

Draft

Pursuant to the UNMIK regulation no.2001/26 on Payment Transaction and in accordance with article 9 of the Rule XVIII on Clearing and Operation of Settlement Accounts rules and procedures on Electronic Interbank Clearing System are established. As stated in article 4 this procedures are put in force aiming to ensure continuity of the interbank clearing operation unrehearsed situations

INSTRUCTION

**ON BACK-UP PROCEDURES FOR EXECUTION OF THE OPERATIONS OF THE ELECTRONIC
INTERBANK CLEARING SYSTEM OF THE CENTRAL BANKIG AUTHORITY OF KOSOVO**

1. Instruction on back-up for Electronic Interbank Clearing System (EICS) defines procedures for back-up for the execution of EICS operations in unrehearsed situations
2. Commercial banks in order to participate in the EICS shall develop back-up procedures for EICS operations in unrehearsed situations.
3. CBAK requests and instructs commercial banks to provide their back-up location
4. If commercial bank does not have its own back up location for execution of ICS it is necessary to enter into contractual agreement with at least one other commercial bank with similar services to execute operations in payment system in unrehearsed and insecure situations from contractor bank location
5. It is commercial bank responsibility to submit copies of agreement with at least one bank for bilateral relations for operations in payment system for CBAK to approve and enable operations in such situations.
6. It is commercial banks responsibility depending on official decisions about preparations of procedures or fulfillment of EICS in their back up location or with commercial banks agreement for mutual services for execution of operations in payment system during a situation of insecurity.
7. It is commercial bank responsibility to submit to CBAK copies of the procedures executed during situations of insecurity in the payment system.

Decision

On minimum computer configuration and back-up location for clearing payments

1. By setting minimum configuration of computers for clearing we define types of equipment that commercial bank shall provide during replacement of existing equipment for clearing with new equipment or when they are included in existing clearing.
2. In order to participate in the clearing, commercial bank shall provide configuration of computers and back-up configuration located at remote location.
3. Minimum configuration of computers or lower necessary for operation of commercial banks with ICS or be included in the clearing shall contain /include:

I. Hardware:

Server

PC

Dial-Up (or lease line , but prices are higher for use of lease lines)

Modem

II. Software:

MS Server 2003

MS SQL 2005

Windows XP

- **PC**
- **Pentium**
- **RAM**

- Hard disk
- Monitor
- Router
- Security card
- Firewall.....
- Windows XP workstation operative system
- Installation of required software (ICS)

4 Minimum configuration of computers for operation in commercial banks in order to complete payment system operations in harsh conditions, in cases of interruption of communication lines through network (cases with e-mail) are as follows:

- *PC*
- *Pentium*
- *RAM*
- *Hard disk*
- *Monitor*
- *Windows XP workstation for Operative System*
- *Internet connection*
- *Reading card.*
- *Installation of required software*

5. Computer equipment, main and reserve that need to be provided by commercial banks

6. According to agreement in force, computer equipment and back-up location shall be provided by commercial bank and be in use for six month before, implementing clearing rules. It is banks duty to prepare procedures for fulfillment of obligations in emergency situations and to submit a copy to CBAK

7. For equipment set out in article 3 of the decision it is commercial banks responsibility to take care, and bear expenses, installation and maintenance. Expenses for maintenance of the application for clearing system central bank will debit directly account in CBAK in accordance with applicable fees based on the agreement contract with provider / contractor.
8. Commercial bank is responsible to maintain and bear expenses for installment and maintenance of the computer equipment from article 6 of the agreement and clearing application.
9. Installment and maintenance for the application of the clearing system, central and reserve can be done only by authorized companies for maintenance of the payment system by CBAK

Draft

ELECTRONIC INTERBANK CLEARING AND SETTLEMENT SYSTEM

- CONTINGENCY OPERATION PLAN

NOTE: This is not an official translation and therefore is not in any way legally binding.

CONTENTS:

EQUIPMENT BACKUP FOR WHOLE EICS SYSTEM

CONTINGENCY MANUAL MEASURES

INTRODUCTION

According to the article 5 of UNMIK regulation No. 199/20, CBAK Rule XVIII on Interbank Payment Clearing and Settlement and UNMIK Regulation on Payment Transactions 2001/26 one of the principal objectives of the CBAK is to provide an efficient and safe system for domestic payments. In accordance with the procedures on Interbank Clearing and Settlement System (approved by the Governing Board on May 2003) the ICS at the CBAK maintain the backup ways of Interbank Clearing system and defines the backup way for all kind of Interbank payment operations. The measures for the contingency ICS system payment operation, which system will be in effect for responding to system emergencies. Primarily to **perform back-up of data** for whole system, and also have available critical facilities for continuing operations in the event of an emergency, and have **disaster recovery procedures**. Understanding that the contingency measures are to counteract the failures in EICS in any unpredicted situation. The exposure to risk is defined and appropriate measures are described in this manual, to prevent or counteract potential failures. To satisfy the requirement it is required that a contingency plan be in effect for responding to system emergencies, plan would be as:

