DISASTER RECOVERY PLAN

1. Objective

The Disaster Recovery Plan is designed to forecast all possible disruptions and disasters, determine the business impact of those disruptions, and prepare the ground to coordinate the response in the event of a disruption.

The aim of the plan is;

- To maintain the highest possible service levels for all services,
- In the event of a disaster, to enable business processes to be restored within the predicted downtime,
- To minimize the probability and negative impact of disruptions.

2. Scope

The Disaster Recovery Plan is structured to ensure operational efficiency and continuity.

- The potential impact of service disruptions on business units is reviewed and recovery plans are developed to ensure service continuity,
- The roles and responsibilities of company personnel in the framework of the Disaster Recovery Plan,
- The outcomes of tests and adhibitions conducted.

3. Definitions

- **Business Continuity:** The ability to plan and respond strategically and tactically to evolving events and business process disruptions in order to maintain business operations at a pre-determined and admissable level.
- **Disaster Recovery Plan:** It is a set of processes and information that is developed, compiled, made available and documented to enable an organisation to continue its critical operations at a pre-determined and admissable standard should the need arise.
- **Business Impact Analysis (BIA):** Business Impact Analysis (BIA) is the process of determining the criticality of business activities and the associated resource requirements to ensure operational resilience and business continuity during and after a business disruption.
- **Adhibition:** Partial or full rehearsal activities to ensure that business continuity plans contain the appropriate information and, when implemented, will generate the intended output.

4. Implementation

4.1 Business Impact Analysis

The Business Impact Analysis study identifies AKFEN's critical business processes, the threats that may affect these processes and the damage that the organization will incur should the processes be disrupted. An acceptable recovery time objective (RTO) for the organization's business processes is agreed upon in consultation with the process owners or their designated representatives. The organization's business processes are prioritized

according to these values. The next step is to identify the IT services that support the business processes. Acceptable downtime for IT services is determined taking into account the business process supported by the service.

The work to be performed in this stage is summarised below:

- Determination of the impact of the interruption of the business processes on the organization in accordance with the Business Impact Analysis,
- Calculation of acceptable downtime for each process,
- Prioritization of business processes on the basis of Business Impact Analysis,
- Identification of the IT services and components that provide support for the processes,
- Determination of acceptable downtime for each IT service and component. Classification of systems as systems that must be operational within one day, one week and thirty days in the event of a disaster. The priority list of systems within AKFEN, classified according to their priority status below, is reviewed and updated as necessary by the Information Security Coordination Board on an annual basis.

  Systems that need to be rebooted within a day in the event of a disaster

  - Active Directory
  - Database Server
  - Application Server
  - Accounting Software
  - Internet Access Mail Server
  - Human Resources System

  Systems that need to be rebooted within a week in the event of a disaster

  - Antivirus and Windows Update Server
  - Document Management System
  - SSL-VPN System

  Systems that need to be rebooted within thirty days in the event of a disaster

  - Network Monitoring System
  - Archive System
- Identification of the shortcomings of the existing technology infrastructure in providing acceptable levels of downtime and identification of areas where technology investment is required,

Performing a Business Impact Analysis is the remit of the Information Security Coordination Board.

4.2 Emergency Response Plan for Disaster Scenarios

Risk	Unable to Access the System Room	Power Outage
Probable Scenario	Fire, Earthquake	Uninterruptible power supply failure, Generator failure
Probability	Low	Low
Impact Level	High	High
Affected Functions	The entire IT infrastructure powered by servers	All of the IT services
Action Plan	• All life forms will be removed from the system room for security reasons. • If the fire prevents entrance, the fire brigade will be called. • If the earthquake makes it impossible to enter, the fire brigade or emergency services will be called. Damage assessment is carried out by the Damage Assessment Team once access to the system room is possible.	• The problem is reported to the designated staff of the AKFEN Central Building Maintenance Unit and the resolution process is followed. • The failure will be rectified by the Mechanical Works department. • Following the rectification of the failure, the operability of all systems is checked by the Units/Groups associated with the system.
Responsibilities	AKFEN Security Team	Building Maintenance/Mechanical Team, IT Manager
Preventive Action	Fire Extinguisher Systems	Replacement UPS, maintenance of the generator
Resources	Members of staff, mobile phones	Generator, UPS units, Human resources

