BUSINESS CONTINUITY - EMERGENCY AND CONTINGENCY PLAN

1. OBJECTIVE

This plan is prepared for Iş Yatırım Menkul Değerler A.Ş. against the possibility of being damaged and facing a potential loss as a result of predictable or unpredictable internal or external factors such as hardware or software failure, electrical and telecommunication interruptions, cyber attacks, and physical attacks, natural disasters, social events, terrorism, infectious and epidemic diseases;

- To ensure continuity of business processes,
- To ensure maintaining customer services uninterruptedly,
- To ensure continuity of fulfillment of responsibilities towards legal authorities and third parties,
- To minimize negative operational, financial, legal and reputational impacts in case of any interruption to maintain activities or recover in time,
- To ensure taking the Company assets under protection in the best way in case of any potential loss, and
- To ensure business processes to be put into operation again as soon as possible after any interruption.

2. BASIS

This plan is prepared pursuant to the Communiqué on the Principles Relevant to the Internal Audit System to be Applied at the Intermediary Institutions (Serial V, No: 68) published in the Official Gazette dated 14.7.2003 with Issue Number 25168 and the Communiqué on the Information Systems Management published in the Official Gazette dated 5.01.2018 with Issue Number 30292 and decided to be applied with the Decision of the Board of Directors.

The main purpose of the Information Policy is to ensure the necessary information and explanations besides those not in the scope of internal information to be transmitted to the shareholders, investors and other relevant parties in a timely, accurate, complete, understandable and easy manner and accessible at the lowest possible cost, on equal terms.

3. DEFINITIONS

Term	Definition and Explanation
Institution	Iş Yatırım Menkul Değerler A.Ş.
The Board of Directors	The Board of Directors of Iş Yatırım Menkul Değerler A.Ş.
General Manager	General Manager of Iş Yatırım Menkul Değerler A.Ş.
Executive Management	Executive Committee of Iş Yatırım Menkul Değerler A.Ş.
General Directorate	General Directorate of Iş Yatırım Menkul Değerler A.Ş.
Directorate	All departments existing within the organization structure of the Institution or shall be established in the future
Business Impact Analysis (BIA)	The analysis process on business processes and the impacts which an activity interruption may cause on business processes.

Business continuity	Institution's strategic and tactical capacity to plan for and respond to contingencies and activity interruptions to conduct commercial activities at an acceptable and predefined level.
Business Continuity Plan	The body of written procedures and information developed to ensure continuing critical activities of the Institution at an acceptable and predefined level and kept ready for use in the event of a contingency.
Business Continuity Strategy	An approach ensuring recovery and business continuity of the Institution in case of a major contingency or a long-term activity interruption.
Business Continuity Management (BCM)	A holistic management process identifying potential impacts threatening an Institution and offering a framework for flexibility which shall put forth an effective response capability that takes interests of key stakeholders, the institution's reputation, brand, and value-creating activities under protection
BCM Team	The team managing and coordinating BCM activities on behalf of the Institution.
Critical Business Process	The process determined during the BIA and is among the processes to be recovered first in the event of an interruption.
Recovery Time Objective (RTO)	Targeted period of time to restart offering products/services after a contingency.
Recovery Point Objective (RPO)	Acceptable data loss value to restart offering products/services after a contingency.
Interruption	An interruption in continuity of Is Investment operations or of functions of a system due to force majeure other than planned transitions.
Emergency	Circumstances of which the place and time of their occurrences are uncertain even if they are foreseen, and if occur, cause losses and business interruption and require the implementation of plans and procedures.
Crisis	Events which cannot be solved by processes defined to be applied in daily routine by local authorities due to their scale, cause death or injury, significant damage to property and the environment, significant interruption in Iş Investment activities or events which have an impact on a societal scale and threats that may cause these results.
Information Systems Continuity Plan	The plan prepared to ensure continuity of information systems services providing maintenance of the activities in case of an interruption and which is a part of the business continuity plan.
Emergency and Contingency Plan	A plan which is part of the business continuity plan in which precautions to be taken and primary actions to be carried out are determined to manage risks and problems in case of a sudden and unplanned interruption of the operations which may cause business loss or crisis
Corporate Crisis Management Team (CCMT)	The team which manages crisis in case of a major and drastic extraordinary situation.

