals.

3. CONTACT PROCEDURES - WHAT TEAM MEMBERS MUST BE NOTIFIED?

This should include communication steps, and the teams which must be alerted and in what order.

© 2022 NovaBACKUP. All Rights Reserved.

6. IT SYSTEMS LIST

Please list all systems critical to your organization and prioritize them by need to be brought back online in the event of a data loss scenario.

	IT SYSTEM NAME:	CRITICAL COMPONENT(S) :
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

7. SERVERS

Please list the servers that must be restored in the event that data is lost and their restore priority.

	NAME:	IMPORTANCE:	PHYS/VIRT:	SPECS:	PURPOSE:
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

© 2022 NovaBACKUP. All Rights Reserved.

8. SYSTEM / SERVER RESTORE PROCEDURES

This section should detail the specific steps required to bring a system completely back online. Important items to be included are backup locations, devices and tools to be used along with specific actions. This section should be copied / replicated for each system to be restored in a disaster (sections 6 & 7).

	STEP:	SPECIFIC ACTIONS:	RESPONSIBLE PERSONS:
1.			
2.			
3.			
4.			
5.			
6.			

9. ANTICIPATION OF POTENTIAL THREATS

Many scenarios are entirely preventable. Depending upon your unique environment, some forms of Rasomware infection may be more likely than others. Now is the time to consider potential attack, vectors and clarify the personal courses of action for your team.

POTENTIAL RANSOMWARE SCENARIOS	
INFECTION SCENARIO 1:	
1.	

© 2022 NovaBACKUP. All Rights Reserved.

POTENTIAL RANSOMWARE SCENARIOS

RESPONSE SCENARIO 1:

INFECTION SCENARIO 2:

2.

RESPONSE SCENARIO 2:

INFECTION SCENARIO 3:

3.

RESPONSE SCENARIO 3:

NovaBACKUP

HIPAA SEAL OF COMPLIANCE COMPLIANCY GROUP HIPAA VERIFIED

For more than a decade, NovaBACKUP has been committed to providing all-inclusive local and cloud-based data protection to thousands of MSPs and professional offices around the globe. Our vast experience in helping specialized industries meet strict regulatory requirements has made NovaBACKUP an industry leader in Backup and Disaster Recovery. From initial contact, to ongoing backup management, our experts are there to support you. Learn more about us at www.novabackup.com or call us directly at **+1 (805) 579-6700**.

© 2022 NovaBACKUP. All Rights Reserved.