UNOFFICIAL TRANSLATION

State registration with the	Approved by
Ministry of Justice of Azerbaijan Republic	Resolution of March 13, 2006 by the Management Board of the Central Bank of Azerbaijan Republic
Registration No. 3217 March 31, 2006	Protocol No. 07
Minister _________________ Fikret Mammadov	Governor of the Management Board ____________________ Elman Rustamov

REGULATION
FOR
IMPLEMENTATION OF INFORMATION TECHNOLOGIES IN BANKS

(as amended on October 9, 2006 and April 15, 2010)

BAKU - 2006

1. General provisions

1.1. This Regulation has been developed in accordance with the Laws of Azerbaijan Republic «On the Central Bank of Azerbaijan Republic», «On data, information and data protection», «On electronic signature and electronic document», other laws of Azerbaijan Republic, as well as best international practices, and identifies the procedures for implementation of information technologies in banks.

1.2. The principal objective hereof is to ensure the security of information technology (IT) systems, data and documents stored, to manage risks in order to minimize the effects of failures and errors, and to identify the minimum requirements for back-up copying and emergency solution/trouble-shooting procedures.

1.3. All banks shall develop and regularly upgrade their information systems and associated security arrangements in accordance with the provisions hereof.

2. Definitions

2.1. Terms and definitions used herein shall have the following meanings:

2.1.1. Information Technologies Department (ITD) — a unit of the bank providing information technology services;

2.1.2. Unauthorized access — an attempt to access information systems and electronic document/record base by an unauthorized user;

2.1.3. Strategic plan — planning of measures to be executed in the future in order to ensure successful long-term performance of the bank, a department or a unit;

2.1.4. Authorization — confirmation of entry of data contained in bank documents in the system;

2.1.5. Online interface — a form of direct online information and communication contact established between two or more system users;

2.1.6. «Hot» replacement — automatic replacement of hard disks (memory drives) by the system without suspending the operation of the server computers.

3. Main requirements to information technology systems

3.1. Banks must meet the following requirements in order to ensure high effectiveness and standardization of IT systems:

3.1.1. systems must operate in a reliable and consistent manner in accordance with the bank's information technology development strategy;

3.1.2. IT systems must be maintained in accordance with high level technology standards;

3.1.3. failure-proof capacities of IT systems in use must be evaluated on a regular basis;

3.1.4. when the IT system structure is approved, related responsibilities must be distributed among bank employees.

3.2. Data entered, processed and stored in IT systems must meet the operating needs of bank employees. Such data must comply with the bank's relevant guidelines and operating procedures, and delivered to users.

3.3. Security arrangements of IT systems shall be managed in accordance with the following requirements:

3.3.1. IT security plans must incorporate risk assessment procedures;

3.3.2. an IT security plan must be implemented;

3.3.3. the IT security plan must be updated to reflect any changes in IT systems;

3.3.4. effects of any changes in IT systems on the IT security system must be evaluated;

3.3.5. implementation of the IT security plan must be monitored;

3.3.6. IT security procedures must be harmonized with other policies and procedures of the bank.

4. Access to data in IT systems

4.1. Access of IT users to information systems must be controlled by authorization mechanisms. Such mechanisms should be designed to prevent any attempts of unauthorized access to computer systems and to stop any access attempts of entering the password more than 3 times.

4.2. Procedures must be developed and put in place to keep and liquidate records of user access. Banks must have written policies that identify information system access procedures for users and system administrators.

4.3. Banks must regularly reconcile system access/entry records against system access authorizations in order to minimize the risks of errors, fraudulent activities, misuse or unauthorized modification of IT systems or data stored in the system.

4.4. According to the security policy, banks must have appropriate physical safeguards and control arrangements for IT hardware to prevent any unauthorized external access to information systems. Physical security and control procedures must cover not only the premises where system hardware is located, but also location of lines used for interconnection of system elements, supporting services (e.g., power supply), back-up facilities and other elements necessary to operate the system.

5. Emergency handling procedures

5.1. Every bank shall take appropriate measures to ensure continuity of operation when IT systems are damaged, destroyed or threatened.

5.2. In order to ensure continuity of operations banks shall:

5.2.1. a Back-Up Center must be created for storage of back-up copies of systems in order to ensure reliable and undisrupted operation of IT systems;

5.2.2. written policies and structures must be developed and put in place for documentation of responsibilities, authorities and approach methodologies and continuity plans to be adopted.

5.3. Banks shall assess hazard and unauthorized access risks that may impact the continuity of operations, and shall have a strategic plan.

