Incident Response and Digital Forensics – Week 1 Deliverables

1. Incident Response Policy Document

Purpose: The policy should state management's commitment to security and the goals of the incident response (IR) program. It must establish why the organization has an IR policy (e.g., to protect critical systems and data) and outline its objectives[1][2]. In practice, this means defining what constitutes a reportable "incident," the overall aim of rapid and coordinated response, and management's endorsement of required resources and authority[1][2]. For example, NIST emphasizes that the IR policy is the "foundation of the incident response program," setting out which events are incidents, organizational structure, and reporting requirements[1].

Scope: Define the boundaries of the policy – e.g., which systems, networks, and personnel it covers, and under what conditions. The policy must specify to whom and under what circumstances it applies[3]. For instance, it should say whether it covers all IT systems, third-party cloud services, remote staff, etc., and under what contexts (work hours, remote access, bring-your-own-device, etc.)[3]. It should also include a clear definition of "incident" and related terms so that everyone understands what must be reported[3].

Roles and Responsibilities: The policy must identify key IR roles and their authority. At minimum, this includes the IR Manager (Team Lead), technical responders, forensic examiners, communications lead, and legal advisor[1][4]. For example, one source notes that IR policies should "define roles and responsibilities" including the organizational structure for response[1]. In practice, the **Incident Response Manager** (team lead) "coordinates the incident response team and ensures the incident is managed effectively"[5][6]. The **Technical Lead / Security Analyst** (sometimes called Engineering Lead) is responsible for monitoring alerts, analyzing compromised systems, and directing technical containment/remediation[7][6]. A **Forensic Analyst** collects and preserves digital evidence, maintains chain-of-custody, and prepares investigation reports[8][6]. The **Communications Lead** (PR/Communications Officer) manages internal and external messaging, keeps stakeholders informed, and handles media inquiries[9][6]. The **Legal Liaison** (or Legal Advisor) reviews actions for legal compliance and liability, advises on legal issues, and coordinates with law enforcement or regulators as needed[10][6]. (Depending on organization size, one person may wear multiple hats or additional roles like HR liaison may be added.) These roles align with best practices that call for an IR team with specialists for management, technical analysis, communications, and legal/regulatory response[4][6].

Incident Classification: The policy should define categories or severity levels to prioritize response. Typical schemes classify incidents by impact (e.g. *Critical* – widespread outage or exfiltration of sensitive data; *High* – system compromise affecting business functions; *Medium/Low* – limited impact or policy violation)[11][6]. NIST guidance specifically calls for

"prioritization or severity ratings of incidents" in the policy[11]. For example, a *Critical* incident might trigger immediate executive notification and 24×7 response, whereas a *Low* incident (e.g. malware on a single non-critical PC) might require standard response procedures with local IT. The policy should document how incidents are classified (impact factors) and ensure that each classification level has predefined escalation and notification requirements.

Escalation Procedures: The policy must set out when and how incidents are escalated to higher authority or to specialized teams. This includes defining **escalation points** in the process[12]. For instance, the policy should specify triggers for escalation (e.g. if an incident is uncontained after a certain time, or if it meets regulatory-reporting criteria) and whom to contact at each stage (e.g. notify the CISO, legal counsel, or CEO for serious breaches). NIST recommends including guidelines for external communications and "handoff and escalation points in the incident management process"[12]. In practice, an escalation matrix is often used (see Section 3). The policy should also require timely reporting: for example, automatically informing designated executives and, if relevant, external parties (e.g. regulators or law enforcement) for high-severity incidents[12][1].

Documentation Requirements: The policy must mandate thorough documentation of all incidents. At minimum, incident handlers should "immediately start recording all facts" once an incident is suspected[13]. NIST advises that every action from detection through resolution be documented and timestamped, ideally in a bound logbook or secured electronic system[13][14]. The policy should require an incident log or tracking system capturing the status of the incident (e.g. new, in progress, resolved), a summary of events, indicators or alerts, related incidents, actions taken by all handlers, and chain-of-custody for evidence[15]. Every document should be signed and dated by the handler, as such records may be used later for forensic analysis or legal proceedings[16]. Finally, the policy should define retention: for example, evidence and logs should be preserved in accordance with a records retention schedule (in some sectors, months or years) and handled with appropriate access controls[17]. In summary, the policy should require that *all* incident data – logs, communications, reports, and evidence – be recorded, protected, and reviewed for compliance with the policy[13][15].

