Syrian Arab Republic

Monetary and Credit Council

Decision No. (1150/M.C.C)

Monetary and Credit Council,

Pursuant to:

- The provisions of Law No. /23/ of 2002 and amendments thereto.
- Letter No. 290, dated 12/08/2014, sent by the managing director of the Directorate of Information Technology, attached to which are the regulations and procedures of using CCTV in banks operating in the Syrian Arab Republic.
- The proposal submitted by the Administration Committee of the Central Bank of Syria in its decision No. 1045/M.C dated 12/08/2014.
- And the revision thereof in its session convened on 17/08/2014.

Decided the following:

Article 1- Granting approval to the adoption of regulations and procedures of using CCTV in banks operating in Syrian Arab Republic, included in Version (1.1) dated 07/08/2014 (attached herein).

Article 2- this decision shall be communicated to all relevant parties for implementation.

Damascus, 17/08/2014

(signed)

Secretary of Monetary and Credit Council **Laila Tannous**	**Head of Credit and Mony Council** **Dr. Adib Mayaleh**
(Signed)	(Signed)

Number of copies (), to be sent to:

Syrian Arab Republic

Monetary and Credit Council

Regulations and Procedures of Using CCTV in Banks Operating in the Syrian Arab Republic.

Version 1.1
07/08/2014

(Three signatures at the end of this page and subsequent pages)

Signed with 3 signatures

Table of Contents:

Preamble:

CCTV surveillance is one of the physical security measures in facility security systems. Facility security means **preserving the safety of the premises of the facility and its occupants, and ensuring the continuity of its operations and activities in a secure environment**.

CCTV system is one of the methods of:

- Providing proactive security measures, as it helps monitor any suspicious activities that may pose a threat to the facility.
- Post-event protection, CCTV recordings can aid in discovering incidents of defalcation or mistakes that may occur.

Objective:

Central Bank of Syria seeks, through this study, to establish a set of guidelines and procedures for the installation and utilization of a CCTV system. Compliance with these guidelines and procedures is essential to ensure a secure working environment and minimize potential risks.

The guidelines and procedures will be categorized as follows:

1. **Defining the purpose of the system and its design principles.**
2. **Technical specifications for system components.**
3. **Policies for system usage.**
4. **Models for verifying the effectiveness of the system.**

First – Defining the purpose of the system and its design principles:

The design of any CCTV system relies on:

1- <u>Two fundamental principles:</u>

1-1 . **Identifying checkpoint locations**:

Which are the spots that individuals or vehicles must pass through to enter the institution. For CBS, these spots are:

- The entire perimeter of the building.
- Entrances and exits of the building.
- Entrances and exits of the garage.
- The garage.
- Lobbies and corridors.
- Client service and visitor reception areas.
- Money machine rooms.

1-2 . **Protecting assets**:

Which are the set of areas or objects requiring monitoring, **<u>such as</u>** physical items like safes and money rooms, as well as critical activity areas like cash registers and parking lots.

Asset determination is based on the institution's needs and priorities, which, for CBS, are as follows:

- Money rooms.
- Secondary money vaults.
- Cash during transportation to and from the bank.
- Technical and information management rooms.
- Document archives.
- Warehouses.
- Internal and external ATMs.

2- <u>System designing method:</u>

The design of any surveillance system begins with answering the following questions:

2-1 From the functional perspective:

Q1. What are the spots that need to be monitored?

Q2. What are the periods during which monitoring is required (during specific hours, during working hours, outside official working hours, other…)?

Q3. What activities need to be monitored, and what are the potential risks?

Q4. What is the purpose of the surveillance, and what details are required in the footage?

Q5. What is the rate of motion in the monitored scene; (High, medium, low, very low, static)?

Q6. Who is responsible for surveillance, and live surveillance periods?

Q7. What is the type of surveillance? Direct surveillance by specific individuals, event-based surveillance with alarms, or pre-programmed surveillance with alarms at certain events?

Q8. Who is responsible for live surveillance and surveillance periods, and where does surveillance take place?

Q9. If there are other security systems, are they linked to the CCTV system? What events trigger responses from the CCTV system (system inputs)? What actions should the system take when an alert is triggered (system outputs?

Q10. Is it necessary to have night surveillance? Is the lighting sufficient? Does it require filtering?

