Incident Response Plan
For
Deerfield Beach Police Department

Prepared by: DeerGuard Defenders - Cyber Security Intern Team

Aadith Preetham (C0902681)

Version 1.0 | Last Reviewed: 30 Jan 2025

Table of Contents

Summary

The Deerfield Beach Police Department (DBPD) functions in a digital landscape where cyber threats are a significant risk to the department's operations and public safety. This Incident Response Plan is designed to provide a structured approach for identifying, tackling and recovering from incidents that are a threat to DBPD's network, data and infrastructure.

A recent incident that took place in South Korean Military's Cyber Command shows how outdated software, weak authentication and poor monitoring can be a threat to an entire department and cause the operations to disrupt. By integrating lessons from this incident, DBPD's Incident Response Plan makes sure that the department operations remain smooth and the department remains resilient to any potential attacks or incidents.

The plan follows a framework provided by NIST and a template by CyberSecure Canada to provide a step-by-step approach for handling incidents. Preparation, Identification, Containment, Eradication, Recovery and Post-Incident are aspects covered. The plan also provides a checklist for DBPD to follow during an incident to ensure quick actions. By implementing this plan, DBPD improves its ability to protect important data, maintain smooth operations and have as few disruptions as possible caused by cyber threats.

Revision History

Date	Version	Modification	Modifier
25 Jan 2025	1.0	Initial Draft	Aadith Preetham
28 Jan 2025	1.1	Integration of Korean Cyber Command Case Study and contact lists	Aditi Jadyal
30 Jan 2025	1.2	Addition of hierarchical flowchart and references	Pratik Dhakal

Testing and Review Cycle

- The IRP will be reviewed annually and tested twice a year through simulations and tabletop exercises.
- An Incident Response Team will assess the plan's effectiveness and update it accordingly.
- Testing will simulate real-world scenarios, including DDoS attacks, ransomware, insider threats, and phishing campaigns.

Introduction

Purpose:

This Incident Response Plan ensures that DBPD can detect, respond to, and recover from cybersecurity incidents effectively.

The Korean Cyber Command breach exposed vulnerabilities in national security systems due to outdated software and weak authentication. DBPD applies these lessons to prevent, detect, and mitigate threats against police infrastructure and protect sensitive law enforcement data.

Scope:

- Applicable to all DBPD networks, systems, devices, and data.
- Covers employees, contractors, third-party vendors, and any external entities with access to DBPD systems.
- Ensures continuity of law enforcement operations while safeguarding public data.

Definitions

1. Confidentiality: Protecting sensitive personal information like social insurance numbers and driver's license details from unauthorized access.
2. Cyber Security Event: Any observable activity within a system or network, such as sending an email or accessing a file.
3. Incident Response Team: A dedicated team responsible for managing cybersecurity incidents.
4. Indicators of Compromise(IoC): Hints that show an ongoing or past cyber attacks like suspicious logins in the system logs, unauthorised file modifications, etc
5. Service Availability: The reliability of a system being accessible to users, typically measured as a percentage of uptime.
6. SLA (Service Level Agreement): A commitment defining expected service reliability, often with financial penalties for non-compliance.
7. Stakeholder Relationship Map: A diagram showing relationships within an organization to assess IT risks and security strategies.
8. Vulnerability: A flaw or weakness in a system that can be exploited for malicious purposes.
9. War Room: A dedicated, well-equipped space for managing critical incidents in real-time.
10. Zero-Day Exploit: A weakness in the system exploited before a fix is available.

How to recognise if we’re down?

Cybersecurity incidents can sometimes go unnoticed initially but may show signs of unusual activity or misuse within your systems or by external partners. Here are some clear indicators that something may be wrong:

1. Strange Login Activity: Unusual or excessive logins, especially from accounts that haven’t been used in a long time.
2. Unexpected Remote Access: Suspicious or frequent remote access attempts, either by staff or external service providers.
3. Unfamiliar Wi-Fi Networks: New or unknown wireless networks appearing near department systems.
4. Suspicious Files or Programs: The presence of unusual software, malware, or programs that weren’t approved or installed by the team.
5. Key-Logging Devices: Discovery of devices or software that secretly track what is typed on department computers.
6. Odd Website Behavior: Department websites or systems acting unusually, such as showing errors or behaving in unexpected ways.
7. Tampered Payment Devices: Card readers or payment terminals showing signs of physical or digital interference.
8. Skimming Devices: Discovery of tools meant to steal card information from payment systems.
9. Missing Payment Records: Lost or misplaced receipts or documents with sensitive payment details.
10. Lost or Stolen Equipment: Missing laptops, hard drives, or other devices containing sensitive police data.