2. Incident Response Team (IRT) Structure

An effective IRT should have a clear chain of command and defined roles. Although an actual organizational chart will vary by company, a typical IR team might be organized as shown in the conceptual structure below (for example, using an Incident Command System approach or similar). In practice, each box (Incident Manager, Technical Lead, etc.) should be a staffed position or role in your organization.

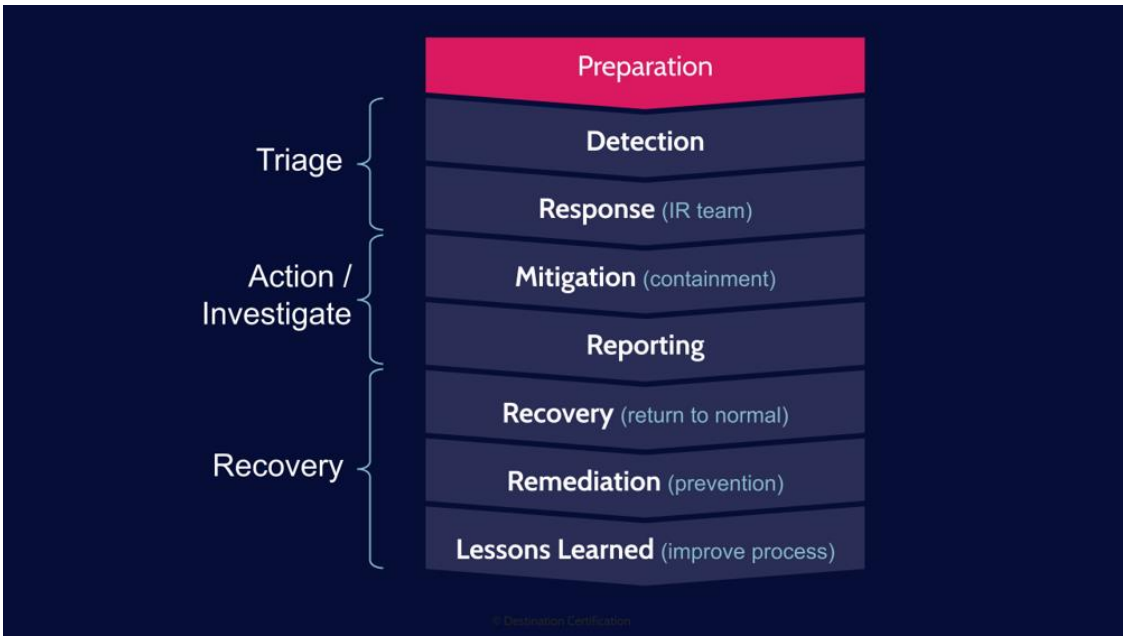

Figure: Incident response lifecycle phases. A conceptual IR workflow (Preparation through Lessons Learned) is shown to illustrate how Week 1 deliverables (policy, team setup) align with the IR process[18].

Key Roles

- **Incident Manager (Team Lead):** Oversees and coordinates the IR effort, ensures plan execution, and serves as liaison to senior leadership[5][6]. This person "leads and coordinates the incident response team" and communicates status to executives[5].
- **Technical Lead (Security Analyst):** Responsible for detecting, analyzing, and guiding the technical response. This role "detects and analyzes security incidents" and recommends containment/remediation measures[19][6]. They manage technical escalations and engage subject-matter experts as needed.
- **Forensic Analyst:** Collects, preserves, and examines digital evidence throughout the incident[8][6]. This person follows chain-of-custody procedures and produces technical forensic reports.
- **Communications Lead:** Manages messaging both internally and externally[9][20]. This role drafts notification templates, handles media and stakeholder updates, and ensures consistent messaging. According to industry guidance, the Communications Lead "handles the internal and external communications" and relieves technical staff from having to communicate incident details to many stakeholders[9][20].
- **Legal Liaison:** Advises on legal/regulatory issues and compliance[21][22]. The Legal Liaison ensures that response actions (e.g. evidence collection, public statements) comply with laws and regulations, and coordinates with law enforcement or regulatory bodies if required[21].
- **Other Roles:** Depending on the incident and organization, additional roles may be needed (e.g. IT Operations to restore systems, HR for insider cases, Privacy Officer for data breaches, etc.). Each role should be staffed or assigned in the IRT structure.

These roles correspond to common frameworks: for example, sources list IR teams comprising a manager (Incident Commander), technical leads/analysts, subject-matter experts, communications, and legal/HR representatives[4][6].

