

# **EMSA Video-Surveillance Rules**

## **SECURITY RULES**

Version: 1.0

Date: 01/05/2016

## Document History

Version	Date	Changes	Prepared	Approved
1.0	02/05/2016	None	A.2	ED

# Table of Contents

<b>1. Purpose, scope and legal basis of the Agency's Video-Surveillance Rules .....</b>	<b>4</b>
1.1 Purpose and scope.....	4
1.2 Legal basis .....	4
<b>2. Specific characteristics of the Agency video-surveillance system.....</b>	<b>4</b>
2.1 Revision of the existing system .....	4
2.2 Compliance status .....	5
2.3 Self-audit.....	5
2.4 Notification of compliance status to the EDPS .....	5
2.5 Contacts with the relevant data protection authority in the host Member State .....	5
2.6 Director's decision and consultation .....	5
2.7 Transparency.....	5
2.8 Periodic reviews .....	6
<b>3. Areas under surveillance .....</b>	<b>6</b>
<b>4. Type and purpose of the surveillance .....</b>	<b>6</b>
4.1 Summary description and detailed technical specifications for the system .....	6
4.2 Purpose of the surveillance .....	7
4.3 Purpose limitation .....	7
4.4 Ad hoc surveillance foreseen .....	7
4.5 Webcams.....	7
4.6 Special categories of data collected .....	7
<b>5. Legal basis of the video-surveillance .....</b>	<b>7</b>
<b>6. Access and disclosure of information .....</b>	<b>7</b>
6.1 In-house security staff and outsourced security-guards.....	7
6.2 Access rights .....	8
6.3 Data protection training .....	8
6.4 Confidentiality undertakings .....	8
6.5 Transfers and disclosures of information .....	8
<b>7. Protection and safeguarding of the information .....</b>	<b>8</b>
<b>8. Storing of the data .....</b>	<b>9</b>
<b>9. Provision of information to the public.....</b>	<b>9</b>
9.1 Multi-layer approach .....	9
9.2 Specific individual notice .....	9
<b>10. Verification, modification or deletion of information .....</b>	<b>10</b>
<b>11. Right of recourse .....</b>	<b>10</b>
<b>12. Final provision .....</b>	<b>10</b>
<b>13. List of Attachments .....</b>	<b>10</b>



# 1. Purpose, scope and legal basis of the Agency's Video-Surveillance Rules

## 1.1 Purpose and scope

For the safety and security of its buildings, assets, staff and visitors, the European Maritime Safety Agency (the Agency) operates a video-surveillance system. These Video-Surveillance Rules, along with their attachments, describe the Agency's video-surveillance system and the safeguards that the Agency takes to protect the personal data, privacy and other fundamental rights and legitimate interests of those individuals whose images may be caught by the cameras.

The purpose of the video surveillance system is the reduction and prevention of security incidents. The system helps to ensure the security of the buildings, the safety of staff and visitors, as well as property and information located or stored on the premises, by means of controlling access to the Agency buildings in compliance with Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data and the applicable Portuguese legislation as well as the European Data Protection Supervisor (EDPS) Guidelines.

The video surveillance system, which operates through a CCTV camera system, complements other physical security measures, such as access control systems and physical intrusion control systems. It forms part of all the security measures taken within the Agency and helps to prevent, deter, and if necessary, investigate unauthorised physical access, including unauthorised access to secure premises and protected rooms, ICT infrastructure, or operational information. In addition, video surveillance helps to prevent, detect and investigate theft of equipment or assets owned by the Agency, visitors or staff, or threats to the safety of personnel working at the offices (e.g. fire, physical assault).

## 1.2 Legal basis

These Rules are based and framed by the following laws and regulations:

- Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (the Regulation 45/2001);
- The European Data Protection Supervisor Video-Surveillance Guidelines (Guidelines) on 17 March 2010 and Video-Surveillance - Follow-up from 2013;
- Lei n.º 67/98 de 26 de Outubro, Lei da Protecção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados);
- Lei n.º 35/2004 de 29 de Julho (Regulamento Do Código Do Trabalho);
- Lei n.º 49/2008 de 27 de Agosto (Lei de Organização da Investigação Criminal);
- Lei n.º 34/2013 de 16 de Maio (Regime Do Exercício Da Atividade De Segurança Privada).

# 2. Specific characteristics of the Agency video-surveillance system

## 2.1 Revision of the existing system

A video-surveillance system had already been operating in the Agency before the issuance of the Video-Surveillance Guidelines by the European Data Protection Supervisor ("Guidelines") on 17 March 2010:

[https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17\\_Video-surveillance\\_Guidelines\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf) and the "Video-Surveillance - Follow-up" from 2013:



[https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/12-02-13\\_Report\\_CCTV\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/12-02-13_Report_CCTV_EN.pdf)

The Agency procedures, however, are hereby being revised to comply with the recommendations set forth in the Guidelines.

