الكليـة الجامعـية
للعلوم التطبيقية
رائـــدة الإبـــداع

(incident response Plan for institution)

Prepared By : Malk Khalid All Banna

ID: 220210141

Cyber Security Engineering Major

Under The supervision Of :

Eng . Alaa All Qazzaz

SEPTEMBER 1, 2024

CONTENTS PAGE

Introduction:

This document presents a detailed Cybersecurity Incident Response Plan (CIRP) tailored for the institution. The purpose of this plan is to ensure effective management and response to any potential cybersecurity incidents. It outlines the responsibilities of the response team, defines the incident types, describes the communication procedures, and provides a structured approach to containment, remediation, and recovery. The goal is to minimize the impact of incidents on the institution and to restore services as quickly as possible.

Purpose :

1. **Immediate incident containment** to protect critical services like payroll, IT, and public utilities.
2. **Protect sensitive data** such as legal and financial records from breaches.
3. **Ensure system integrity** by securing key infrastructure (firewalls, switches, servers).
4. **Maintain business continuity** by rapidly restoring essential operations.
5. **Clarify responsibilities** for coordinated incident response across departments.
6. **Address risks from outdated systems** and strengthen overall cybersecurity.
7. **Enhance long-term security** by implementing preventive measures and improving awareness.

Scope:

This plan applies to the entire IT infrastructure of the institution, which includes firewalls, switches, servers, virtual machines, employee workstations, and networked devices such as printers. It covers any potential incidents that may affect the confidentiality, integrity, or availability of institutional data and systems.

Incident Identification:

Upon detection of a cybersecurity incident, it is critical that the individual or system identifying the issue (whether it is IT staff, a user, or a third-party vendor) immediately reports the incident to the Incident Response Manager. The following questions should be addressed as part of the initial investigation:

-What is the nature of the incident? (e.g., malware infection, unauthorized access, data breach)

-What systems are affected?

-How severe is the impact on the organization's operations?

-What is the suspected cause of the incident?

Roles and Responsibilities

⇨ Points of Contact for Reporting Cyber Incidents

Name	Contact Details	Role Title	Responsibilities
....	Phone Number & email	On-Call IT Point of Contact	Primary Point of Contact

⇨ Cyber Incident Response Team (CIRT)

Include details of the CIRT responsible for managing responses to cyber incidents.

CIRT Role Title	CIRT Responsibilities
Cyber Incident Manager	• Response planning • CIRT Operations
Deputy Cyber Incident Manager	• Situational analysis • Threat intelligence • Technical advice
Security Manager	• Investigation (if suspected internal threat) • Law enforcement liaison
Incident Responder	•Technical investigation (collection and processing of network and host data) • Containment, remediation and recovery efforts • Investigation findings report
Communications, engagement and media advisor	• Information and warnings • Internal communications • Media and community liaison/ spokesperson
Business continuity advisor	• Facilities support • Business and community consequence analysis/ management
Legal advisor	• Legal advisory services (incl. regulatory compliance)
Finance and procurement advisor	• Facilities and finance support
Administration and record keeping	• Administration support, incl. Incident Log, Evidence and Situation Reporting

⇨ Senior Executive Management Team (SEMT)

Significant cyber incidents may require the formation of the SEMT to provide strategic oversight, direction and support to the CIRT, with a focus on:

- Strategic issues identification and management
- Stakeholder engagement and communications (including Board and ministerial liaison, if applicable)
- Resource and capability demand (including urgent logistics or finance requirements, and human resources considerations during response effort).

Title	SEMT Role
Chief Executive Officer	SEMT Chair
Chief Information Officer	SEMT Deputy Chair
Chief Information Security Officer	SEMT Deputy
Chief Operating Officer	Operational functions of the institution
Legal Council	Regulatory compliance, cyber insurance
Media and Communications Manager	Public relations and stakeholder engagement
Media and Communications Manager	Staff welfare management

Incident Severity Levels:

The severity of an incident will determine the scale of the response. This institution will classify incidents into three levels based on their impact:

1. **High Severity (Level 1) :**

- Systems critical to operations are compromised.
- Sensitive data such as personally identifiable information (PII) is exposed.
- Widespread disruption to business operations or theft exceeding $10,000.