Recognizing these signs early is key to protecting department systems and sensitive information. Stay vigilant and report anything unusual immediately.

Incident Response Team

Role Title	Definition
Incident Response Team Lead	Responsible for managing and coordinating the entire incident response process. Makes key decisions during incidents and ensures all team members fulfill their responsibilities effectively.
Incident Handler	Acts as the primary point of contact for managing incidents. Organizes team efforts and initiates the Incident Response Plan to address and resolve security threats.
Communications	Handles internal and external communications during an incident. Ensures timely updates are provided to stakeholders, staff, and the public, as needed.
Network Engineer	Provides technical expertise related to network security. Monitors, analyzes, and mitigates threats to network infrastructure.
Desktop Technician	Focuses on the security and functionality of desktop systems. Provides support for endpoints impacted by incidents.
Server Specialist	Ensures the security and operational stability of servers. Handles threat removal and system restoration tasks.
Legal Advisor	Provides legal expertise to ensure compliance with regulations. Advises on incident communication strategies and potential liabilities.

Responsibilities of All DBPD Staff Members:

1. Ensure the staff is familiar with how to recognize and report any suspected or confirmed security incidents.
2. Promptly report any suspected or actual security incidents to the Incident Handler or another member of the Incident Response Team
3. Notify the supervisor or an IRT member about any security-related concerns or issues.
4. Follow the Deerfield Beach Police Department's security policies and procedures, including any temporary or updated measures introduced to maintain operations, recover from an incident, or prevent future incidents.

Contact Information:

Department Contacts:

Role	Name	Title	Phone	Email
Incident Handler (Lead)	Jay Chhanang	Cybersecurity Officer	555-0101	j.chhanang@dbpd.gov
Incident Handler (Backup)	Mishika C.	IT Manager	555-0102	m.chhanang@dbpd.gov
Note-taker	Mark Taylor	Admin Assistant	555-0103	m.taylor@dbpd.gov
Communications	Sarah Lee	Communications Officer	555-0104	s.lee@dbpd.gov
Network	Linda B	Network Engineer	555-0105	l.bray@dbpd.gov
Server	Xytus Joseph	Server Specialist	555-0106	x.joseph@dbpd.gov
Legal	Ohm Trivedi	Legal Advisor	555-0107	o.trivedi@dbpd.gov
Executive	Jishant Acahrya	Chief of Police	555-0108	j.acharya@dbpd.gov

External Contacts:

Role	Organization	Name	Title	Phone	Email
Network Security Vendor	TechSecure Solutions	Peter Clark	Support Lead	555-0201	p.clark@techsecure.com
Cyber Insurance Provider	SafeNet Insurance	Amanda White	Account Manager	555-0202	a.white@safenet.com
Legal Counsel	LegalEase Law Firm	Laura Green	Lawyer	555-0203	l.green@legalease.com
Ransomware Response Team	Encryptor Recovery Inc.	Rachel Adams	Recovery Manager	555-0204	r.adams@encryptor.com
Data Backup Vendor	CloudSafe Solutions	David Parker	Account Manager	555-0205	d.parker@cloudsafe.com
Card Payment System Vendor	SecurePay Ltd.	Karen Taylor	Support Lead	555-0206	k.taylor@securepay.com

Incident Types and Severity Matrix

Here is a list of possible incidents that could occur at the Deerfield Beach Police Department (DBPD):

1. Unauthorized Access or Usage: Someone gains unauthorized physical or digital access to DBPD's network, systems, or sensitive data.
2. Service Interruption or Denial of Service (DoS): An attack that disrupts DBPD's systems or network, preventing normal operations.
3. Malicious Code: Installation of malicious software (e.g., viruses, worms, Trojans) that compromises police systems.
4. Ransomware: A type of malicious software that encrypts DBPD's files and demands payment to restore access.
5. Distributed Denial of Service (DDoS): Overwhelming DBPD's online services with excessive traffic, making them unavailable to users.
6. Network System Failures (Widespread): An incident that affects the availability or security of DBPD's network infrastructure.
7. Application System Failures: Disruption or compromise of software applications critical to DBPD operations.
8. Unauthorized Disclosure or Loss of Information: Accidental or deliberate exposure or loss of sensitive law enforcement data.
9. Privacy Breach: A breach involving the unauthorized release of personal information, such as criminal records or employee data.
10. Account Data Compromise: Unauthorized access to accounts containing sensitive authentication data or login credentials.
11. Other: Any other incidents impacting DBPD's networks, systems, or data, such as insider threats or physical theft of IT equipment.

