


King AbdulAziz University
Cyber-Security Center

Cyber-Security Incident Response Plan

Restricted-Internal

Document Authorization:

Role	Name	Date	Signature
Owner	Cyber-Security Center	14/11/2022 CE	

Document Versions:

Version	Date	Editor	Reasons for Revision
1.0	15/11/2021 CE	Maram bint Khalid Hambishi	

Table of Contents

<i>Objectives.....</i>	<i>4</i>
<i>Scope and Applicability of the Work.....</i>	<i>4</i>
<i>The Definition of “Incident”</i>	<i>4</i>
<i>The Cyber-Security Incident Response Team.....</i>	<i>4</i>
<i>Structure of the Cyber-Security Incident Response Team.....</i>	<i>6</i>
<i>Roles and Responsibilities of the Cyber-Security Incident Response Team</i>	<i>6</i>
<i>Cyber-Security Incident Response Plan-Operational Stages</i>	<i>8</i>

Objectives

The purpose of the Cyber-Security Incident Response Plan is to provide and fulfill cyber-security requirements, based on best practices and standards, relating to cyber-security incidents and threats pertaining to King AbdulAziz University, to reduce cyber-risks, and to protect the University from internal and external threats, through focus on the essential objectives of security, which are: Confidentiality, integrity, and availability of information.

Scope and Applicability of the Work

The Cyber-Security Incident Response Plan cover all King AbdulAziz University informational and technical assets, and applies to all King AbdulAziz University employees.

The Incident Response Plan also lays down essential guidelines for crisis-management at King AbdulAziz University, and defines potential crisis situations. This Plan does not cover all potential situations, but rather is comprised of the basic principles and operations necessary for the management of potential incidents.

This plan only applies to adverse events pertaining to computer security, not to those arising from natural disasters, power outages, etc.

The Definition of “Incident”

“Incident” is defined as a breach, or imminent threat of a breach, of computer security policies, acceptable use policies, or standard security practices that poses a risk to the confidentiality, integrity, or availability of informational resources or processes.

Incidents may have one or more of the following characteristics:

- An explicit or implicit breach of King AbdulAziz University cyber-security policies.
- Attempts to gain unauthorized access to King AbdulAziz University.
- Refusal of service to a King AbdulAziz University information source.
- Unauthorized use of or modification to King AbdulAziz University.
- Loss of confidentiality or protection for King AbdulAziz University information.

The Cyber-Security Incident Response Team

The cyber-security incident response team is the team responsible for decision-making, coordinating the efforts of concerned offices and entities internal and external to King AbdulAziz University, strategic partners, and external suppliers, and identifying the most suitable response to incidents when they occur, so as to allow for rapid and appropriate response to information security incidents. The cyber-security incident response team structure puts forward a three-tiered approach. The three tiers together work to build situational awareness through optimal information-sharing and teamwork. The following figure displays the proposed approach:

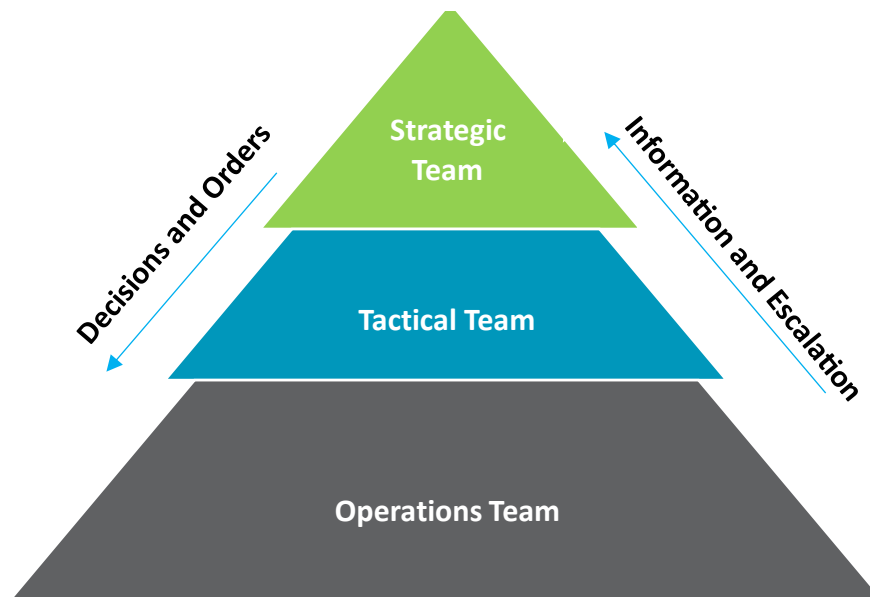


Figure 1: Approach to Incident Response Team Assignments

- **Strategic Team (Senior Management)**

The upper level of the Cyber-Security Incident Response Team is responsible for the Incident Management Plan, and provides overall direction and strategic guidance for incident management procedures to be undertaken by the tactical and operations teams. The Strategic Team has the authority to activate the management plan/plans when to do so is required. The Strategic Team consists of the following:

- The Supervisory Committee for Cyber-Security

- **Tactical Team (Middle Management)**

The second level is represented by the Tactical Team, which is responsible for overall tactical decision making and guidance concerning the operations space. The Tactical Team consists of the following:

- The Head of Cyber-Security Incident Response (the Director of the Cyber-Security Center)

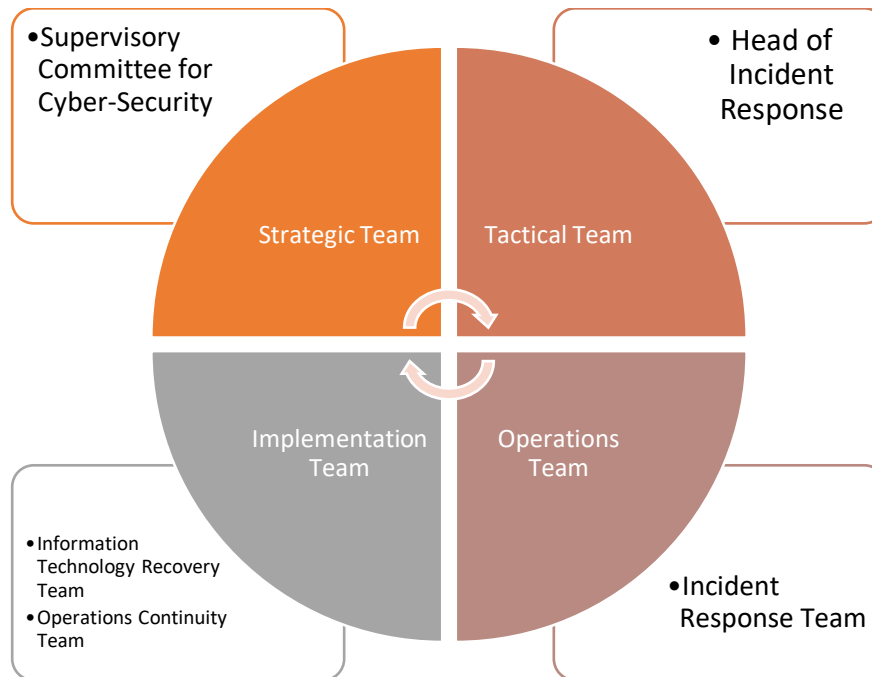
- **Operations Team**

The third tier is represented by the Operations Team, which is responsible for cyber-security incident response activities on the operational level, and for implementing the strategic and tactical decisions conveyed to them by the strategic and tactical teams. This team must be formed with reference to the character of operations teams and representatives in the field of cyber-security incident response. The operations team consists of the following:

- The Cyber-Security Incident Response Team
- The Information Technology Disaster Recovery Team
- The Operations Continuity Team

Structure of the Cyber-Security Incident Response Team

The Incident Response Team is composed of the members of the King AbdulAziz University Supervisory Committee for Cyber-Security, and the team is ultimately responsible for timely recovery and resumption of critical operations following catastrophic failure.



Roles and Responsibilities of the Cyber-Security Incident Response Team

*Roles and Responsibilities of the Strategic Team

Before Incidents
<ol style="list-style-type: none">1. Being composed of legal experts, risk managers, and other departmental administrators who may provide advice or information during incident response.2. Providing guidance concerning incident response activities relating to members' fields of specialization.3. Ensuring that incident response operations are conducted in accordance with legal, contractual, and regulatory requirements.
During Incidents
<ol style="list-style-type: none">1. Ensuring the availability of the resources necessary for effective management.2. Giving incident response administrators the necessary powers to quickly seize assets and cease services so as to contain a moderate or serious incident.3. Responding to any incident that has the potential to escalate into a crisis.4. Holding meetings in the physical or virtual Command Center immediately upon receiving notification.
After Incidents
<ol style="list-style-type: none">1. Announcing return to normal operations.