RACI Matrix

To avoid ambiguity, use a RACI (Responsible, Accountable, Consulted, Informed) matrix for core IR activities (Detect, Contain, Eradicate, Communicate, Recover, Report). For instance, one may assign: the **Incident Manager** as *Accountable* for all major activities (owns the overall response) and *Responsible* or *Consulted* for communications; the **Technical Lead** as *Responsible* for detection, analysis, containment, and eradication tasks; the **Forensic Analyst** as *Responsible* for evidence collection (Eradicate) and *Consulted* on technical analysis; the **Communications Lead** as *Responsible/Accountable* for notifying stakeholders and issuing reports; and the **Legal Liaison** as *Consulted/Informed* for all high-severity actions. ("Responsible" means performing the task, "Accountable" means ultimately answerable for completion[23].) In all cases, clearly document in the matrix which individual or role (often with backups) will fulfill each R/A/C/I designation for each step of the IR process[23][6].

3. Communication Plan

An IR communication plan ensures timely, coordinated notifications. It should include:

- **Escalation Matrix:** A table or matrix that maps incident severity or category to who to notify (role/position), and within what time frame. For example, a *Critical* incident (e.g. data breach) might require notifying the CISO, CEO, legal counsel, and external regulators immediately, while a *High* incident (major service outage) might notify the security operations center manager and IR Manager first. The matrix should list primary and alternate contacts (with 24×7 reachability) for each role. This aligns with best practices of having an "up-to-date contact list with alternate contacts" for IR escalation[24]. (See Section 2.1 for an example RACI template, which also clarifies communication responsibilities.)

- **Stakeholder Contact Channels:** Clearly specify communication channels and protocols. Common channels include secure email distribution lists, phone call trees, instant messaging (e.g. encrypted chat), and an incident-management system. For each stakeholder group (operations, IT, executive management, customers, media, regulators), define the preferred contact method and backup. Also prepare a list of key stakeholders' contact information (internal and external) so responders can quickly reach out. NIST advises documenting "reporting and contact forms" and communication procedures[11].

- **Notification Templates:** Provide sample messages for different audiences. For instance:

- *Internal Incident Alert:* A brief template email or SMS to notify the IR team and affected departments (e.g. "Security Alert: Possible network breach detected at 10:42 AM on 7/21/25. Please stand by for further instructions. Do not power down any systems.").

- *Executive Briefing:* A concise incident summary for senior management (impact, scope, next steps).
- *External Notice:* If applicable (e.g. regulators or law enforcement), a formal notification letter with incident details.
  Each template should have placeholders (date, time, incident ID, summary of impact, contact person) and should be reviewed by legal before use. As one guide notes, it is critical to clarify "who needs to be informed… which communication channels should be used, and what level of detail should be provided"[25]. In all cases, communications must align with the policy's rules on sharing (e.g. not revealing sensitive information unnecessarily).

By predefining these matrices and templates, the team can escalate incidents swiftly and keep stakeholders informed without delay or confusion[11][25].

4. Incident Response Checklist

An initial response checklist helps first responders ensure nothing is missed. Key steps include:

- **Verification:** Confirm that alerts or signs truly indicate an incident (rule out false positives). Check logs and monitoring tools for corroborating evidence.
- **Notification:** Immediately activate the IR team. Notify the Incident Manager and key team members per the escalation matrix[25]. If warranted by severity, notify senior management and any legal/regulatory parties.
- **Evidence Preservation:** Before isolating systems, preserve volatile data (e.g. memory dumps, network captures) and static evidence (log files, disks). For example, one should immediately start "recording all facts regarding the incident" in a secure logbook or database[13]. Ensure chain-of-custody for any collected evidence.
- **Containment/Isolation:** Once evidence is secured, isolate affected systems to prevent further damage. This may include disconnecting networks, disabling compromised accounts, or shutting down malicious processes. Log each action.
- **Documentation:** Keep a detailed timeline of all actions from detection onward. NIST advises documenting every step with date/time and handler's signature[14]. Record incident status, summary, indicators, and next steps in the incident log[15].
- **Communication:** Use predefined templates to inform stakeholders of the situation. For example, send an initial "Security Incident Notification" email to relevant parties with basic facts and warnings. Update the communications log for any calls/emails sent.
- **Law Enforcement/Regulatory:** If the incident involves criminal activity or regulated data, engage law enforcement or breach-notification processes per policy.
- **Post-Containment:** Verify that the threat is fully contained. Capture post-incident evidence if needed. Begin recovery steps (see below).