5.4. Banks shall identify possible damage levels and develop appropriate arrangements to address such damages in order to identify the anticipated impact of emergency hazards.

5.5. In order to ensure continuity of operations in emergencies, banks shall train relevant personnel in the IT emergency procedures to be followed.

6. Risk management requirements

6.1. The objective of risk assessment/analysis is to get a good understanding of security risks associated with material and information IT assets and to identify security measures to reduce the impact of risk levels.

6.2. Banks must properly identify risk management and assessment/analysis methods to ensure that controls are put in place in all IT-related areas. Risk assessment must be a continuous process and able to respond efficiently to any changes in the business of banking. A daily activity plan must be developed and put in place to ensure that risks are controlled and security arrangements are implemented on a continual basis.

6.3. Banks must implement the following operating system arrangements in order to reduce the information technology risks encountered:

6.3.1. maintain daily, weekly, monthly and annual back-up copies of databases;

6.3.2. maintain of back-up copies of daily logs of any changes in databases;

6.3.3. keep weekly back-up copies of the database for no less than 1 month, monthly copies no less than 1 year and yearly back-up copies not less than 5 years;

6.3.4. keep daily, weekly, monthly and yearly back-up copies on external memory drives;

6.3.5. before handing yearly copies over to the bank's archives, run them through a data restoration procedure on the back-up server;

6.3.6. operate document authorization mechanisms in the bank's operating system;

6.3.7. establish interfaces between the bank's operating system and other systems, including payment systems;

6.3.8. establish online interfaces between the bank's head office and branch offices, divisions and exchange bureaus;

6.3.9. maintain back-up copies of IT systems at the Back-Up Center.

7. Information security requirements

7.1.Data processing servers of banks must meet the following requirements:

7.1.1. use licensed software or freeware;

7.1.2. server applications must be agreed upon with the information security officer.

7.2.Business data processing servers must meet the following requirements:

7.2.1. archiving, back-up server, monitoring, anti-virus applications must be coordinated and identified in collaboration with the information security officer;

7.2.2. a management function must be put in place that meets the following requirements:

7.2.2.1. system administrators must be able to get user passwords;

7.2.2.2. a remote operation capacity must be available in the normal course of operation of the operating system.

7.3.IT system users and system administrators must be equipped with an authentification function meeting the following requirements:

7.3.1. each user must have an authentification code;

7.3.2. attributes of each user's authentification code must be clearly identified;

7.3.3. the system must have an authentification function;

7.3.4. groups must be used to identify user authorities;

7.3.5. system access must be provided in accordance with the set of authorities defined by the system administrators;

7.3.6. user password modification period must be not more than 60 days;

7.3.7. system user password must have at least 6 characters;

7.3.8. system administrator password must have at least 10 characters;

7.3.9. the password must be changed at the first entry to the system;

7.3.10. after 3 erroneous entries of a password, only system administrators must be authorized to lift the system access denial;

7.3.11. use of old passwords must be automatically prevented, maintaining an encoded record/history of the last 13 passwords;

7.3.12. an automatic verification function must be activated to check the complexity of passwords, that is, whether passwords have both letters and numbers;

7.3.13. passwords must not be displayed on the screen;

7.3.14. passwords must be changed by users individually;

7.3.15. passwords must be encrypted when transmitted via telecommunication systems;

7.3.16. password-protected screen savers must be made available.

7.4.The following requirements must be met when implementing cryptographic protection systems:

7.4.1. passwords must be maintained in encrypted form;

7.4.2. password transmission must be encrypted;

7.4.3. data must be encrypted when transmitted to external communication channels;

7.4.4. data must be recorded to external drives in encrypted form;

7.4.5. electronic signatures must be included for data transmissions.

7.5. Each bank shall have the following safeguards and security arrangements for server rooms:

7.5.1. only the personnel operating the servers and telecommunication hardware installed in server rooms must have access to these rooms;

7.5.2. the list of individual authorized to access the server rooms must be coordinated with the Security Department;

7.5.3. access to server rooms must be administered using electronic or mechanical locks;

7.5.4. access to server rooms must be limited to the bank's office hours only;

7.5.5. in emergencies, authorized persons must be granted access for the whole day with the Security Department's approval;

7.5.6. external specialists may work in server rooms only in the presence and under supervision of the bank's information technology and security personnel;

7.5.7. hardware must be installed, replaced and repaired in server rooms under the supervision of information technology and security personnel;

7.5.8. hardware may be removed from server rooms only with involvement of security personnel;

7.5.9. server rooms must be equipped with fire alarm systems;

7.5.10. server rooms must be equipped with a ventilation system;

7.5.11. server rooms must be equipped with a power generator and uninterruptible power supply source;

7.5.12. server rooms must be equipped with closed circuit surveillance cameras.