Risk	Natural Disasters and Acts of Sabotage	Network Services Outage
Probable Scenario	Fire, Earthquake	LAN, WAN interruptions/malfunctions
Probability	Low	Low
Impact Level	Extremely High	High
Affected Functions	All of the functions	All network-related systems and processes
Action Plan	• Relevant institutions (fire brigade, police, etc.) are immediately contacted. • Damage attributable to natural disasters or sabotage is assessed. • The systems are tested for operability and functionality. • Should there be a system that is not working, it is ensured that the backup system is operational. The information will be checked for complete precision and accuracy.	• Failure reporting is notified to network systems. • Depending on the type of failure, the failure will be rectified by the network personnel or by the service provider. • Once the problem has been resolved after troubleshooting, all relevant units are informed that the problem has been resolved. • The cause of the malfunction is identified and corrective action is taken.
Responsabilities	AKFEN Security Team	The IT manager is responsible for troubleshooting and repairing the breakdown.
Preventive Action	Fire Extinguisher Systems, Physical Security and Safety Measures	Monitoring, back up
Resources	Members of staff, mobile phones, Back up and recovery media and hardware	Network devices, E-mail correspondence

Risk	Server Services Outage and Breakdown	Virus Attack / Security Breach
Probable Scenario	Hardware failure, Database problems, Application server problems	Virus attack, Data breach attempts to violate privacy of data
Probability	Medium	Low
Impact Level	High	High
Affected Functions	J-guar, QlikView and other associated systems	All of the functions
Action Plan	• The problem is reported to the Information Technology Directorate. The problem identification and troubleshooting is carried out by the IT Manager. • The operational functionality of the system is checked by the relevant units. • The root cause of the problem is identified and corrective action is taken as and when required.	• The situation should be reported to the Information Communication Manager by the person or unit noticing the breach or attack. • The Information Technology Manager's team ensures that the incident is detected and analyzed promptly, and that the necessary precautions are taken. • In the event of a virus attack, it is determined whether the current anti-virus programme provides protection against the virus in question. If there is no virus protection, the manufacturer is contacted and the necessary work is carried out to speed-up the removal of the patch. • Where necessary, judicial and legal action will be taken against the perpetrators of the security breach or attack. • The root cause of the violation is identified and corrective action is taken.
Responsabilities	Affected system users, IT Manager	All members of staff and the IT team
Preventive Action	Server monitoring program, disk and server hardware back up, application server back up, network device back up, power redundancy	Access control, Endpoint protection mechanisms (anti-virus, host IP, firewall), Network and security devices
Resources	Hardware and equipment, Human Resources	Network and security devices, anti-virus software

5. Tests and Adhibitions

The organisation's business continuity and case management procedures cannot be considered reliable unless they are tested and kept up to date through exercises and drills. Drills are essential to develop the teamwork, cohesion, confidence and knowledge that are vital in the event of an incident.
Policies should be reviewed through exercises, and audit and internal evaluation processes should confirm that the policies are fit for purpose.
For this reason, the Information Security Coordination Board coordinates the preparation of the plan. In this context, the Board is responsible for reviewing and approving the annual exercise plans prepared by the IT Manager.

The purpose of the test of the Disaster Recovery Plan shall be defined as follows:

- To determine the effectiveness of the plan,

- To determine the state of preparedness and proficiency of designated relevant persons to fulfil their assigned rescue and response responsibilities,
- To determine whether modifications or updates to the Disaster Recovery Plan are required to ensure that recovery within acceptable downtime is achievable and acceptable to users.

6. Assessment of Adhibition / Test Results

The IT Manager is responsible for coordinating the review and updating of the plan by analyzing the results of the tests and exercises.

Following the drill, the IT Manager works to document the test results. To identify deficiencies and problematic issues, the IT Manager reviews the test/exercise results in a meeting with the Information Security Coordination Board. Based on the input from the meeting, the deficiencies and shortcomings in the plan are corrected and updated.