Each of these checklist items should be ticked off and annotated in real time by the response team. Crucially, NIST recommends that "every step taken from the time the incident was detected to its final resolution should be documented and timestamped"[14], and that logs be

maintained by one person while others perform technical work. This ensures a systematic, well-coordinated response.

5. Incident Response Playbook Template

A playbook provides step-by-step guidance **by incident type** and **by IR phase**. It typically has sections for each major incident category (e.g. *Malware/Ransomware*, *Phishing*, *Data Breach*, *Denial of Service*, etc.), and under each type, subsections for the lifecycle phases. Below is a simplified template outline (to be customized):

Incident Type: [e.g. Ransomware, Phishing, Data Breach, DoS]

1. Preparation

- *Ensure staff training and awareness*
- *Maintain updated tools (AV, IDS/IPS, SIEM)*
- *Backup systems regularly*
- *Define contact lists and escalation paths*

2. Detection & Analysis

- *Identify potential incident via alerts/logs/reports*
- *Verify incident (rule out false positives)*
- *Collect initial indicators (IP addresses, file hashes, logs)*
- *Assess scope and severity*

3. Containment

- *Isolate affected systems (disconnect network, disable accounts)*
- *Implement temporary controls to limit spread*
- *Preserve volatile data before shutdown*

4. Eradication

- *Remove malicious code or unauthorized access*
- *Patch vulnerabilities or misconfigurations*
- *Validate eradication with system scans*

5. Recovery

- *Restore systems from clean backups*

- *Validate system integrity and monitor for reinfection*
- *Re-enable business functions gradually*

6. Post-Incident / Lessons Learned

- *Conduct debrief with IR team and stakeholders*
- *Document timeline, findings, and impact*
- *Update playbook, policies, and training*
- *Implement preventive measures (new controls, awareness campaigns)*

Each phase above follows NIST's IR process model (Preparation → Detection & Analysis → Containment → Eradication & Recovery → Post-Incident)[18]. The playbook should be as detailed as possible (listing tools, scripts, log locations, contact persons, etc.) but also easy to follow under stress. By having a structured template, responders can quickly skip to the relevant section when a particular incident type occurs.

6. Project Visuals

4-Week Project Timeline

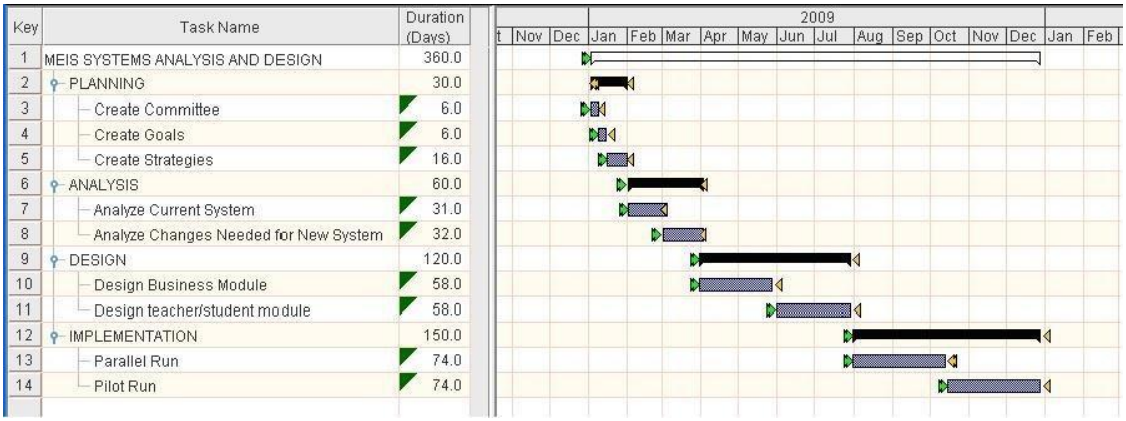

Figure: Example 4-week IR project timeline with tasks and milestones. The above Gantt chart illustrates a sample schedule for a 4-week incident response project. Week 1 might include tasks like drafting the IR policy, forming the IR team, and developing the communications plan. Week 2 could cover team training, tabletop exercises, and contingency planning. Week 3 and 4 would implement the playbook development, finalize documentation, and obtain management approvals. Such a timeline helps ensure each deliverable has clear deadlines and resource assignments, and that critical milestones (e.g. Policy approval, team readiness) are met on schedule.