2. **Medium Severity (Level 2) :**

- Moderate impact on business operations, such as partial system downtime or exposure of limited sensitive information.
- No immediate evidence of data theft, but systems have been compromised.

3. **Low Severity (Level 3) :**

- Minor incidents that have limited impact on operations and no exposure of sensitive data.
- For example, failed phishing attempts or temporary malware infections with no data loss.

⇨ Incident register table

#	incident	Date and Time Detected	Current Status	Incident Type	Incident Priority	Incident Impact	Assistance Required	Actions Taken to Resolve Incident	Contact Details
1	Expired CISCO ASA 5525 Firewall exploited	01/10/2024, 10:15 AM	New	Unauthorized Access	High	Firewall breached, internal network exposed. Affected systems: network infrastructure, internal databases. Public services at risk due to potential data breach.	Law enforcement, cybersecurity consultants	Firewalls were manually reconfigured to block access; investigation launched to track unauthorized entry	Name :........ Phone Number.... Email.......
2	Outdated Cisco switches causing network outage	02/10/2024, 01:30 PM	In Progress	Denial of Service (DoS)	Medium	Network communication disrupted due to failure of outdated switches. Affected systems: internal communications, public-facing websites. No public safety impact but operational downtime observed.	External network experts for switch replacement	Manual switch reset, replacement order placed, rerouting of traffic to minimize downtime	Name :........ Phone Number.... Email.......
3	Malware on employee workstations	03/10/2024, 09:00 AM	Resolved	Malware Infection	High	Malware spread through traditional antivirus failures. Affected systems: 25 workstations, financial databases. Public services temporarily impacted, financial data potentially compromised.	Law enforcement for data theft investigation	Workstations isolated, anti-malware tools deployed, and affected systems cleaned. Financial data audit conducted.	Name :........ Phone Number.... Email.......
4	Surveillance camera hack	03/10/2024, 11:20 AM	New	Unauthorized Access	Medium	Cameras hijacked for potential spying or tampering. Affected systems: physical security, potential privacy violations. Public safety not directly impacted, but organizational security weakened.	Law enforcement for physical breach review	Camera network isolated; external IP access blocked, camera system review and reconfiguration initiated.	Name :........ Phone Number.... Email.......
5	Misconfigured VMware ESXi leading to data breach	04/10/2024, 04:00 PM	In Progress	Unauthorized Access	High	Virtual machines exposed, data breach risk high. Affected systems: virtual servers, customer databases. Public services impacted, potential data leakage.	Cybersecurity consultants, law enforcement	Misconfiguration addressed, affected VMs isolated. Incident under investigation to determine extent of data exposure.	Name :........ Phone Number.... Email.......
6	Ransomware attack due to lack of EDR	05/10/2024, 08:15 AM	New	Ransomware	High	20 machines infected, files encrypted. Affected systems: HR and financial databases. Public services disrupted due to data access restrictions.	Law enforcement, ACSC	Incident isolation ongoing, ransom demands refused, backup data restoration started.	Name :........ Phone Number.... Email.......
7	Phishing attack resulting in credential theft	06/10/2024, 02:40 PM	In Progress	Phishing	Medium	Employee credentials stolen, unauthorized system access possible. Affected systems: internal applications, email systems. No immediate public service impact.	No external assistance required	Credentials revoked, affected accounts reviewed. Two-factor authentication (2FA) enabled for impacted employees.	Name :........ Phone Number.... Email.......
8	Wireless network breach through guest access	07/10/2024, 11:00 AM	New	Unauthorized Access	High	Unauthorized access to internal systems via guest wireless network. Affected systems: employee databases, visitor access logs. Public services potentially at risk if sensitive data is accessed.	Cybersecurity experts, law enforcement	Guest network disabled, investigation into breach origins, wireless segmentation initiated.	Name :........ Phone Number.... Email.......
9	Denial of Service attack on VOIP systems	07/10/2024, 03:30 PM	Resolved	DDoS	Medium	Communications down, internal voice services disabled. Affected systems: VOIP systems, communications infrastructure. Public services briefly impacted due to communication outages.	External communication infrastructure experts	Mitigation tools deployed, traffic rerouted, and VOIP systems restored to full service.	Name :........ Phone Number.... Email.......
10	Database compromise due to lack of encryption	08/10/2024, 12:00 PM	New	Data Breach	High	Customer and employee data compromised. Affected systems: HR, finance, and customer databases. Public services impacted due to potential identity theft and financial loss.	Law enforcement, external cybersecurity firm	Incident containment ongoing; database encryption initiated, further access restricted to compromised databases.	Name :........ Phone Number.... Email.......
11	Physical breach in server room	08/10/2024, 10:30 PM	In Progress	Physical Breach	Medium	Physical access to servers gained, potential hardware tampering. Affected systems: virtual servers, internal communications. Public services not immediately impacted but data at risk.	Law enforcement for physical security review	Incident investigation ongoing; biometric access enforced, review of physical security measures initiated.	Name :........ Phone Number.... Email.......