4. SCOPE OF BUSINESS CONTINUITY AND EMERGENCY MANAGEMENT

4.1 Scope of Information Systems Continuity Management

Information systems continuity management; expresses the management process relevant to conducting business processes carried out and services offered at the Institution effectively, reliably and uninterruptedly, fulfilling responsibilities towards legal authorities and third parties, establishing a proper information systems environment to ensure integrity, consistency, reliability, timely availability and confidentiality of information provided from the accounting and financial reporting system, ensuring control and follow up of risks arising from usage of information systems and taking necessary systemic and administrative precautions.

Circumstances of which occurrence place and time are unknown even if they are foreseen, and if occur, cause disruptions and/or interruptions in the Institution operations and require implementation of the relevant procedures, such as interruption of basic investment operations carried out in connection with information technologies, loss of communication and telecommunication opportunities and information processing capacity and opportunities and disappearance of infrastructure access opportunity are within the scope of the Information Systems Continuity Management. For this, also an "Information Systems Continuity Plan" which describes the circumstances and the procedures applied in case of an interruption and which is a part of this plan is prepared by the Institution.

4.2 Scope of Emergency and Contingency Management

Emergency and contingency management; expresses the management process relevant to ensuring control and follow up of circumstances which may cause a sudden and unplanned interruption of the operations carried out at the Institution, business loss or crisis and taking necessary systemic and administrative precautions for this purpose.

Circumstances of which occurrence place and time are unknown even if they are foreseen, and if occur, cause losses and disruptions and/or interruptions in the Institution operations and require implementation of the relevant procedures, such as natural disasters (earthquake, fire, flood, etc.) and circumstances as disruption or interruption of operational transactions with physical security source, loss or damage of Institution employees and customers and assets of the Institution are within the scope of the Emergency and Contingency Management.

5. COMMUNICATION, COMMISSIONING AND UPGRADE PROCESS

In case of a severe and/or drastic extraordinary circumstance threat for the Institution is in question or occurs, Business Continuity Plan shall be put into action by the instruction of the relevant Deputy General Manager or Business Continuity Team. In case of a comprehensive extraordinary situation affecting more than one department, the crisis management shall be coordinated by thr Corporate Crisis Management Team (CCMT).

5.1 Effective Communication

In some cases, it may not be possible to make a face-to-face talk. In such cases, providing and maintaining an effective communication is important. All the managers at the directorate should have the mobile phone numbers of all directorate employees. In case of an extraordinary situation, managers should be in contact with the employees reporting to them (Cascading telephone contact).

The Directorate and the Branch Business Continuity Coordinator should evaluate the information obtained and determine who shall establish a communication with an upper management level. Cascading telephone contact shall work in two directions and by this way, any worrying situation or problem regarding the employees shall be conveyed to the department crisis management team.

5.2 Evaluation of Effects of Emergency and Contingency on Customers

In Emergency and Contingencies, service interruptions as ending of the communication with the customers or failing to fulfill the instructions may be experienced. In our business continuity plan, it is planned to continue our operations with minimum interruption and loss in emergencies. All values, from the protection of our employees and customers to the continuity of our operational services, shall be met with superior and appropriate operation. Basic purpose of all these measures is continuity of the operations.

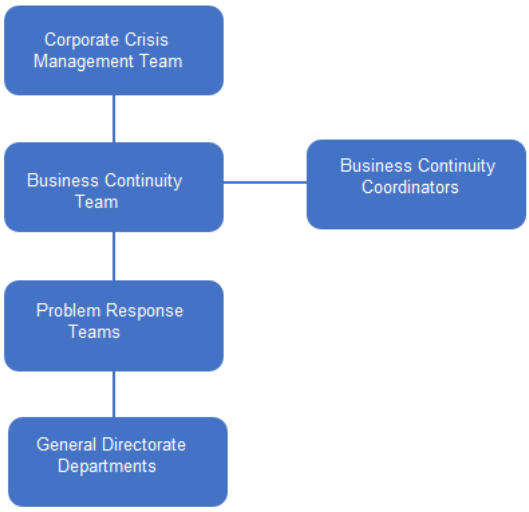
The General Manager may take the decision of suspending the operations at some premises according to the scale and impact of the emergency and contingency. In such case, our customers are informed through the fastest communication channels. Necessary records for announcements from the Institution's website and for sending electronic mail or SMS to the customers on this issue are kept ready and tasks are distributed in advance between the Directorate of Information Technologies and Project Management and the Directorate of Marketing and Product Management.

