Pragmatic GRC™

C-001
Incident Response Playbook Guide

Cybersecurity Operations Resource | Version 1.0 | Practical Implementation Guide

Executive Summary

The Incident Response Playbook provides a practical framework for preparing for, responding to, containing, recovering from, and learning from cybersecurity incidents. It is designed specifically for small and medium-sized businesses and aligns with the Pragmatic GRC™ Methodology.

Document Information

Field	Value
Resource ID	C-001
Resource Family	Cybersecurity Operations
Version	1.0
Status	Initial Release
Related Chapters	4, 6, 8
Related Resources	F-001, F-002, R-001, C-002, C-005, G-002

1. Purpose

Provide a standardized approach for identifying, reporting, responding to, containing, eradicating, recovering from, and documenting cybersecurity incidents.

2. Incident Categories

Malware, ransomware, phishing, business email compromise, unauthorized access, denial-of-service, insider threats, data loss, cloud security events, and third-party incidents.

3. Incident Response Lifecycle

Preparation → Identification → Containment → Eradication → Recovery → Lessons Learned.

4. Roles and Responsibilities

Define the Incident Coordinator, Executive Sponsor, Business Owner, IT/MSP, Communications Lead, and Legal/Compliance responsibilities.

5. Escalation Criteria

Document when incidents require executive notification, customer notification, regulatory reporting, law enforcement engagement, or cyber insurance notification.

6. Evidence Handling

Preserve logs, screenshots, timelines, forensic evidence, and chain-of-custody documentation.

7. Communications

Prepare internal notifications, executive updates, customer communications, media statements, and post-incident reporting.

8. Post-Incident Review

Conduct a lessons-learned meeting, update the SSP, Risk Register, and playbooks, and track corrective actions.

Incident Response Workflow

Detect Incident
↓
Report Incident
↓
Triage & Classify
↓
Contain
↓
Eradicate
↓
Recover
↓
Lessons Learned
↓
Update F-002, R-001 & G-002

Severity Classification

Severity	Description	Typical Response
Critical	Business operations severely impacted	Immediate executive response
High	Major service disruption	Priority response within hours
Medium	Limited operational impact	Business-day response
Low	Minor issue	Routine handling

Best Practices

• Report incidents immediately.
• Preserve evidence.
• Practice with tabletop exercises (C-005).
• Update the Unified System Security Plan (F-002) and Enterprise Risk Register (R-001) after significant incidents.
• Review response effectiveness during the Monthly GRC Heartbeat™.

Revision History

Version	Date	Author	Description
1.0		Pragmatic GRC™	Initial publication