7.6. All servers and workstations of the bank shall have antivirus protection.

7.7. To provide antivirus protection of the bank's server and workstations:

7.7.1. the antivirus application/package installed on workstations shall be updated automatically on a daily basis;

7.7.2. an antivirus package shall be installed on all workstations and servers in addition to the module operated for real time checks of workstations and servers.

7.8. Banks must be equipped with back-up hardware in addition operating local network management hardware.

7.9. Payment and operating servers must be equipped with the following back-up facilities:

7.9.1. large capacity mirrorred hard-disks with «hot» replacement option;

7.9.2. automatic shutdown of a failing processor;

7.9.3. back-up server (if the operating server fails, it must be replaced with a back-up server in 1 hour).

7.10. If the system downtime is more than 3 hours when main servers fail, these servers must be replaced with the bank's Back-Up Center's servers.

7.11. The bank's power supply lines (fibers) must be duplicated by two different substations.

8. Vendor and provider requirements

8.1.All computer hardware of banks must meet the following requirements:

8.1.1. must have a certificate of origin;

8.1.2. hardware must be acquired from manufacturer-authorized dealers (representatives);

8.1.3. a written technical support agreement must be signed;

8.1.4. warranty period must be at least 12 months;

8.1.5. timeframe for repair or complete replacement of hardware from the time a relevant request has been made: 24 hours for servers, 48 hours for other hardware.

8.2.Software used in the bank's IT systems:

8.2.1. must be procured from a reputable vendor with at least 3 years of experience in software sales;

8.2.2. a support agreement must be signed with the software vendor;

8.2.3. the software vendor must provide at least 12 months of software support.

8.3.Communications provider must meet the following requirements:

8.3.1. must be licensed by the Ministry of Communications and Information Technologies of Azerbaijan Republic;

8.3.2. must be reputable;

8.3.3. must sign a supplier support agreement;

8.3.4. must operate in communications for at least 3 years.

9. Reporting

Banks shall submit their information technology reports together with prudential reports submitted to the Central Bank on an annual basis. The Central Bank shall determine the form and contents of such reports.

10. Final provision

This Regulation shall take effect upon the date of state registration.

UNOFFICIAL TRANSLATION

INFORMATION TECHNOLOGIES
REPORT

Name of bank

Report submitted by:

Full name	
Telephone	
Fax	
E-mail	

General:

Information technologies structure	

IT Security Unit	

Total number of branch offices			
Number of branch offices using the head office's information system	dedicated line	dial-up	other

Money transfer system used by the bank:

AZIPS	SWIFT	XOHKS WESTERN UNION
MoneyGram	Migom	Europay Visa
Trevelex	Other	

Payment system connection plans:

Networks and information systems available at the bank:

Internal local computer network	Web-site Internet
Bank Business Day:	Internal correspondence (mail) system
Other	

Internet connection:

dial-up dedicated line Internet access speed_________

The bank has an internal correspondence/communication system:

NO YES number of users ___________________

Hardware used by the bank:

	Number	Type and configuration
Server hardware		
Workstation computers		
Other hardware		

Licensed software:

Operating system	
Database management system	
Other	

The bank's Business Day System:

Name of the System used System developed by	
Support method	

Language of the System:

Azerbaijani Russian English Other

____

Automated modules or automated workplaces:

Statement/report development	
General Ledger management	
Uniform information book	
Loans	
Deposits	
Other	

Architecture of the Bank's Business Day and automated workplace systems (customer-server, etc.):

____

____

Interfaces connecting the Bank's Business Day system and other systems, and their description:

____

____

Interconnection and data sharing methods between branch offices and the Head Office:

____

____

A Back-Up Center is available:
NO YES location________________________________

Systems backed-up:

____

____

Timeframe for emergency restoration of systems and operations:_______________

Plans for upgrade and development of the existing systems and introduction of new systems in the next year:

____

____

Development of the local network and implementation of new technologies:

____

____

Information security

An umbrella document is in place that identifies information security arrangements (concept, policy, regulation, etc.):

____

____

Information security development plans:

____

____

Corporate network security capacities of the Bank:

____

____

Antivirus protection facilities (availability of licenses):

____

____

Current problems of the Bank:

____

____

Signatory: _______________

Date: _______________