

Example Table of Contents for a Computer Incident Response Plan

Revision History	5
Forward	6
Plan Introduction	7
Plan Objective	7
Plan Scope and Assumptions	7
Plan Execution and Command Topologies	8
Plan Ownership	9
Plan Structure	10
Updating and Synchronization	10
Incident Preparation	12
Statutory/ Compliance Framework	12
Sensitive Data	12
PCI Data Map (Encl 1) **RESTRICTED**	12
ISOC Threat Portfolio (PCI) (Tab B) **RESTRICTED**	12
PCI Log Data - Tab (C)	13
Third-Party (Payment) Connections (Tab D)	13
Third-Party Services	13
VISA Qualified Incident Response Assessor	13
Identity Protection Services	14
Compromise Notification fulfillment	15
Incident Detection, Analysis and Declaration	19
Sources of Precursors and Indicators	19
ISOC Monitoring Feeds Tab (F) (RESTRICTED)	19
Malware	19
Law Enforcement, Common Point of Purchase (CPP) or Other External Sources	20
NOC, Service Desk and Other Internal Sources of Detection	21
Incident Thresholds	22
Data threshold	22
Compromise threshold	23
Incident Analysis	23
Technical Impact	23
Business Impact	24
Incident Categories	24
P1	24
P2	25
Non-Actionable/Informational	25
Incident Declaration	26
Incident Notification and Mobilization	26
Incident Documentation	30
Incident Response Supporting Actions	30
Plan Execution	30
Organization and Roles	30
Process and Rhythm	34
Synchronization and Decision Making	35
Mandatory Reporting/Notification(s)	36
Payment Card Industry Data Security Standard (PCI DSS)	37

Example Table of Contents for a Computer Incident Response Plan

Release of “Public Facing Documents”	41
Draft/Approve/Release Process	41
“Public Facing Documents” Participants	42
Evidence discovery and retention	43
Criminal prosecution	43
Civil Litigation	43
Managing Evidence	43
Liaison with Local Law Enforcement	44
Loss Prevention (LE Liaison)	44
Law Enforcement Points of Contact (POC) (Tab I)	45
Incident Containment, Eradication and Recovery	47
The (Data Compromise) CIRP SWAT Team	47
Containment	47
Identification and Isolation of Affected System(s)	47
Verification of Non-Affected systems	48
Third-Party and External Connections	48
Consequence Management	49
Eradication and Recovery	49
Remediation	49
Compensating Controls	50
Disaster Recovery/Business Continuity	50
Post Incident Activity	50
Incident Termination	50
Criteria for Terminating an Incident	51
Decision Process for Terminating an Incident	51
Evidence Retention	53
Response Statistics	53
Lessons Learned	53
CIRP Roles and Responsibilities	54
Advertising	54
Corporate Accounting	54
Disaster Recovery	54
Human Resources	55
Incident Control Center (ICC)	55
Information Security Forensics	55
Information Security Operations Center (ISOC)	55
Internal Communications	55
Investor Relations	56
IT	56
IT Retail Portfolio	56
Compliance	56
Legal	56
Loss Prevention	57
Problem Management	57
Public Affairs	58
Retail Operations	58

Example Table of Contents for a Computer Incident Response Plan

Reviewing Senior Executive	58
CISO	58
Plan Maintenance	59
Overview	59
Regular Updates	59
Verification/Updates of Perishable Data	59
Incorporation of Previous Lessons Learned	59
Annual Testing of the Plan	59
Requirement	59
Exercise Mechanics	59
Lessons Learned	61
Record(s) Retention	61