- 1. Equipment back up for ICS system; hardware and software installation and maintenance in or out of site**

- 1.1.** A CBAK in order to maintain properly the full system of Inter bank clearing and settlement system should provide the **backup** firstly for ICS and also for CBAK core accounting system FC.
- 1.2.** A commercial bank in order to take part in ICS should provide the backup ways for ICS in the contingency situation
- 1.3.** CBAK/ICS suggest to commercial banks to provide the own back up location for the performance of the ICS in contingency situation
- 1.4.** If a commercial bank does not have the own backup location for the performance of the ICS, it is required to be ready in any way (including manual data exchange) but to be possible to participate in clearing session at last to contract the agreement with one commercial bank on the mutual services for the performance of the payments systems operations in the CONTINGENCY SITUATION
- 1.5.** Commercial Banks is responsible, depending of the Official decision to prepare the procedures for the performance of the full EICS in own back up location or with the commercial banks contracted with it on mutual services for the performance of the payments system operations in the contingency situation
- 1.6.** Commercial bank is responsible to deliver to the ICS at the CBAK a copy for the performance of the Inter Bank payment system in Contingency Situation

There may be any number of mediums incorporated within the institution to accomplish data processing needs. Networks are increasingly prevalent in the present multi-location banking environment. As with any other function in banking, operation of information systems presents certain risks and may ultimately impact safety and soundness of the institution. For this reason, the operation and control over information systems should be identified and reviewed at every **six month**. Protecting or securing information and facilities that process and maintain information is vital to the continuity of operations. It is essential that information be accurate, safeguarded and provided without interruption. In order to maintain continuity and reliability of information, institutions should, at a minimum, formulate a comprehensive security plan to ensure that operations and data are not vulnerable to undue risks and exposures. The plan should, at a minimum, address:

- 1) **Physical security;**
- 2) **Data security; and**

3) **Backup and contingency planning.**

Emergency Preparedness Plans are written as preparedness plans and off-premise storage of backup files for all critical records, to be maintained in the event of natural disaster or physical damage to premises.

Equipment back up for whole system; hardware and software installation and maintenance out of site

A disaster recovery plan including data backup for whole system:

Hardware and software installation and maintenance, review and testing for security features

Security procedures and testing

Virus checking

Procedures for verifying access authorization prior to access maintenance of the technical security services: To guard data integrity, confidentiality and availability

Access control

There would be a requirement for access control which would restricted access; and allow access only by authorized personnel in ICS system. Types of access control include among others, mandatory access control and classification on time of day.

I. Security purpose

The security purpose is to provide value by enabling an organization to meet all mission/business objectives while ensuring that system implementations demonstrate due care consideration of risks to the whole system.

Security requirements

NOTE: This is not an official translation and therefore is not in any way legally binding.

Security requirements generally include both requirements for the presence of desired behavior and requirements for the absence of undesired behavior. It is normally possible to demonstrate, by use or testing, the presence of the desired behavior. It is not always possible to perform a conclusive demonstration of absence of undesired behavior. Testing, design review, and implementation review contribute significantly to reducing the risk that such undesired behavior is present. The types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy. Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet ICS security policy.

A description of minimum requirements necessary for a system to maintain an acceptable level of security.

Security safeguards

Protective measures and controls prescribed to meet the security requirements specified for a system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. The protective measures and controls are prescribed to meet the security requirements specified for a system, hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices.

Security service

(I) A processing or communication service that is provided by a system to give a specific kind of protection to system resources. ICS back up provided by a layer of communicating, which ensures adequate security of the computer, systems or the data transfers. Security services implement security policies, and are implemented by security mechanisms. A service, provided by a layer of communicating open systems, which ensures adequate security of the computer systems or of data transfers

Sequence number

A time variant parameter whose value is taken from a specified sequence, which is non-repeating within a certain time period.

A system that provides a back up service in response to requests from other system entities called participants. A computer running a server program is frequently referred to as a server back up (plan to be used the old ICS system with infrastructure both servers and other equipments included and old PTK dial-up connection lines)

CONTINGENCY MANUAL MEASURES

To be maintained the inter bank clearing system in old classic manual way in any exposure of operational risk exist the full documented material on ICS procedures (**attached II**). In this case the clearing session will be held at the CBAK building (or out of site) at 15.30 o'clock, where the payment orders will be changed between the participants and CBAK; full data entry processes in manual way for all payment orders. The standard ICS form should be prepared by originating banks as single entries, paper lists of orders, or electronic files (diskettes) is identified by the CBAK standard identification number and according the standard format requested from CBAK as is described in detail in table below (ICS form 004, 005, 006, 007 and 008) the commercial bank can participate in daily clearing session.