6. BUSINESS CONTINUITY AND EMERGENCY MANAGEMENT STRUCTURE

An integral business continuity management structure is established in the Institution for taking effective measures in disaster, crisis or interruption circumstances, minimizing negative operational, financial, legal and reputational impacts, ensuring continuity of operations determined critical in the targeted time frame and reverting back to the status before the crisis.

Coordination of the activities relevant to preparation of the Business Continuity Plan, Business Impact Analysis studies and creating/updating of the scenarios in the Business Continuity Plan are fulfilled by the Directorate of Information Technologies and Project Management. Following the evaluation of the General Manager, the Plan is submitted to the approval of the Board of Directors. The Business continuity management structure is comprised of the Business Continuity Coordinators, BCM Team, Problem Response Teams and the Corporate Crisis Management Team.

Management Structure



Regulations regarding the supply of necessary employees and duties and responsibilities of employees in an emergency are determined and information and training are provided on the duties undertaken by the employees by the Directorate of Human Resources.

7. MAIN FACTORS OF BUSINESS CONTINUITY PLAN

Communication strategy, Recovery Strategy, Distribution Strategy, Testing the Plan, Updating the Plan, Business Continuity and Emergency Trainings, Business Continuity within the Scope of the Suppliers and Forms and Documents to be Used within the Scope of the Plan constitutes the main elements of the Business Continuity Plan and the details are given below.

7.1 Communication Strategy

In emergency or crisis times; ensuring an accurate, clear and reliable information flow is very important in terms of preventing panic and turmoil environment and ensuring control over business processes. Effective Communication is the basis for proper functioning of the Business Continuity Plan. Responding information requests in time and transmitting the information accurately are important. Accordingly, in case of an emergency and contingency, employees, Business Continuity Coordinators, Business Continuity Team, Response Teams, legal authorities, suppliers, customers, relatives of the employees and the public should be informed within the framework of an effective communication. In emergency and contingencies, the Directorate of Human Resources or the team to be determined by the relevant Deputy General Manager is responsible from the communication throughout the Institution.

Problems arising in the basic communication systems are resolved with the coordination of the Directorate of Information Technologies and Project Management.

Primary Information to be Transmitted in Emergencies

- Time of the Event
- Occurrence Way
- Relevant Scenario in the Plan
- Sharing Duties and Responsibilities
- Recovery Strategies
- Status of the Employees and Customers
- Loss Assessment

GSM phones shall be used in emergencies as an alternative communication source. During the period when the main exchange fails servicing in contingencies, GSM mobile lines shall be used as an alternative communication method. In case an emergency or contingency arises, our customers, legal authorities and third parties shall be informed about the alternative contact information when necessary. Communication shall be provided over the central switchboard having geographical redundancy throughout the Institution. In case the Institution employees are not able to provide communication over the central switchboard, they may establish communication over the institution GSM lines given to them or their personal GSM lines. Residential addresses and fix and mobile contact information are already given to all department managers and the members of the Business Continuity Team.

Main Communication Methods and Tools which may be Used in Emergency

- Web Site of our Company
- Telephone
- E-Mail
- Video – Conference Tools
- Bulk SMS
- Instant Message Applications

7.2 Recovery Strategy

Each operation conducted in the Institution has a separate importance. However, some operations determined by the Business Impact Analysis are separately mentioned in the Business Continuity Plan as the subject operations are critical. From this point of view, the Institution has developed a recovery

strategy taking the business impact analysis as the basis and putting the recovery priorities and targets forth. Recovery strategy may be defined as a method the Institution determines and conducts for restoring critical operations and ensuring business continuity after emergency.

These methods may be listed as;

- Referring to manual operations during interruption,
- Starting to use alternative applications by which business processes may be conducted,
- Backing up important data,
- Activation of backup systems for critical and urgent activities,
- Waiting for repair of existing systems for activities with critical but tolerable interruption period,
- Receiving alternative outsourcing, and
- Inactiveness.

In case of an operational interruption, priority of the Institution is ensuring continuity of the critical operations determined as a result of the Business Impact Analysis and the target of the Institution is ensuring continuity of the systems again in the shortest time with minimum loss. In the Business Impact Analysis, transaction intermediation considered critical (transmitting customer trading orders to the stock exchange), IT operations, clearing, operation and custody activities, management of the Institution's portfolio and portfolio brokerage activities have priority in the Institution's recovery plan.

