


King AbdulAziz University
Cyber-Security Center

Cyber-Security Incident Recovery 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	Sultana bint Ahmad al-Ghamidi	

Table of Contents

<i>Objectives of the Plan</i>	4
<i>Scope and Applicability of the Work</i>	4
<i>Definition of “Disaster Recovery”</i>	4
<i>Steps for Addressing Emergencies</i>	4
<i>Appendices</i>	5

Objectives of the Plan

The purpose of this plan is to protect the University's electronic network and all its sources for electronic devices and services, according to their sensitivity and priorities, and to ensure the University's operation in the required manner in the event of a complete or partial breakdown. This is to be accomplished by advanced preparedness, by putting in place alternative and inventive plans based on sound strategic studies and the best prior historical experience, and by defining tasks and roles in a standardized and focused manner, so as to ensure their smooth and successful implementation in the event of disasters or emergencies.

Scope and Applicability of the Work

The Disaster Recovery Plan is a fundamental requirement for King AbdulAziz University, due to the fact that the University is an entity that provides services on a daily basis, and that this Plan is an operational one that describes how to quickly and effectively resume work after a disaster has occurred, how to maintain and quickly restore continuity of service operations, and how to ensure that the University's losses are minimized.

Definition of "Disaster Recovery"

"Disaster Recovery" refers to the process undertaken when entities or institutions are subjected to an event that impacts the work of providing electronic services, halting them completely, or that results in data loss, as in the case of fire, deliberate sabotage, natural disasters, or system failure. The disaster recovery process is comprised of a set of operations, policies, and actions that the affected entity undertakes.

Steps for Addressing Emergencies

In the event that an emergency occurs that leads to stoppage, disabling, or change in the performance of one of the network's electronic services, resulting in disruption of King AbdulAziz University operations or significant losses to the University, the following steps must be followed:

1– Notification of the Event

When an emergency occurs, the Cyber-Security Center must be notified immediately by a member of staff or external office, such as the National Cyber-Security Authority, which then subsequently further informs, whether by phone or email, the Cyber-Security Center of the complete or partial stoppage of one of the electronic services provided by the network domain operated by the Deanship of Information Technology. The office receiving the notification transfers it to the responsible office, such as the Response Team or the Deanship of Information Technology, assigning the necessary tasks based on their nature.

2– Assessment of the Event

The office concerned with service assessment evaluates the event, estimates the size of its impact, and considers whether to address it or escalate it. (See Table 1).

3– Addressing the Event

Information that will aid in resolving the event or crisis must be provided. The table below explains the methodology to be followed in the event of an incident, as well as the roles and responsibilities of the relevant offices. (See Table 2).

In addition, determination of the category of recovery from the effects of the incident must be made, in accordance with the timeframe used in classifying events. (See Table 3).

4– Report Preparation (Security Incident Reports)

All required documents must be stored, discussions concerning lessons learned must be held with all concerned offices if necessary, such points of weakness as exist must be corrected, and the technologies employed must be improved.

Appendices

Table 1: Classification of Services and Information

The electronic information and services provided through the University domain network are classified and evaluated subsequent to disasters and emergencies on the basis of a variety of factors, as described in the following table:

Information/Service	Description
Technical Services Affecting the Reputation of the University	Services and information that must necessarily be provided, or upon which many important services depend, whose ongoing disablement or unavailability would cause significant losses to the University.
Production Services	Electronic services that provide the University with the opportunity to operate productively, continually, and securely, with reasonable financial expenses.
Electronic Infrastructure	Technologies necessary for the operation of essential services on the network domain, such as electric power sources, cooling systems, network devices, service plans, utilities, etc.
Manpower	Providing and assigning specific places and offices for seven workers, at a minimum, at the information center backup site, in addition to providing to those concerned the ability for remote electronic communication in case they are unable to access the site.
Technical Devices	Allocating certain necessary back-up technical supplies, as well as a reserve budget to allow for the potential to purchase certain necessary supplies directly.

Table 2: Classification of Incidents and Assignment of Roles and Responsibilities

Description	Recovery Method
Routine Events	<ul style="list-style-type: none">Assigned to the Response Team during regular working hours.
Events with the Potential to Escalate	<ul style="list-style-type: none">Assigned to the Response Team during and outside of regular working hours.

	<ul style="list-style-type: none"> • The Director of the Cyber-Security Center is notified. • The concerned work-team in the Deanship of Information Technology and other departments are notified if necessary. • Initiation of the steps necessary for resolution. • Escalation of the event to the Supervisory Committee if necessary.
Abnormal Events Requiring Immediate Response	<ul style="list-style-type: none"> • The Director of the Cyber-Security Center notifies the Supervisory Committee, initiates solutions, evaluates the extent of harm, and makes quick decisions. • The budget and resources necessary for recovery are allocated. • The work-team in the Deanship of Information Technology and other concerned offices are notified. • The planned steps and procedures are initiated, and tasks and responsibilities are assigned to all offices. • The Technical Disaster Recovery Plan is activated, if necessary.

Table 3: Classifications of Recovery from Event Effects

Category	Definition
Normal	Recovery times with the use of current resources can be predicted.
Supplementary	Recovery times with the use of additional resources can be predicted.
Extended	Recovery times cannot be predicted, and there is need for additional resources and outside support.
Irrecoverable	Recovery from the event is not possible (for example, in the event of theft or publication of critical data), and an investigation must be undertaken.