To meet the required effects in arrangement with participants the ICS will maintain the payment system manually via an excel-sheet (by phone, fax or materially, basing in job experience, from time before where the ICS was implemented and a lot of flexibility was needed to maintain the system).

The payment orders in the central clearing system at the CBAK to be received in manual way: by persons (courier), via fax or through diskettes. Subsequently is the registering the payment orders in ICS (by ICS operator) and after that is the checking if the payments are properly accounted, and entry onto CBAK books.

When the all ICS calculations have been completed, the ICS Manager will prepare the debit or credit entry ticket for each bank (see the standard format of ICS which is presented in table below), and deliver it to the accounting department for posting to the bank settlement accounts accompanied by the completed form of ICS, 004, 005, 006 and 008. Account booking being in net base for all ordinary payments and individually for urgent payments. For exchanging paper and electronic media such as diskette files physically brought to the CBAK, in central clearing system (clearinghouse) also exist the following form of applications, which are accepted by all ICS participants.

FORMULARI MBI TRANSFERIN E LLOGARISË
STANDARD ACCOUNT TRANSFER FORM

Të transferuara nga / Transferred from Të transferuara nga / Transferred to

Numeric i Ilogarisë / Account number		Numri i Ilogarisë / Account number	
Klienti urdhërues/Ordering Customer		Emërtmi I Përfituesit/Rec.cust.name	
Valuta / Currency	Shuma / Amount	Currency	Amount / Amount
Ref.e klientit / Customer ref	Data e valutës / Value date		
Teksti / Text			

Detajet e transaksionit /
Transaction Details

Të transferuara nga / Transferred by

Name / Name	Adresa / Address :
-------------	--------------------

NOTE: This is not an official translation and therefore is not in any way legally binding.

Nënshkrimi / Signature
Nr.DI / ID No

V. V.
P.S.

Nënshkrimi - Signature

ICS Form 004

Batch payments

Number of PO

Amount

Total: _____

Name of Bank _____
Date,
ICS Form 005
Date

Name of Bank	Amount Brought	Number of Payment Orders	Amount Received	Number of Payment Orders
PCB				
BRK				
BpB				
BE				
RBKO				
BKP				
KSB				
CBAK				
Total				
Net				
	(Debit 005)		(Credit 006)	

Authorized Signature

Interbank Payment and Settlement System -
Payment order data
 ICS 006

Name of bank

Nr	Amount shuma-EURO	Ordering Customer Client urdhërues	Ordering Bank Bank underused	Banka Pranuese Receiving bank	Emri i Bankës (Shkurtesa)	Receiving Customer emri I shfrytëzuesit	Receiving Customer Name Emërtimi	Control Nr. kontrollit	Description Përshkrimi	Type of payment Lloji i pagesës
----	-------------------	------------------------------------	------------------------------	-------------------------------	---------------------------	---	----------------------------------	------------------------	------------------------	---------------------------------

NOTE: This is not an official translation and therefore is not in any way legally binding.

							i			
							Përfituesit			
1										
2										
3										
4										
5										
6										
7										
8										
	0.00	€TOTAL								

Certify that CBAK is ordering these payments on_____.

Consolidated Settlement Form

Date _____ ICS 007

Name of Bank	Amount brought	Number of Payment Orders	Amount received	Number of Payment Orders	Net Difference	Authorized Signature
PCB						
NLBBRK						
BpB						
BE						
RBKO						
BKT						
NLBKSB						

NOTE: This is not an official translation and therefore is not in any way legally binding.

CBAK						
Total						

Coordinating wide system

Through communication network, which means a telephone directory of all relevant internal and external communication participants (commercial banks and any other ICS client). In case of service interruptions, the ICS should be ready to coordinate the contingency communications, by: phone, fax, and materially through the contact persons (attach document). In case of a system failure the commercial banks inform the ICS manager about the problem. The ICS/CBAK take the following steps as are describing in above (daily sessions) in coordination with all participants.

ICS have the register with address, telephone, fax, e-mail address, and the communication structure is distributed also to the relevant persons in seven commercial banks. Only ICS participants are responsible for their own financial commitments, they can provide authorization service with independence and objectivity, with qualified personnel, adequate testing and review of information systems, adequate documentation of tests and findings of any corrective actions.

Gjylfidane Kastrati - Kadrijaj, Manager

Interbank Payment Systems Department

Central Banking Authority of Kosovo

33, Garibaldi Str. Prishtinë - Kosovë

Tel: ++381 222 055 279; Tel&Fax: ++ 381 229 253

Email: gjylfidanek@cbak-kos.org

Web Page: www.cbak-kos.org