7.3 Distribution Strategy

An electronic copy of the Business Continuity Plan is on the intranet for providing all Institution employees to be informed and access at any time and a printed copy is available at the Business Continuity Coordinators and the Business Continuity Team.

7.4 Testing the Plan

A process is created to review the Plan to see the functionality of the Plan, time of response to interruptions and the structuring relevant to business continuity. Within this scope, the Business Continuity Plan is tested by the Business Continuity Team at least once a year against possible inconveniences in accordance with the organization. Test results are recorded and reported to the Top Management by the Business Continuity Team.

7.5 Updating the Plan

Business Continuity Plan is reviewed at least once a year and updated if found necessary. In case of changes in business conducting in the business processes, IT application changes, etc. within the year, the plan is reviewed and updated. Following the evaluation of the Business Continuity Plan by the General Manager, it is submitted to the approval of the Board of Directors.

7.6 Business Continuity and Emergency Trainings

Training programs are organized to have the Business Continuity Plan a part of the corporate culture, understand the things required to be made within the scope of the Plan and to inform the Business Continuity Coordinators, the Problem Response Teams and all employees of the Institution about their duties and responsibilities. Attendance of the employees to the business continuity and emergency training is provided and followed under the responsibility of the Directorate of Human Resources.

7.7 Business Continuity Within the Scope of Suppliers

Reviewing regularly the status of the solution provider supplier companies of the Institution and preferring the companies which shall not disrupt the services and instructions of the Institution in case of emergency/contingency are under the responsibility of the Department authorized in this aspect.

8. EMERGENCY AND CONTINGENCY PLAN

It is prepared for determining the measures and priority actions to be taken to manage risks and problems in case of a situation resulting in sudden and unplanned interruption, business loss or crises in operations, and constitutes a part of the business continuity plan.

8.1 Determining Critical Emergencies

8.1.1 Earthquake

It includes earthquakes which may occur as a result of natural factors and damages they may bring along them at the Headquarters" or "Branches". It may be possible to affect only one "Settlement" as well as multiple "Settlements". Hazard, severity and impact area of the earthquake shall constitute the basis of evaluation.

Employee loss, structural damage, software damage, hardware damage and process interruption are thought to occur as a result of an earthquake. According to the extent of the damage, it is estimated that there will be primarily short-term process disruptions, and then, disruptions will occur at variable times depending on the damage specifications. It is estimated that disruptions in the processes will be for a short-term in short-term and minor and light earthquakes but the processes that require employees will be disrupted for a longer time in relatively stronger earthquakes even if there is no damage.

In case of structural damage, a disruption in the processes is thought to occur in line with the situation of the systems and employees in the relevant department. It is estimated that many "Settlements" will be affected especially by severe earthquakes and accordingly, many processes will be greatly disrupted. In such case; since the Stock Exchange, Central Registry Agency (CRA), the Settlement and Custody Bank (Takasbank) and the companies traded in the Stock Exchange are expected to be significantly affected by an earthquake of this size, business processes of our Institution may be disrupted accordingly.

It is thought that the servers affected by the hardware damage, network cabling infrastructure and the working processes in line with the employees will be greatly disrupted for the relevant "Settlement". Besides, recorded data loss, loss of process data in the system or disruption of continuity of the processes may disrupt other relevant processes, moreover, the basic network services shall be interrupted according to the recovery time from the backup in line with the lost information. Communication between the "Settlement" affected by the earthquake and the "Headquarters" or "Branches" is thought to be majorly disrupted.

8.1.2 Fire

Includes fires arising from electric, heat or gas explosions which may occur at the "Headquarters" or "Branches". Fire may occur due to actions of the Institution employees, actions of the employees of external service providers, problems in electricity infrastructure, warming due to external effects or problems in gas circulation infrastructure. In addition to actions involving negligence or intentional factors, fire may occur due to external factors.

Occurrence of employee loss, structural damage, software damage, hardware damage and process interruption problems are thought as a result of a fire. It is estimated that according to the extent of the damage, there will be short-term process disruptions and afterwards, in accordance with the damage assessment, there shall be interruptions in variable periods of time.

In case the employees are injured as a result of the fire, it is estimated that the relevant processes shall interrupt in variable periods of time in accordance with the position of the employees. In case of a structural damage, interruption in the processes is expected in accordance with the status of the systems and employees in the relevant department.