⇨ Incident register table

12	Outdated software causing vulnerability	09/10/2024, 01:15 PM	New	Software Vulnerability	Medium	Legacy system vulnerability detected. Affected systems: customer service software, finance applications. Public services slightly impacted due to software performance issues.	External software vendor support	Software patches applied, legacy systems in the process of being upgraded.	Name :........ Phone Number.... Email.......
13	Unnecessary services running on servers exploited	09/10/2024, 03:00 PM	Resolved	Exploitation of Misconfigured Service	Low	Unauthorized access to servers via unused services. Affected systems: internal servers, low-sensitivity databases. Public services not impacted.	No external assistance required	Unused services disabled, server configurations reviewed to prevent future issues.	Name :........ Phone Number.... Email.......
14	Minor data leakage from low-sensitivity databases	10/10/2024, 05:30 PM	Resolved	Data Leakage	Low	Limited access to non-critical data. Affected systems: low-sensitivity databases. Public services not impacted, minimal operational disruption.	No external assistance required	Data access revoked, affected databases encrypted. Incident marked as closed after confirming no further access points.	Name :........ Phone Number.... Email.......
16	Lack of centralized logging leading to delay in detection of security incidents	11/10/2024, 09:15 AM	New	Delayed Detection	High	Lack of SIEM caused delay in detection of breach. Affected systems: critical servers and databases. Public services indirectly impacted due to delayed response.	Law enforcement, cybersecurity consultants	SIEM implemented, logs reviewed manually, further investigations initiated.	Name :........ Phone Number.... Email.......
17	Physical security breach in server room	12/10/2024, 02:00 PM	New	Physical Security Breach	Medium	Server room access compromised, potential data and hardware tampering. Affected systems: physical servers. Public services could be impacted depending on data tampering.	Law enforcement for forensic analysis	Physical locks replaced, access restrictions enforced, further investigations ongoing.	Name :........ Phone Number.... Email.......
18	Unauthorized access through phishing attack	12/10/2024, 03:15 PM	New	Phishing	Medium	Employee credentials stolen via phishing email. Affected systems: email and internal databases. Public services not yet affected, but data exposure possible.	External forensic team	Affected accounts locked, phishing awareness training initiated, systems audit ongoing.	Name :........ Phone Number.... Email.......
19	Unauthorized access through legacy systems	13/10/2024, 02:45 PM	New	Unauthorized Access	High	Legacy systems exploited due to outdated software. Affected systems: finance and HR databases. Public services indirectly impacted due to data exposure.	External consultants for software upgrades	Legacy systems isolated, patches applied, upgrade roadmap initiated.	Name :........ Phone Number.... Email.......
20	Unauthorized access due to weak employee security awareness	14/10/2024, 09:30 AM	New	Social Engineering	High	Weak employee security awareness allowed unauthorized access. Affected systems: internal databases. Potential data leakage.	External training providers	Employee retraining initiated, affected accounts locked, investigation ongoing.	Name :........ Phone Number.... Email.......
21	Data leakage from unnecessary services running on servers	15/10/2024, 11:20 AM	Resolved	Data Breach	Low	Unnecessary services running on servers caused minor data leakage. Affected systems: non-critical databases. Public services not impacted.	No external assistance required	Unused services disabled, server configurations reviewed.	Name :........ Phone Number.... Email.......
22	Sudden power outage in data centers	01/09/2024, 10:15 AM	Resolved	Infrastructure	High	Data center down, impacting core systems. Public services and internal networks offline.	None at the moment	Power restored, systems rebooted, UPS inspection in progress	Name :........ Phone Number.... Email.......
23	Loss of a key employee	02/09/2024, 09:00 AM	In Progress	Human Resource	Medium	Project delays, knowledge gaps. No public impact, internal project timelines affected.	None required	Reassigning tasks, preparing cross-training documentation	Name :........ Phone Number.... Email.......
24	Fire occurrence in data centers	03/09/2024, 02:30 PM	New	Physical	High	Potential data loss, equipment damage. Emergency services contacted. Partial service outages in several departments.	Fire department, law enforcement	Fire suppression systems activated, evacuating building	Name :........ Phone Number.... Email.......
25	Water leakage in data centers	04/09/2024, 11:00 AM	Resolved	Infrastructure	Low	Minor leakage, no major systems affected. Inspections ongoing.	None required	Leak contained, systems inspected, preventive measures implemented	Name :........ Phone Number.... Email.......
26	Theft of servers and equipment	05/09/2024, 08:45 PM	In Progress	Security Breach	High	Several servers stolen, sensitive data compromised. Affected departments: Finance, HR, IT systems partially compromised.	Law enforcement, forensic analysis	Security systems reviewed, compromised systems isolated	Name :........ Phone Number.... Email.......