2-2 Once the functional needs or sites that require monitoring are identified, it becomes possible to answer the following basic technical questions:

Q1. How many cameras are sufficient for monitoring each site, what are their specifications, installation methods, protections, how to link them with other security systems, power supply, and signal type?

Q2. What type of cables is suitable, what are the appropriate standards for cable installation, and what is the required signal quality?

Q3. What are the suitable intermediary devices (video encoders, signal amplifiers, network switches…)?

Q4. How should the cameras be connected to the management system?

Q5. What type of management system should be used (DVR, NVR, server-based system…)?

Q6. What type of storage should be used (SAN Storage, NAS Storage, server-based storage…)?

Q7. What type of analysis should be used?

Q8. How should the system be viewed?

Q9. How should integration between the surveillance system and other systems be achieved? (in case other security systems are available, such as access control systems, security doors, alarm systems, or evacuation systems).

Q10. Is remote monitoring available (linking surveillance systems for branches together)?

2-3 Regarding legal aspect:

Q1. Are there any restrictions that must be adhered to in the installation or use of CCTV surveillance?

Q2. Is there a need to place signs or banners indicating that the site is under surveillance? Can surveillance be covert? Which requires focus on prohibiting the installation of moving cameras or cameras with zoom lenses in areas that infringe upon public freedoms and privacy?

Q3. Are there any restrictions regarding the periodic inspection of cameras or access to surveillance system equipment for maintenance?

Q4. Which cameras can or should have their images displayed on public display screens (e.g. for clients)?

Q5. Which cameras' images can only be viewed by specific individuals?

Q6. Is the surveillance system connected to a security entity (the police for example)?

Q7. Legally, what is the law that must be complied with regarding data retention and access thereto?

2-4 Post utilization:

Q1. How to evaluate the effectiveness of the system?

Q2. Are there recurring malfunctions in the system, and what is the extent of availability of the surveillance system?

Q3. Is periodic maintenance carried out according to a predefined schedule, and what is the level of response to malfunctions?

Q4. Does the system support development and expansion when necessary?

3- Identifying key components of the system:

Cameras, camera covers, holders, motors, cables, signal amplification devices, video encoders, monitoring screens, network linking devices, storage units, management system, recording and archiving system, analysis system, monitoring room, etc.

Second – Key components of the CCTV system:

When the area to be monitored is determined, it becomes possible to specify the type and specifications of the cameras, and consequently, the rest of the system components will be defined.

2-1 Cameras:

The following main specifications of the cameras shall be defined:

1. In terms of the place of installation: We have indoor and outdoor cameras.
2. In terms of Night Vision: We have coloured daytime cameras that detect normal lighting for sites requiring only daytime monitoring, and colour daytime and nighttime cameras in normal lighting conditions and non-colour cameras in low-light conditions, which can detect low light through an automatic filter switching to infrared mode in extremely low or absent lighting conditions, with the necessity of having IR light source for night vision in sites requiring nighttime monitoring or in low-light conditions.
3. Fixed cameras compared to rotating cameras:
   A. Fixed cameras are used to view a single perspective and can be box-shaped or dome-shaped.
   B. Rotating cameras are used to view multiple perspectives, areas of continuous activity, moving targets such as vehicle movement areas, client reception areas, and for monitoring surrounding streets, (especially when monitoring cash transportation). These cameras can be box-shaped with the possibility of rotation using a special rotating motor or the PTZ type motor capable of scanning 360 degrees horizontally and 180 degrees vertically. Movement of the cameras can be manual or automated.
4. Lenses: We have separate lenses and lenses that are integrated with the camera. The lens can be of fixed-focus, which are suitable for scenes with a fixed horizontal field of view, or of automatically changing focus (controlled via DC control or video signal) which are suitable for sites with a variable horizontal field of view.
5. Maximum required Decision for the camera:

330X240	QVGA
352X240	CIF NTSC
320X288	CIF PAL
640X480	VGA
704X240	2-CIF-H NTSC
704X288	2CIF PAL
704X480	4CIF NTSC
704X576	4CIF PAL
800X600	SVGA
1280X720	HD
1280X960	1.22 MP