It is thought that the servers affected by the hardware damage, network cabling infrastructure and the working processes in line with the employees will be greatly disrupted for the relevant "Settlement". Besides, recorded data loss, loss of process data in the system or disruption of continuity of the processes may disrupt other relevant processes, moreover, the basic network services shall be interrupted according to the recovery time from the backup in line with the lost information. Communication

between the “Settlement” affected by the fire and the “Headquarters” or “Branches” is thought to be majorly disrupted.

8.1.3 Terror

It involves acts of violence made by an external group or individual against the institution. Acts of violence may occur as disruption of the Institution’s business processes or giving harm to the properties or employees of the Institution.

Occurrence of employee loss, structural damage, software damage, hardware damage and process interruption problems are thought as a result of acts of violence. It is estimated that according to the extent of the damage, there will first be short-term process disruptions and afterwards, in accordance with the damage assessment, there shall be interruptions in variable periods of time.

In case the employees are injured as a result of acts of violence, it is estimated that the relevant processes shall interrupt in variable periods of time in accordance with the position of the employees. In case of a structural damage, interruption in the processes is expected in accordance with the status of the systems and employees in the relevant department.

It is thought that the servers affected by the hardware damage, network cabling infrastructure and the working processes in line with the employees will be greatly disrupted for the relevant "Settlement". Besides, recorded data loss, loss of process data in the system or disruption of continuity of the processes may disrupt other relevant processes, moreover, the basic network services shall be interrupted according to the recovery time from the backup in line with the lost information. Communication between the “Settlement” affected by the acts of violence and the “Headquarters” or “Branches” is thought to be majorly disrupted.

8.1.4 Other Extraordinary Situations

Within the scope of critical emergencies, the issues listed below may be included besides the subject extraordinary situations.

- Social Events
- Robbery
- Bomb attack
- Biological and Chemical Attacks
- Infectious and Epidemic Diseases

8.2 Emergency and Contingency Scenarios

Emergency and Contingency Scenarios are designed to evaluate potential risks the interruptions which may occur in the operations may cause and the potential effects of the risks.

In case of an interruption in the operations, it is necessary to act in compliance with the Emergency and Contingency Scenarios. Life safety of the employees and the customers is predominant. In case of an emergency, the Business Continuity Coordinator of the relevant department determines the subject of emergency immediately.

Along with the determination of which scenario or scenarios the subject of the emergency falls into, scenarios are implemented.

In case of receiving the intelligence that our Institution will be targeted in social events, central or local decisions taken by the administration (curfew, etc.) etc., Business Continuity Team shall be immediately contacted with and informed about the situation and actions shall be taken according to the instructions to ensure emergency action initiative. Activity Interruption Report is prepared about the reason of the problem and the measures taken and submitted to the Business Continuity Team.

During the emergency, collection of information received from local sources about the emergency and transmitting to the Business Continuity Team is provided.

Scenario 1: Operation platforms are running; but it is not possible to enter the General Directorate or Branch building.

If the process platforms are active and the terminals can be reached within the scope of Emergency and Contingency Plan Scenario 1, it shall be acted in accordance with the recovery strategy to be implemented with the coordination of the Business Continuity team

It shall be possible to provide service via remote access and mobile phones by a secure IT infrastructure and the continuity of the processes in the recovery location for physical operations will be ensured.

In case it is possible to access transaction terminals via remote access, customers' trading transactions are carried out via terminals that can be accessed remotely

As it is considered that the Institution activities are fulfilled, it shall be worked with the Business Continuity Team to enter the General Directorate or Branch building.

Scenario 2: There is a general situation which prevents use of Iş Investment General Directorate building and access to the system throughout Istanbul.

Within the scope of Emergency and Contingency Plan Scenario 2, it is deemed as there is a problem in the region and the geographical area where the Institution Headquarters is. It is not possible to enter the headquarters and the building is unusable. If there is no interruption in the Primary data center it is acted as in Scenario 1.

In case of an interruption in the Primary data center, it is worked on elimination of the interruption experienced in the primary data center. Unless it is possible, backup systems are activated for systems with redundancy structure. Continuity of the operations is provided from there. Works are carried out with the Corporate Crisis Management Team.

Restoring time of the systems may be short or long according to the work and backup/recovery procedure of the systems and platforms. These values are determined by the Business Impact Analysis.

Continuity of the processes are ensured at the minimum level by acting in accordance with the actions determined by the Business Impact Analysis.

- Customers are directed to alternative channels.
- Manual operations are resorted to.
- Alternative applications which business processes can be conducted are started to be used.
- Alternative outsourcing is provided.

