HALOCK® Checklist

INCIDENT RESPONSE PLAN

It is a **best practice** to have an **Incidence Response Plan** developed and implemented.
Use this checklist as a guide to ensure your plan will help your organization respond to incidents

ITEM 1 Identify the Fundamentals

- ☐ Detail Scope, Goals, and Management Support
- ☐ Identify required alignment to established standard(s) (PCI, HIPAA, ISO, NIST, etc.)
- ☐ Reference to other supporting IRR documents (Policy, Standards, Procedures, etc.)
- ☐ Incident Response Plan Approvals and Revision Dates

ITEM 2 Teams and Contacts

- ☐ Response Team Membership - Contact info
- ☐ Incident Alert Hotlines
- ☐ Incident Response Roles and Responsibilities
- ☐ Incident Response Experts, Legal Authorities, Legal Counsel, Interested and Connected Parties

ITEM 3 Establish Definitions

- ☐ Security Event
- ☐ Incident
- ☐ Breach

ITEM 4 Identity Phases of the Incident Response Lifecycle

- ☐ Planning & Prevention – People, Process & Technology
- ☐ Alerting – The method to report an incident
- ☐ Triage – Determine between an event an incident
- ☐ Investigation – Identity the scope & source of incident
- ☐ Containment – Prevent the spread of damage
- ☐ Eradication – Remove the source of incident
- ☐ Recovery – Restore systems to secure operations

ITEM 5 Detail Phases of IR Lifecycle – Include for each phase

- ☐ Description of Phase
- ☐ Detailed Guidance/Checklist
- ☐ Flow Diagram
- ☐ References to Forms Used
- ☐ Payment Brand Specific activities (PCI DSS)s

ITEM 6 Obligation Notification/Communication Plan

- ☐ Identification of Notification Requirements
- ☐ Determine incident scenarios (Breach Unlikely, Breach, Contained Disclosure, etc.)
- ☐ Per Scenario: Who, What, When, Why, What Message, How, Who is authorized to send
- ☐ Template for: Internal Communications, Breach Notification Letter & Press Release

ITEM 7 Establish Status Internal Team Communications Plan

- ☐ Establish Mechanism for Communication
- ☐ Define Schedule for Status Updates

ITEM 8 incident Response Forms

- ☐ Observations and Action Log
- ☐ Inventory of Impacted Assets
- ☐ Incident Classification Worksheet
- ☐ Impact Analysis Worksheet
- ☐ Third Parties Contacted Log
- ☐ Chain of Custody Form
- ☐ Root Cause Analysis Form
- ☐ Internal Investigation Form
- ☐ Status Meeting Minutes
- ☐ Repose Approach Worksheet

ITEM 9 Continuous Improvement Procedures

- ☐ Updating the Incident Response Plan
- ☐ Approval Procedures for the Incident Response Plan

ITEM 10 Including Scenario Run Books for Specific Types of Incidents

ITEM 11 Include a Glossary and Definitions

ITEM 12 Align to other Requirement

- ☐ Including Requirements from your industry
- ☐ Include Requirements from your internal policies
- ☐ Refer to Information aligning to your company processes