2. Reviewing and approving post-incident summary reports concerning the operations that were conducted during the crisis/disruption, and providing comments and recommendations.
--

***Roles and Responsibilities of the Tactical Team (Head of the Cyber-Security Incident Response Team)**

Before Incidents
<ol style="list-style-type: none">1. Ensuring that staff bearing responsibility for incidents response are sufficiently trained and aware to respond to incidents.2. Communicating with regulatory authorities, concerned entities, the general public, and staff.3. Reviewing the Cyber-Security Incident Response Plan (“the Plan”) to ensure that it fulfills policy objectives and reflects accurately the objectives of King AbdulAziz University.
During Incidents
<ol style="list-style-type: none">1. Making the necessary arrangements for alternative systems to enable operational continuity.2. Participating in tests of plans and procedures for cyber-security incident response.3. Bearing responsibility for internal and external communications pertaining to cyber-security incidents.4. Coordinating response operations with support administrators and external suppliers as needed to minimize damage to information resources.
After Incidents
<ol style="list-style-type: none">1. Securing assets.2. Ensuring the implementation of lessons learned.

***Roles and Responsibilities of the Operations Team**

Before Incidents
<ol style="list-style-type: none">1. Understanding the King AbdulAziz University Incident Response Plan and Procedures in order to be able to respond to incidents in an appropriate way.2. Participating in tests of the Cyber-Security Incident Response Plan and Procedures.3. Continually developing skills for cyber-security incident response management.
During Incidents
<ol style="list-style-type: none">1. Ensuring that all tools are used and managed in the proper way to raise alerts concerning security events/incidents.2. Analyzing network traffic for signs of denial of service attacks, distributed denial of service attacks, or other types of attack.3. Reviewing logs of important systems for signs of unusual activity.4. Monitoring the implementation of operations and services for signs of attacks.5. Gathering information relevant to incidents at the request of the Director of the Cyber-Security Center.
After Incidents
<ol style="list-style-type: none">1. Ensuring that all evidence and chains of custody are maintained appropriately.2. Preparing reports concerning security incidents, and participating in working meetings with the other teams and the Director of the Cyber-Security Center to discuss lessons learned.

Cyber-Security Incident Response Plan-Operational Stages

The Cyber-Security Incident Response Plan is essentially divided into four basic stages, described below, with the addition of details concerning the specific elements of the plan that are to be put into effect at each stage:

- **Detection and Escalation of the Incident**
- **Activation of the Plan and Response to the Incident**
- **Recovery**
- **Deactivation of the Plan and Return to Normal Operations**

Figure 2: Stages of the Cyber-Security Incident Response Plan

The following table describes the operations to be undertaken during the four stages of cyber-security incident response:

No.	Stage	Operations
1.	Detection and Escalation of the Incident	1. The individual or team that has detected the disruption contacts the relevant office (Information Technology, Cyber-Security, Human Resources, etc). 2. The relevant office escalates to the Tactical Team, which in turn escalates to the Strategic Team, following the Escalation Matrix, according to the classification of the incident. 3. The Head of the Crisis Management Team activates the Command Center,

		according to the information given him by the Strategic Team.
2.	Activation of the Plan and Response to the Incident	1. The Response Team activates the Plan, performs further research concerning the event, analyzes the details, meets with the Director of the Cyber-Security Center, and arrests the impact of the incident in accordance with its classification.
3.	Recovery	<p>1. Implementing recovery procedures, after the incident has been classified (for example, installing update packages for operating systems and applications, restoring backups, downloading protection software, restricting the use of user privileges, changing passwords, etc.), and including them in a security incident report.</p> <p>2. In the event that it is necessary to activate the Recovery and Operational Continuity Plan, the Tactical Team holds meetings with the Operations Team, the Implementation Team, and other concerned offices (Upper Management, Planning, etc.) to complete the process.</p>
4.	Deactivation of the Plan and Return to Normal Operations	1. A report is prepared concerning the incident, and meetings are held to discuss lessons learned.