8.3 Storing Financial Statements and Records Kept Pursuant to the Legislation and Negotiable Documents

The Institution keeps all kinds of information, records and financial statements electronically for the periods stated in the legislation of CMB and other legal legislation to ensure business continuity and the operations to continue without victimization of the customers. Physical documents and backed up records are stored in different location. Records and documents relevant to financial statements are stored both electronically and physically. The Institution receives physical archiving service from an authorized institution which is 7/24 under observation, specially designed in terms of engineering and architecture and equipped with special security and fire equipment and has separate custody centers. Images and voice records of all legal documents as agreements and instructions are stored electronically.

8.4 Storing Electronic Records Backups
Backups taken to ensure continuity of data processing systems for maintaining operations uninterruptedly are stored during the legal period.

8.5 Operational Risk Evaluation including Financial and Information Communication Infrastructure
When operational risks are evaluated, actions required to eliminate risks which shall prevent Institution operations within the scope of this Plan are planned. In case of emergency and contingencies access to the systems shall be provided by remote connection and the operations shall be continued.

8.6 Procurement of Alternative Communication Channels and Ensuring Continuity with Customers
Effects of the experienced interruption on customers are evaluated according to article 5.2 – Evaluation of Effects of Emergency and Contingency on Customers – of this Plan and necessary communication actions are taken.

The Customers shall be able to provide communication with the Institution in extraordinary circumstances by communication tools they use in ordinary conditions. Within this scope, telephone, fax and mail addresses which are current contact information shall be exactly valid or according to the effects of the situation,

- All kinds of money transfers and EFT transactions,
- Buying and selling capital market instruments and placing orders for all other transactions within this scope,

Shall be carried out referring to the instructions the customers shall transmit to the Institution via new communication channels to be notified to the customers, as in the ordinary circumstances without causing any interruption or disruption and without any customer victimization.

Access to the systems shall be provided as stated in the relevant scenarios of this Plan and business continuity shall be established. In case of any problem in the internet system, uninterrupted service shall be offered through Sales Units and investment consultants.

8.7 Procurement of In-house Alternative Communication Channels and Ensuring Continuity
According to the impact of the interruption, necessary in-house communication actions are taken according to article 7.1 - Communication Strategy – of this Plan.

8.8 Alternative Institution Center
When necessary, the Institution provided remote access to the systems from an alternative working location as stated in Establishing a Secure IT Infrastructure to Provide Remote Working Environment article of IT Continuity Plan and ensures business continuity

8.9 Evaluation of the Possible Effects of the Emergency and Contingency on the Other Party
The Institution informs its customers on how the business continuity shall be provided in emergency and contingencies and on work flow procedures relevant to this. The subject informing is made while opening an account; besides, emergency and contingency plan is also given in the Institution's website, www.isyatirim.com.tr.

In case of any emergency and contingency, all investors shall be immediately informed that they'll be able to continue their transactions over alternative channels and that their transactions requests shall be fulfilled with the best effort.

8.10 Routine Mandatory Notices
All kinds of contact information including titles, e-mail addresses, phones and fax numbers of persons responsible from application of emergency and contingency plan stated in the annex of this Plan which

are prepared by the Institution and put into effect after the approval of the Board of Directors are reported to the Board, Istanbul Stock Exchange, Central Registry Agency (CRA), Settlement and Custody Bank (Takasbank) and other institutions to be determined by the Board.

8.11 Customers' Access to His/Her Accounts and Transfer of Accounts to Another Intermediary Institution in the Case a Decision to Discontinue Operations is Taken

Iş Yatırım Menkul Değerler A.Ş. has planned the actions required to provide continuity of the operations within the framework of this plan and created procedures for reviewing them regularly. It regularly tests the procedures to be applied in the subject interruption scenarios.

According to the scale and impact of the emergency and contingency, the Board of Directors may take the decision of suspending the operations. In such case, our customers are informed by the fastest communication channels. Records and technical works necessary for announcements from the Institution website to send electronic mail or SMS to the customers on this subject are kept ready and task distribution is made in advance between the Directorate of Information Technologies and Project Management and the Directorate of Marketing and Product Management.

Continuous access to the Central Registry Agency (CRA), Settlement and Custody Bank (Takasbank) and EFT systems shall be ensured and it shall be possible for the investors to transfer their assets to the institutions they want without any problem in accordance with the customers' instructions.