Incident Severity Levels:

Severity Level	Description	Response
Critical	Data breach affecting law enforcement operations	Activate full IRT, notify FBI/CISA
High	Ransomware attack on critical systems	Isolate infected systems, implement backups

Medium	Phishing attempts detected	Security awareness training, email filtering
Low	Minor security policy violation	Internal corrective action

Incident Response Plan

This plan outlines the process for identifying, managing, and resolving cybersecurity incidents at the Deerfield Beach Police Department (DBPD). It divides the response process into distinct phases and assigns responsibilities to ensure effective resolution.

Phase 1: Preparation

To do:

- Train staff to recognize and report incidents.
- Conduct regular security awareness programs and phishing simulations.
- Maintain and test incident response tools like firewalls, endpoint protection, and backup systems.
- Define roles and responsibilities of the Cyber Security Incident Response Team (IRT).
- Perform regular vulnerability assessments and patch management.

Roles involved:

- Incident Response Team Lead: Oversees preparation efforts and ensures readiness.
- IT Manager: Manages technical preparations and infrastructure security.
- Admin Assistant: Maintains documentation and training records.

Phase 2: Identification

To do:

- Monitor systems using Security Information and Event Management (SIEM) tools.
- Investigate alerts for signs of suspicious activity (e.g., unusual login attempts, unauthorized access).
- Validate reported incidents from staff or external notifications.
- Classify incidents based on severity (e.g., Critical, High, Medium, Low).

Roles involved:

- Network Engineer: Monitors system traffic and analyzes anomalies.
- Incident Handler: Leads the investigation and confirms incident status.
- Server Specialist: Identifies and logs server-related issues.

Phase 3: Containment

To do:

- Disconnect compromised systems from the network.
- Apply network segmentation to isolate affected areas.
- Disable compromised accounts and block malicious IP addresses.
- Deploy temporary security measures, such as restricting external access.

Roles Involved:

- Incident Response Team Lead: Coordinates containment efforts.
- IT Manager: Implements technical controls to isolate threats.
- Network Engineer: Ensures network segmentation and containment.

Phase 4: Eradication

To do:

- Perform malware removal using Endpoint Detection and Response (EDR) tools.
- Patch vulnerabilities identified during the investigation.
- Reconfigure security controls to close exploited gaps.
- Conduct forensic analysis to ensure all threats have been removed.

Roles Involved:

- Server Specialist: Cleans and restores affected servers.
- IT Manager: Verifies successful eradication of threats.
- Incident Handler: Ensures proper documentation of eradication steps.

Phase 5: Recovery

To do:

- Restore systems from secure, verified backups.
- Test systems to confirm they are clean and functioning correctly.
- Monitor network traffic and logs for signs of reinfection or new threats.
- Notify stakeholders when systems are operational.

Roles Involved:

- Server Specialist: Leads system restoration efforts.
- Communications Officer: Updates stakeholders on recovery progress.
- Incident Response Team Lead: Oversees the recovery process.

Phase 6: Post-Incident Activity

To do:

- Conduct a post-mortem review to identify root causes and lessons learned.
- Document the incident, response actions, and outcomes.
- Update security policies and refine the incident response plan.
- Provide refresher training to staff and IRT members.

Roles Involved:

- Admin Assistant: Compiles and organizes post-incident reports.
- Legal Advisor: Ensures compliance with legal and regulatory requirements.
- Incident Response Team Lead: Oversees the post-incident review.

