

BUSINESS CONTINUITY PLANNING SYSTEM FOR THE KDPW GROUP - BCP SYSTEM POLICY (EXCERPT)**Contents:**

I. Introduction	1
II. BCP System general principles	1
II.1. Application	2
II.2. Processes.....	3
II.3. Recovery parameters.....	3
III. BCP System operational resources	3
III.1. The Business Recovery Site.....	4
III.2. The Crisis Response Group	4
III.4. The Operational Group	5
III.5. Procedures and documentation	5
IV. BCP System testing.....	5
V. Maintenance and development of BCP System.....	5

I. Introduction

The loss of the high standard and of the timeliness of services provided by the KDPW Group as a result of adverse operational conditions, may lead to disruptions in the financial market, which may in turn lead to loss of revenues and affect the corporate reputation of the companies belonging to the KDPW Group and its stakeholders.

In order to minimise the impact of incidents and disruptions on the business operations of KDPW and KDPW_CCP and their business partners, a Business Continuity Planning (BCP) System has been introduced within the Group, as a range of technical and organisational processes established to enable the maintenance – in the event of a serious emergency or disaster – of business continuity or to ensure the fastest possible recovery time for core business processes while lessening the impact of the incident on operations of the KDPW Group and of other financial market institutions.

Integrated into the BCP System is the business continuity strategy for the information and communication technology (ICT) on which the KDPW Group companies' operations are based, which in particular includes a communication strategy for informing the relevant entities of major ICT-related incidents.

II. BCP System general principles

The purpose and scope of the BCP System derive from the analysis of the impact of potential disruptions on the operations of the companies belonging to the KDPW Group, based on the assessment of operational risk within the Group.

II.1. Application

The BCP System has been prepared in order to recover the major business processes in the event of emergencies, which generally fit into two general scenarios:

- 1) a comprehensive failure of IT processing systems or other ICT assets, interruption of critical utilities or unavailability of telecommunications services, resulting in the need to deploy back-up assets;
- 2) inability to use the primary business site of the Group companies, which requires the relocation of employees from the primary to the back-up site or their remote work.

In addition, separate procedures are provided for in the event of:

- 1) global emergencies which broadly affect many entities and objectively restrict the ability of the KDPW Group companies to operate, where additional protection plans governed by the relevant legislation apply;
- 2) problems in the execution of individual business processes, whose elimination is regulated by the relevant operating procedures or procedures agreed with external partners.

II.2. Processes

For the purposes of the BCP System, the business processes performed in the companies belonging to the KDPW Group have been divided into four categories:

- 1) Critical processes;
- 2) Important processes;
- 3) Support processes;
- 4) Ancillary processes.

Critical and important processes are processes whose performance within a set time and in a pre-determined manner have a significant impact on the business operations of the companies belonging to the KDPW Group (achieving corporate goals set out in the company statute, obligations deriving from provisions of law and contractual agreements, financial obligations) as well as on other financial market entities, whose business activities are dependent on the operations of the KDPW Group and whose unintended disruption may result in severe adverse consequences, in particular including financial costs, breach of laws or loss of professional standing.

Support processes are processes, whose performance is necessary for critical processes to be fully realised, but they are not the main actions result in realisation of critical or important processes.

All remaining processes performed within the companies belonging to the KDPW Group, whose realisation may be delayed without causing any significant impact on the business functions carried out by the KDPW Group, or without leading to legal or financial consequences for the KDPW Group, shall be assigned the status of **ancillary** services.

II.3. Recovery parameters

The BCP System sets a Recovery Time Objective (RTO) for **critical processes** at **2 hours**, which is the maximum time from the occurrence of a contingency until the process is resumed.

The RTO of **important processes** is 4 hours, and the recovery of **support processes** should take place before the end of the relevant business day.

The BCP System does not envisage recovery of **ancillary processes** on the same business day that the emergency took place. In instances where it is expected that long-term access to the KDPW Group head office will not be possible, recovery of ancillary processes shall be determined on the basis of need within 1-5 business days.

The BCP System envisages a Recovery Point Objective (RPO) for critical and important processes at zero, meaning that the period between the last replication of data to back-up systems and the time of an emergency, for which data could be lost, should be zero.

Following the end of the emergency, full recovery of business activities by the companies belonging to the KDPW Group should take place including the possibility of work in the KDPW Group head office and the full redundancy of IT systems.

III. BCP System operational resources

The KDPW Group BCP System relies on the following operational resources:

- 1) back-up site and back-up IT systems;
- 2) teams of staff designated to deal with an emergency:

- a) The Crisis Response Group;
 - b) The Recovery Unit;
 - c) The Operational Group;
- 3) procedures and documentation.