1280X1024	1.3 MP
1600X1200	2 MP
1920X1080	Full HD
2048X1536	3 MP
2288X1712	4 MP
2600X1950	5 MP

6. Audio Support: IP cameras support two-way audio.
7. IP cameras compared to Analog cameras.

Currently, IP cameras offer the best possible vision and clarity. It's advisable to install them when setting up a new system or completely replacing an old one. If IP cameras are used and connected via the internet for remote access or for linking with branches, multi-layered protection systems should be employed. These protection systems should include advanced encryption systems (AES 256) and robust authentication systems for equipment and software applications to prevent unauthorized access. Additionally, if the institution desires to fully exploit existing systems or upgrade them without replacement, it can apply a mixed solution of cameras according to the locations, provided that the recording and retrieval system is able to handle this mix of equipment and technologies. For example, it is possible to install:

- Fixed analogue infrared cameras around the building perimeter.
- Rotating analogue cameras with wide-view angles in the parking lots.
- Inside the building: it is possible to install fixed cameras with megapixel Decision in warehouses, and a number of IP cameras covering entrances and corridors.

2-2 Rules for the Installation and Protection of Cameras:

2-2-1. Camera box: External cameras should be protected by external enclosures shielding them from vandalism and weather elements and rain, while internal cameras should have sufficient protection available.

2-2-2. Mounting and Fixation: Appropriate standard mounting elements should be specified for each type of cameras.

2-2-3. Reflections: Light reflections on glass towards the camera should be avoided.

2-2-4. Security: Cameras should be installed in secure locations that are difficult to access and tamper with.

2-2-5. Adequate lighting, including IR illuminators, should be added to ensure proper illumination.

2-2-6. Direct exposure to sunlight should be avoided.

2-2-7. Bright areas in the scene should be avoided.

2-2-8. Contrast should be optimized where possible.
2-2-9. Auto-focus lenses should be used in outdoor locations.
2-2-10. Camera settings should be adjusted to optimize performance for its location.

2-3 Cables, Connection, and Power Supply:

2-3-1 Varies according to the type of camera, whether IP camera or Analog camera:

2-3-1-1 IP Camera:

- The data cable is a suitable cable for the network, while power supply should be Power over Ethernet (PoE) cables, or the one that operates under Protocol IEEE802.3af, which allow power supply through the same network cable.
- For cameras that do not support Protocol IEEE802.3af: checking power cables and adapters to reach the power source.

2-3-1-2 Analog cameras:

These cameras shall be treated similarly to IP cameras that do not support Protocol IEEE802.3af in terms of power supply. However, for data signal, coaxial cables should be used.

2-3-1-3 Regardless of their type, all cables connecting to the cameras should be hidden whenever possible, either over false ceilings, if any, or within conduits that are difficult to access or tamper with.

2-3-1-4 power supply must be stable, continuous, and uninterrupted.

2-4 Monitors:

2-4-1 Based on the institution's activities and needs, surveillance or monitoring can be:

- Direct monitoring, based on the monitored activity, such as cash receipt or handing, cash payments ….
- Archival recording: for investigations into cases of fraud or embezzlement…

2-4-2 Depending on the size of the institution, surveillance can be done through:

- Computer.
- Or monitors on the walls allowing simultaneous monitoring of multiple cameras.

2-5 Management, recording, and analysis system:

Based on the size of the institution, this system can be installed on a server, computer, DVR, or NVR. In all cases, the system should meet the following specifications:

