INCIDENT RESPONSE PLAN CHECKLIST

It is a **best practice** to have an **Incident Response Plan** developed an implemented.

Use this checklist as a guide to ensure your plan will help your organization respond to incidents:

☑	Item to Include in Plan	☑	Item to Include in Plan
	ITEM 1: Identify the Fundamentals		**ITEM 6: Obligation Notification/Communication Plan**
	Detail Scope, Goals, and Management Support		Identification of Notification Requirements
	Identify required alignment to established standard(s) (PCI, HIPAA, ISO, NIST, etc.)		Determine incident scenarios (Breach Unlikely, Breach, Contained Disclosure, etc.)
	Reference to other supporting IRR documents (Policy, Standards, Procedures, etc.)		*Per Scenario:* Who, What, When, Why, What Message, How, Who is authorized to send
	Incident Response Plan Approvals and Revision Dates		*Template for:* Internal Communications, Breach Notification Letter & Press Release
	ITEM 2: Teams and Contacts		**ITEM 7: Establish Status Internal Team Communications Plan**
	Response Team Membership - Contact info		Establish Mechanism for Communication
	Incident Alert Hotlines		Define Schedule for Status Updates
	Incident Response Roles and Responsibilities		**ITEM 8: Incident Response Forms:**
	Incident Response Experts, Legal Authorities, Legal Counsel, Interested and Connected Parties		Observations and Actions Log
	ITEM 3: Establish Definitions		Inventory of Impacted Assets
	Security Event		Incident Classification Worksheet
	Incident		Impact Analysis Worksheet
	Breach		Third Parties Contacted Log
	ITEM 4: Identify Phases of the Incident Response Lifecycle		Chain of Custody Form
	Planning & Prevention – People, Process & Technology		Root Cause Analysis Form
	Alerting– The method to report an incident		Internal Investigation Form
	Triage – Determine between an event and an incident		Status Meeting Minutes
	Investigation – Identify the scope & source of incident		Response Approach Worksheet
	Containment – Prevent the spread of damage		**ITEM 9: Continuous Improvement Procedures**
	Eradication– Remove the source of incident		Updating the Incident Response Plan
	Recovery – Restore systems to secure operations		Approval Procedures for the Incident Response Plan
	Lessons Learned – Eliminate the root cause		**ITEM 10: Include Scenario Run Books for specific types of Incidents**
	ITEM 5: Detail Phases of IR Lifecycle— Include for each phase:		**ITEM 11: Include a Glossary and Definitions**
	Description of Phase		**ITEM 12: Align to other Requirements:**
	Detailed Guidance/Checklist		Include Requirements from your industry
	Flow Diagram		Include Requirements from your internal policies
	References to Forms Used		Refer to Information aligning to your company processes
	Payment Brand Specific activities (PCIDSS)		

HALOCK®

847-221-0200
NON-EMERGENCY

800-925-0559
EMERGENCY RESPONSE HOTLINE

INFO@HALOCK.COM WWW.HALOCK.COM

Inc. 5000

BBB ACCREDITED BUSINESS