

The background is a dark gradient, transitioning from a slightly lighter grey at the top to a deep black at the bottom. Scattered across this background are numerous water droplets of various sizes. Some droplets are large and prominent, showing clear highlights and reflections, while others are small and subtle. The droplets are primarily located in the upper left and lower right areas, with a few smaller ones in the center.

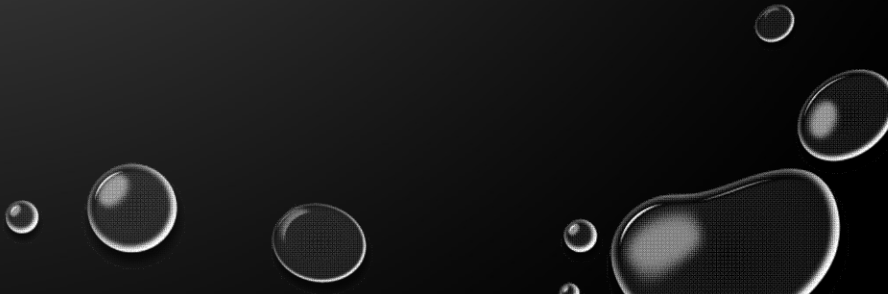
INCIDENT RESPONSE PLAN

ANEES AHMED



PURPOSE

THIS DOCUMENT ESTABLISHES THE PROCEDURES FOR IDENTIFYING, REPORTING, AND RESPONDING TO AN INFORMATION SECURITY INCIDENT. IT ESTABLISHES THE BASIC LANGUAGE TO DISCUSS SUCH EVENTS, IDENTIFIES ROLES AND RESPONSIBILITIES INVOLVED IN RESPONDING TO AND RECOVERING FROM THESE EVENTS, AND PROVIDES A PROCESS FOR HANDLING THESE EVENTS FROM THE TIME AN EVENT IS DETECTED TO THE FINAL DEBRIEFING AND CLOSEOUT.





SCOPE

THIS PLAN APPLIES TO ALL INCIDENTS THAT MAY IMPACT THE SECURITY, INTEGRITY, AVAILABILITY, AND CONFIDENTIALITY OF THE ORGANIZATION'S INFORMATION SYSTEMS.



INCIDENT RESPONSE TEAM (IRT)

- INCIDENT COMMANDER
- TECHNICAL LEAD
- COMMUNICATIONS OFFICER
- LEGAL ADVISOR
- HR REPRESENTATIVE

INCIDENT IDENTIFICATION AND SCENARIOS

TYPES OF INCIDENTS:

- DATA BREACH
- MALWARE INFECTION
- DENIAL-OF-SERVICE (DOS) ATTACK
- INSIDER THREAT
- PHISHING ATTACK
- PHYSICAL SECURITY BREACH

Incident Scenarios:

Scenario 1: Unauthorized access to sensitive data

Scenario 2: Ransomware infection spreading through the network

Scenario 3: DoS attack affecting website availability

Scenario 4: Phishing email compromising user credentials

Scenario 5: Physical theft of a company laptop containing sensitive information

ROLES AND RESPONSIBILITIES

1. INCIDENT COMMANDER:

- LEADS THE RESPONSE EFFORT.

2. Technical Lead

- Analyzes the incident.

3. Communications Officer

- Manages internal and external communications related to the incident.

4. Legal Advisor

- Provides guidance on legal and regulatory obligations during the incident.

5. HR Representative

- Manages any personnel-related issues arising from the incident.

INCIDENT RESPONSE PROCEDURES

1. DETECTION AND IDENTIFICATION

- MONITORING
- ALERTING
- INITIAL ASSESSMENT

2. CONTAINMENT

Isolate affected systems to prevent the incident from spreading.

3. ERADICATION

REMOVE MALICIOUS CODE, PATCH VULNERABILITIES, AND SECURE ENTRY POINTS TO PREVENT RE-INFECTION.



CONTINUE...

4. RECOVERY

RECOVER LOST OR CORRUPTED DATA, ENSURING ITS INTEGRITY AND COMPLETENESS.

5. POST-INCIDENT REVIEW

CONDUCT A DEBRIEF WITH THE INCIDENT RESPONSE TEAM TO REVIEW THE INCIDENT RESPONSE PROCESS.



The background of the slide is dark gray with several translucent, realistic-looking bubbles of various sizes scattered across it, particularly concentrated in the top-left and bottom-right corners.

TRAINING AND SIMULATION EXERCISES

- REGULAR TRAINING

PROVIDE CONTINUOUS TRAINING TO THE INCIDENT RESPONSE TEAM.

- TABLETOP EXERCISES

CONDUCT TABLETOP EXERCISES TO SIMULATE VARIOUS INCIDENT SCENARIOS AND PRACTICE RESPONSE ACTIONS.

- FULL-SCALE DRILLS

PERIODICALLY RUN FULL-SCALE DRILLS TO TEST THE PLAN UNDER REALISTIC CONDITIONS, INVOLVING ALL RELEVANT STAKEHOLDERS.



PLAN REVIEW AND MAINTENANCE

- PERIODIC REVIEW

REVIEW THE INCIDENT RESPONSE PLAN EVERY TO ENSURE IT REMAINS UP-TO-DATE WITH CURRENT THREATS, TECHNOLOGIES, AND ORGANIZATIONAL CHANGES.

- FEEDBACK INCORPORATION

INCORPORATE FEEDBACK FROM TRAINING EXERCISES, ACTUAL INCIDENTS, AND CHANGES IN THE ORGANIZATIONAL ENVIRONMENT INTO THE PLAN.

- DOCUMENTATION

KEEP ALL DOCUMENTATION UP-TO-DATE.