2-5-1 to support playing and recording full, natural, and real-time audio for each camera (Audio recording capability).
2-5-2 Motion detection capability activation on the cameras, and it should support motion-triggered recording (video motion detection).
2-5-3 It must support multiple search levels (by date, camera, or event…etc.).
2-5-4 It must support image enhancement by adding brightness or colour saturation.
2-5-5 Supporting review and playback of recorded data while continuing recording.
2-5-6 Automatic alarms for camera failure, network disconnection, or disconnection of the cable to which a camera or multiple cameras are linked.
2-5-7 capability to display the status of surveillance recording storage disks and give appropriate alerts, such as audio or visual alerts for errors of full storage disk, stopped recording….
2-5-8 Ability to control alerts based on the motion in front of the cameras and based on video motion or motion sensor.
2-5-9 Ability to detect loss of signal for any channel (video loss), and giving an audio or visual alert.
2-5-10 The system must support: footage playback, footage magnification, fast forward, pause, rotating recording when the memory space allocated for recording is almost depleted, and give alert when desks are almost full.
2-5-11 Real-time feed, with the possibility of inserting date, time, and name of the camera into the footage, and renaming each camera.
2-5-12 The program shall support the feature of handling interactive maps of the location, in addition to the possibility of reviewing and controlling any camera by clicking its icon on the interactive map, along with the possibility of categorizing cameras into formerly specified groups (monitors) chosen as needed.
2-5-13 Capability to capture snapshot images from any scene of any camera.
2-5-14 Support compression of footage (Motion JPEG, MPEG-4, H.264). 2-5-15 Support image analyses feature to reduce network load.
2-5-16 Support equipment of direct connection with LAN (Local Area Network) or WAN (Wide Area Network).
2-5-17 Recording on network-attached storage units.

2-5-18 Regarding recording:
Recording is one of the most significant basics of designing CCTV systems, and it's crucial to ensure that the system's recording requirements are sufficient

to meet operational needs, in addition to a storage space of at least 25% of the storage capacity (to calculate for variations resulting from differences in used compression systems, which is resulted in turn from the amount of motion). Recording depends on:

2-5-18-1 duration of the recording: the type of security threats affects the determination of storage duration, for example, the main threat to banks is the investigation report of forgery, which is often reported by affected clients only after 60 or 90 days after the incident.
Accordingly, banks have a great need for long-term storage, with a minimum duration of three months.

2-5-18-2 Depending on the image and motion analyses significantly decreases the storage spaces according to several criteria, as follows:

1. According to locations or check spots.
2. According to timing: during working hours and peak hours, outside working hours, and holidays.

3. According to recording method: (continuous recording, event-triggere recording, or manual recording).

4. According to the number of cameras.
5. According to camera Decision:
6. According to the number of frames per second per camera and scene change rate.
7. According to the video compression system used: (best compression system is H.264, followed by MPEG-4, then Motion JPEG).
The table below outlines the storage requirements according to the Decision of the used camera:

Storage Requirements			
Camera Decision	Per day	Per week	Per month
640X480, (15 fps)	32.4 GB	227 GB	1.7 TB
640X480, (5 fps)	16.2 GB	114 GB	0.502 TB

Notice: the requirements of transmission over the network must be considered.
2-5-18-3 Storage method: which is determined based on the size of the institution and the nature of its operations, as it can be:

- Directly on DVR (Digital Video Recorder) (DVR doesn't support IP cameras).
- Directly on NVR (Network Video Recorder) (supports analogue cameras when there is a compatible system between them).

- On a central server with storage units.

When adopting any recording method, we should take into account not to affect the clarity and speed of the footage, i.e. real-time recording.

The table below outlines the required Decision according to the location of the camera:

Checkpoint	**Minimum frames per second (fps)**
Limited activity areas in the institution / perimeter of the building.	5 (NTSC) / 4 (PAL)
Access control areas	5 (NTSC) / 4 (PAL)
Ticket machines and payment devices	15 (NTSC) / 12 (PAL)
Vehicle movement areas, The garage	30 (NTSC) / 25 (PAL)

2-5-19 Method of archiving, backup, and data retention:

The institution shall adhere to the following principles:

A. Store recordings on external storage devices to allow accessing them when needed, especially if the DVR, NVR, or server does not allow recording for the specified period of /3/ months.
B. The institution can choose which cameras to save recordings from based on the importance of the location of the camera being recorded.
C. In case of an incident requiring review, it should be saved on an external device.
D. Establishing a policy for storing backups, controlling access to it, designating personnel authorized to access and retrieve data from it.
E. Store digital recording devices in secure locations that are difficult to tamper with.
F. Store hard drives in secure and clean locations away from sunlight, magnetic fields, fire, and explosions.

Third – System Usage Policies:

The institution shall:

3-1 Ensure the presence of a responsible employee who is knowledgeable in security operations, capable of managing and operating the security system, and with good ethics and reputation, and to ensure that capacities and authorization boundaries are clearly specified or defined.