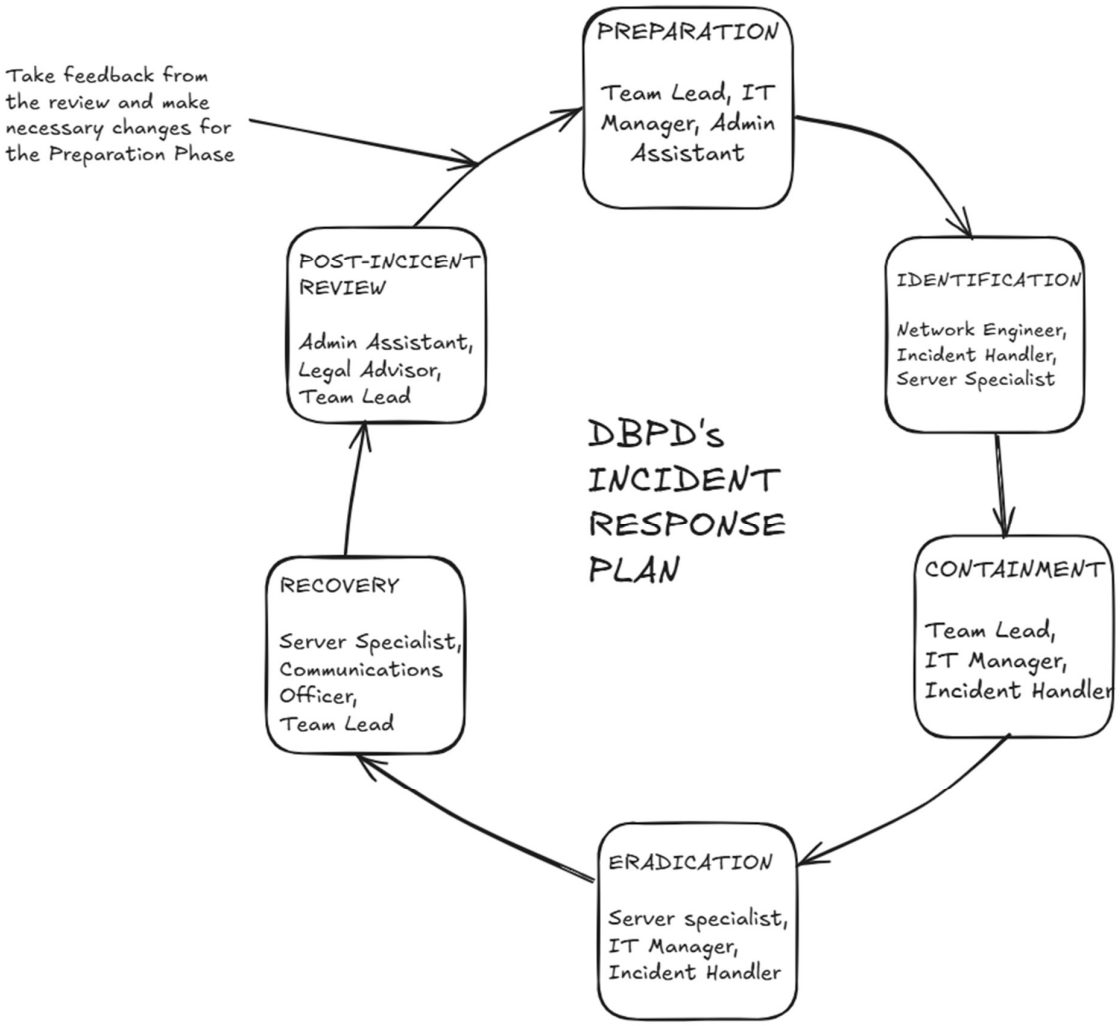

Fig 1: Flowchart for IRP

References

- Calendar for 5/23/2020 - The Florida Senate. (2020). Retrieved from Flsenate.gov: https://www.flsenate.gov/
- Canada, P. S. (2018, December 21). Cyber Security. Retrieved from www.securitepublique.gc.ca: https://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/index-en.aspx
- Canada, P. S. (2024, April 29). Federal Cyber Incident Response Plan. Retrieved from www.publicsafety.gc.ca: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/fdrl-cbr-ncdnt-rspns-pln-2023/index-en.aspx

- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *Computer Security Incident Handling Guide*, *2*(2). https://doi.org/10.6028/nist.sp.800-61r2
- CIS. (2018). CIS. Retrieved from CIS: https://www.cisecurity.org/
- Government of Canada, I. (2021, December 8). Develop an Incident Response Plan: Fillable template and example. Retrieved from ised-isde.canada.ca: https://ised-isde.canada.ca/site/cybersecure-canada/en/certification-tools/develop-incident-response-plan-fillable-template-and-example
- Kirvan, P. (2024, October 16). 5 critical steps to creating an effective incident response plan. Retrieved from SearchSecurity: https://www.techtarget.com/searchsecurity/feature/5-critical-steps-to-creating-an-effective-incident-response-plan
- MITRE. (2024). MITRE ATT&CK™. Retrieved from Mitre.org: https://attack.mitre.org/
- Security, C. C. for C. (2018, August 15). Canadian Centre for Cyber Security. Retrieved from Canadian Centre for Cyber Security: https://www.cyber.gc.ca/en/guidance/developing-your-incident-response-plan-itsap40003