INCIDENT RESPONSE PLAN

ECHO TECHNOLOGY SOLUTIONS

DEFINITION OF A DATA BREACH

A data breach is the unauthorized access of the organization data. The access may compromise the confidentiality, integrity or availability of the data. Good faith access of the data by employees or agents or legitimate purposes is not a breach.

TYPES OF INCIDENT

Events that will trigger this plan includebut are not limited to:

- Internal data breach
- Supplier or partner data breach
- Website breach
- Social media breach
- The personally identifiable information of multiple stakeholders has been breached.
- Denial of service attack
- Firewall breach or malicious portscans
- Virus/malware outbreak
- Ransomware attack
- Successful phishing attack
- Fire or natural disaster

PERSONALLY IDENTIFIABLE INFORMATION

This includes but is not limited to:

- Social Security number
- Driver's license number or Identification Card numbers
- Financial account number, credit ordebit card numbers
- Home address or e-mail addresses
- Medical, health information or HIPAA protected data
- Data protect by regulatory compliance

ABOUT THE INCIDENT RESPONSE PLAN TEMPLATE

ECHO has created this template for your organization's own use with recommended and example action items. Depending on your size, industry and compliance requirements, you may have multiple security incident response plans depending on the scope and severity to your organization.

For more information or clarification, reach out to us at
CLIENTSUCCESS@ECHOTS.COM

ORGANIZATION

DATE

INCIDENT RESPONSE TEAM

ROLE	TITLE	NAME
Team Lead	CIO, VP IT, CFO	
Cybersecurity Expert	CISO	
User Expert	Help Desk Manager, Dir of HR	
Communications Expert	Dir of Marketing, Dir of Development	
Applications Expert	Applications Manager	
Network/ Systems Expert	Network/ Systems Manager	
Operations Expert	COO, Dir of Ops, Dir of Finance	
Legal Expert	In House or External Counsel	
Executive Liaison	Firm Managing Director	

INCIDENT RESPONSE PLAN

1. Notify Incident Response Team

➡ All employees and organization agents must immediately report any suspected or confirmed data breach, internal or by partners, to their manager, plus one or more ofIncident Response Team.

2. Control the event

- ➡ Stakeholder communications
- ➡ Closing access
- ➡ Actions required by insurers and regulators
- ➡ Preventing further damage

3. Stabilize data

- ➡ Use of backup data
- ➡ Temporary measures: The temporary removal of the affected systems.

4. Declare that systems are clear

- ➡ Removing temporary measures
- ➡ Resuming normal operations : Determine conditions required to end the Incident Response Plan activation and restore normal operations.

5. Clean Up

- ➡ Process and systems changes
- ➡ Collection of incident data, email, logs and forensic evidence. Review of privileged applications,system files, password changes, configurations changes to software and systems and files systems.
- ➡ Update and test.