3-2 Define four levels of permissions for managing and using the system, this matter depends on the size and field of operations of the institution:

- **Level 1: System administration and initial and ongoing settings.**
- **Level 2: Permanent operating (monitoring).**
- **Level 3: Access to backups.**
- **Level 4: Access to stored backups.**

Fourth – Models of verifying the effectiveness of the system:

Once the system design is complete and the necessary diagrams for the camera placements and their numbers are in place, verification of the system's effectiveness is conducted through the following tables:

Table /1/: Checkpoints and locations to be monitored.

Table /2/: Asset protection.

Table /3/: Activities to be monitored and potential risks.

Table /4/: Cameras, cables, connections, and power supply.

Table /5/: Effectiveness of the surveillance system.

Table /6/: Effectiveness of the recording system.

Table /7/: Administrative and legal aspects.

Table /8/: Maintenance.

Table /1/: Checkpoints and locations to be monitored:

Question	Answer	Notes
Does the system cover the entire perimeter of the premises?		
Does the system cover all entrances and exits?		
Does the system cover the entrance and exit of the garage?		
Does the system cover the motion and activity in the lobbies and corridors?		
Does the system cover the areas of reception of clients and visitors?		
Does the system cover the money machines rooms?		

Table /2/: Asset protection:

Question	Answer	Notes
Does the system cover the entire perimeter of the premises?		
Does the system protect money rooms?		
Does the system protect secondary money vaults (safes, treasurers….)?		
Is the transportation of money to and from the bank safe for the money itself?		
Is the transportation of money to and from the bank safe for the clients?		
Is the transportation of money to and from the bank safe for the employees?		
Are the server rooms and the activities therein safe and monitored?		
Are the activities and motion within the warehouses and document archive clear and monitored?		
Are the ATM booths safe from the inside and outside?		

Table /3/: Activities to be monitored and potential risks:

Activity	Answer	Notes
Entrance of the employees		
Entrance of the clients and visitors.		
Receiving money from the clients		
Handing money to clients		
Transferring money from money rooms		
Transferring money to money rooms		
Money counting process		
Providing services to the clients		
Ongoing operations within the server rooms and technical equipment.		

Table /4/: Cameras, cables, connections, and power supply:

Question	Answer	Notes
Is the type of the cameras suitable for the purposes of indoors and outdoors surveillance?		
Are the external cameras installed and fixed properly?		
Are the cameras protected from natural factors and elements (dust, rain, sunshine, heat sources…)?		
Can the cameras be reached for the purpose of tampering with?		
Do any cameras face the problem of light reflection or excessive illumination?		
Is the contrast of the cameras' feed appropriate?		
Are the lenses of the cameras well-focused?		
Is the illumination sufficient for capturing good footage? Are their IR illuminators for night vision?		
Are the cables and installations concealed?		
Can the cables (network, power supply, or signal cables) be reached for the purpose of tampering with?		
Can the connection points (in case of using IP cameras) be reached for the purpose of tampering with?		
Is the entire surveillance system powered by a UPS (Uninterruptible Power Supply)?		
Is electricity feed continuous over 24 hours?		
Is electricity feed stable {protected with an electrical current optimizer or a UPS that supports On-Line technology}?		
Are there any critical cameras (in terms of distance, for example) and test results?		

Table /5/: Effectiveness of the surveillance system:

Surveillance system effectiveness indicators	Answer	Notes
Detect		
Monitor		
Recognize		
Identity		

Table /6/: Effectiveness of the recording system:

Question	Answer	Notes
What is the duration of playback (recording) period?		
When reviewed, does the footage achieve clarity and accuracy?		
Does the system provide search capabilities and ease?		

Table /7/: Administrative and legal aspects:

Question	Answer	Notes
Are there any visible signs showing that the premises is monitored by cameras?		
Are there any covert cameras?		
Is the system linked to any official entities or authorities concerned with security and safety?		
Who is responsible for the surveillance process?		
Who is the keeper of the recordings?		
Who is authorized to review saved recordings?		
Who has access to saved recordings?		
Is the place where recordings are saved safe and adequate for the possibility of access?		
Where are the monitors located?		

Table /8/: Maintenance:

Question	Answer	Notes
Are there any periodic maintenance cards?		
Does the maintenance card include the history and sort of malfunctions?		
Does the maintenance card include the date of fixing the malfunctions?		