Incident Response Phases:

.1 . Detection and Reporting :

- All incidents should be reported immediately to the Incident Response Manager.
- A ticket should be created to track the incident's progress and resolution.

.2. Containment :

- Immediate actions are taken to contain the incident and prevent it from spreading further. This may include isolating affected devices, disabling compromised accounts, or modifying firewall settings.

.3. Eradication :

- Once the incident is contained, the underlying cause is identified and removed from the environment. This might involve patching vulnerabilities, removing malware, or enhancing security measures such as updating firewall rules or upgrading licenses (e.g., expired Cisco ASA 5525 firewall licenses).

.4. Recovery :

- Systems are restored to normal operations. The VMware ESXi virtual machines, servers, and services (e.g., Active Directory, databases, VOIP) are carefully brought back online, ensuring that all vulnerabilities have been addressed. Backup systems are validated to confirm data integrity.

5. .Post-Incident Review :

- A full review is conducted after the incident to assess the response, identify weaknesses, and improve future preparedness. This includes analyzing logs from firewalls, switches, and servers.

Communication Plan:

Effective communication during a cybersecurity incident is crucial. The following communication will be followed based on the incident's severity:

-Level 1 (High) :

- Immediate notification of the board of directors, relevant authorities, and affected stakeholders.
- Provide continuous updates to senior management.
- External communication, including customers, if sensitive data is breached.

-Level 2 (Medium) :

- Notify the executive team and affected internal stakeholders.
- Authorities and external stakeholders may be notified if required by regulations.
- Provide internal updates to relevant departments as the situation evolves.

-Level 3 (Low) :

- Notify internal teams and stakeholders.
- No external communication is required unless necessary.

Containment, Eradication, and Recovery:

.1.Containment:

- The IT Security Team will immediately isolate affected systems, such as the CISCO 4600 switches, and prevent further spread by updating firewall settings or disconnecting network devices.
- If necessary, quarantine affected servers in the HPE Gen10 DL380 rack.

.2.Eradication:

- Remove all traces of the threat from the environment. This could involve cleaning infected systems, updating firewall firmware, or addressing vulnerabilities in network configurations.

.3.Recovery:

- Restore affected services and systems, ensuring that no further vulnerabilities exist. Validate the integrity of the VMware ESXi virtual machines and ensure that services such as the Active Directory and databases are operational.

Post-Incident Evaluation:

After the incident is fully resolved, the team will conduct a comprehensive review to identify lessons learned and improve the response strategy. This review will examine system logs, firewall configurations, and incident reports to understand what went wrong and how future incidents can be prevented.

The findings will be used to update the organization's cybersecurity policies, including addressing outdated equipment, such as renewing the expired CISCO ASA 5525 licenses and upgrading security systems like EDR and antivirus solutions.