IR Team Structure and Policy Diagram

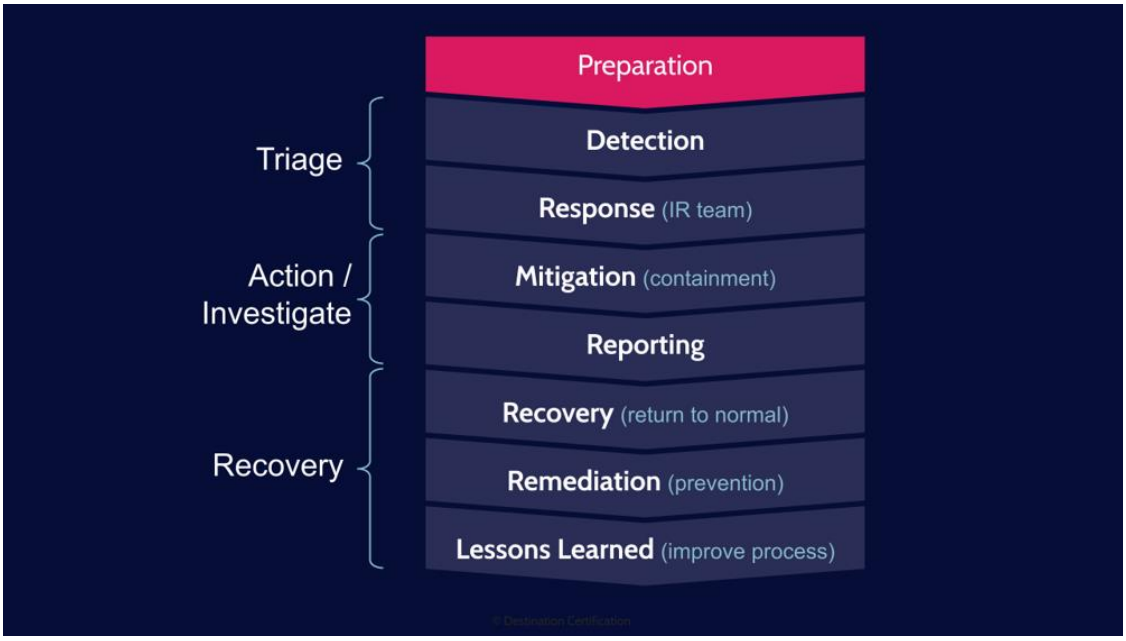

Figure: High-level incident response lifecycle phases (Preparation to Lessons Learned). This conceptual diagram shows the main phases of incident response and illustrates how Week 1 outputs align with the "Preparation" stage (establishing policy and roles) and early "Detection/Response" activities. It emphasizes a structured approach from preparation through containment to recovery and continuous improvement. The stages shown are consistent with industry guidance (NIST SP 800-61) on the IR lifecycle[18]. By visualizing the phases, the chart underscores that the IRT's roles and the IR policy feed into a coordinated process: first setting up (Prep), then detecting and responding to incidents, and later reviewing lessons learned.

Sources: Authoritative IR frameworks and publications informed this content, including NIST SP 800-61r2 guidelines[3][1] and practitioner references[5][6]. All recommendations above reflect industry best practices for incident response (e.g. alignment with NIST 800-61 rev.2)[1][18]. Any images included are for illustrative purposes and are either public-domain examples or conceptual diagrams.

---

[1] [2] [3] [11] [12] [13] [14] [15] [16] [17] Computer Security Incident Handling Guide

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[4] [20] [22] Who Should Be On Your Incident Response Team? | xMatters

https://www.xmatters.com/blog/who-should-be-on-your-incident-response-team

[5] [7] [8] [9] [10] [19] [21] Incident response team depth chart: Roles & responsibilities | Wiz

https://www.wiz.io/academy/incident-response-team

[6] How to use the incident response lifecycle: NIST, CISA, & SANS | PDQ

https://www.pdq.com/blog/how-to-use-incident-response-lifecycle/

[18] [25] NIST Incident Response: 4-Step Life Cycle, Templates and Tips

https://www.cynet.com/incident-response/nist-incident-response/

[23] resource.redcanary.com

https://resource.redcanary.com/rs/003-YRU-314/images/RACI_Matrix_CompanionGuide_RedCanary.pdf

[24] [DOC] Cyber Incident Response Standard - CIS Center for Internet Security

https://www.cisecurity.org/-/media/project/cisecurity/cisecurity/data/media/files/uploads/2020/06/Cyber-Incident-Response-Standard.docx