III.1. The Business Recovery Site

In order to ensure business continuity in the event of emergencies, KDPW Group retains its own business recovery site, located at a reasonable distance from the primary location.

In order to ensure the continuity of business processes of the companies belonging to the KDPW Group, the business recovery site has been equipped in particular with the following:

- 1) back-ups of all IT production systems;
- 2) essential number of staff posts corresponding to the designation of company business processes being realised;
- 3) essential technical and office equipment;
- 4) a fixed telecommunication link, connected with the KDPW Group primary business site and holding sufficient capacity to transfer all production data online;
- 5) fixed links access to telecom operator services;
- 6) its own emergency power supply;
- 7) essential social facilities.

III.2. The Crisis Response Group

As part of the Business Continuity Planning System, the Crisis Response Group is established whose duties include in particular:

- 1) Analysis of the impact of an existing event on KDPW Group business operations;
- 2) Initiation of the Business Recovery Plan and coordination of all activities of the companies belonging to the KDPW Group in relation to business continuity management in the event of an emergency;
- 3) Analysis of the security level of KDPW Group operations and submitting relevant observations to the Management Boards of the KDPW Group.

In order to accelerate the recovery of the KDPW Group operations in emergencies, the Crisis Response Group acts as a decision-maker in the process of restoring the business operations of the KDPW Group and launching the execution of Business Recovery Plan procedures.

The responsibilities of the members of the Crisis Response Group in the event of an emergency are detailed in the Business Recovery Plan.

III.3. The Business Recovery Unit

The Business Recovery Unit is comprised of designated employees from the KDPW IT Systems Department (providing services to both KDPW Group companies). The role of the Business Recovery Unit is to make immediate preparations – as soon as possible following the start of an emergency – for the deployment of essential back-up IT systems, and if necessary, to prepare the business recovery site for the recovery of KDPW Group business processes, depending on the crisis management strategy approved by the Crisis Response Group.

III.4. The Operational Group

The Operational Group consists of designated employees from each organisation unit of companies belonging to the KDPW Group, whose business processes are covered by the BCP System.

The role of the Operational Group is to initiate the creation of specific staff posts in the event of an emergency, to monitor the level of completion of business processes and the state of applications, as well as to inform outside parties and employees of companies belonging to the KDPW Group of the emergency situation, which has arisen.

Following the completion of the status analysis of processes and systems, members of the Operational Group commence the recovery of each business process covered by the BCP System.

III.5. Procedures and documentation

BCP System Documentation includes the following elements:

- 1) BCP System Policy;
- 2) The Business Recovery Plan and the general recovery procedures;
- 3) Recovery rules for organisational units;
- 4) Operational procedures for organisational units.

The BCP System Policy provides general information on the KDPW Group's Business Continuity Planning System, its objectives and elements.

The Business Recovery Plan contains a general description of the critical points and an algorithm for recovery of the operations of the KDPW Group companies in an emergency, with reference to the general recovery procedures which set out the course of action to prepare the KDPW Group for an emergency.

The recovery procedures for organisational units set out detailed rules of measures to be undertaken in order to plan for the recovery of business processes by individual organisational units of the KDPW Group companies.

The operational procedures of the organisational units describe to the standard course of action regarding individual business processes by employees of the KDPW Group companies participating in the execution of those processes.

IV. BCP System testing

BCP System tests which check the readiness of the KDPW Group for operation in a crisis are performed regularly, including tests in co-operation with other financial market institutions at least once per year.

Moreover, every significant change in the area of business activities of the companies belonging to the KDPW Group, or of the business environment, and all major changes relating to technology within the IT environment will require testing of the relevant BCP System to be performed.

V. Maintenance and development of BCP System

Documentation related to the BCP System is reviewed and verified at least once a year and in the event of any significant disruption to the processes carried out by the KDPW Group companies.

The results of tests and review of BCP System documentation, the publication of standards as well as implemented legislation, performed operational risk analyses, and analyses of the impact that operational changes taking place in the KDPW Group and its business environment may have on the level of the Group's operational security, all form the basis for measures to improve and develop the BCP System, ensuring that it meets the required standard of efficiency.

In the event of an emergency requiring the Business Recovery Plan to be put into effect an additional review is required in order to evaluate:

- 1) the correct identification and classification of the event and its effect on the business operations of the KDPW Group;
- 2) whether the Crisis Response Group is performing its duties in the correct manner and all other processes are executed in a crisis;
- 3) whether the goals of the BCP System have been effectively met, including recovery time;
- 4) the skills of the employees carrying out their responsibilities as part of the BCP System.

Conclusions from a review form the basis for necessary improvements in the BCP System.