## 2.2 Compliance status

The Agency processes the images in accordance with both the Regulation (EC) No 45/2001 and the Guidelines and on the protection of personal data by the EU institutions and bodies.

## 2.3 Self-audit

The system is subject to a self-audit on an ad-hic basis.

## 2.4 Notification of compliance status to the EDPS

Considering the limited scope of the system, it was not necessary to carry out a formal impact assessment (Guidelines, Section 3.2) or to submit a prior checking notification to the EDPS (Guidelines, Section 4.3). However the Executive Director, Staff committee and the Agency DPO have been consulted by the means of a Note dated 17 December 2015 'On Enhancement of video-surveillance in the Agency Premises' describing the main characteristics and proposing upgrades of the system.

Simultaneously with adopting these Video-Surveillance Rules the Agency also notified the EDPS of its compliance status by sending a copy of its Video-Surveillance Rules.

## 2.5 Contacts with the relevant data protection authority in the host Member State

The competent data protection authority in Portugal (Comissão Nacional de Protecção de Dados) was informed about the installation of the video-surveillance system on the outside of the building. On the-spot notices on video-surveillance are also available in Portuguese language.

## 2.6 Director's decision and consultation

The decision to use the current video-surveillance system and to adopt the safeguards as described in these Video-Surveillance Rules was made by the Director of the Agency after consulting the Agency's Security Officer (Head of Unit A.2), the Agency's Data Protection Officer and the Staff Committee.

During this decision-making process, the Agency demonstrated and documented the need for a video-surveillance system as proposed in these rules, discussed alternatives and concluded that the maintenance of the current video-surveillance system, after the adoption of the data protection safeguards proposed in these rules, is necessary and proportionate for the purposes described in Section 1 (Guidelines, Section 5), and addressed the concerns of the DPO and the Staff Committee (Guidelines, Section 4).

## 2.7 Transparency

The Video-Surveillance Rules have two versions, a version for restricted use and this public version available and posted on Agency internet: <http://emsa.europa.eu/> and intranet sites at <http://emsanet/>. This public version of the Video-Surveillance Rules contains a summary information with respect to particular topics or attachments. Information is only omitted from the public version when the preservation of confidentiality is absolutely necessary for compelling reasons (e.g. for security reasons or to preserve the confidentiality of commercially sensitive information or to protect the privacy of individuals).

## 2.8 Periodic reviews

A periodic data protection review will be undertaken by the Unit A.2 every two years save in justified cases may be carried on more frequently, the first by 31 May 2017. During the periodic reviews the following aspects of the system will be re-assessed:

- if there continues to be a need for the video-surveillance system,
- if the system continues to serve its declared purpose, and that
- if adequate alternatives remain unavailable.

The periodic reviews will also cover all other issues addressed in the first report, in particular, whether the Video-Surveillance Rules continue to comply with the Regulation and the Guidelines (adequacy audit), and whether they are followed in practice (compliance audit). Copies of the periodic reports will also be attached to these Video-Surveillance Rules in Attachment 1.

## 3. Areas under surveillance

The video-surveillance system consists of 64 fixed cameras. A map with the location of the cameras is included in Attachment 2.

Based on their type and location the cameras are divided into 3 categories:

1. Five (5) cameras of the type 'Domus' are located on the facade of the main the Agency building. They are movable (head) type of cameras with a 'zoom' function;
2. Nineteen (19) cameras are located as fixed cameras in the inside of the Agency building. They are facing the entrances and other access points of the building. This includes also possible entrance points from the south side of the building (the courtyard and the garden) which are considered to be particularly vulnerable from a security perspective.

The above categories of cameras cover also the Agency LRIT Data Centre and are operational on a 24/7 basis.

3. Forty (40) cameras are located in the inside of the Agency building and cover the common areas such as corridors and hallways. They operate on a daily basis between 20:00h and 8:00h (i.e. outside of working hours).

Besides the cameras mentioned above, there are no cameras elsewhere either in the building or outside of it. There is no monitoring of areas under heightened expectations of privacy such as individual offices, leisure areas, toilet facilities and others (Guidelines, Section 6.8). The location of the cameras was carefully reviewed to ensure that they minimise the monitoring of areas that are not relevant for the intended purposes (Guidelines, Section 6.1).

Monitoring outside our building on the territory of Praça Europa in Lisbon, Portugal is limited to an absolute minimum (Guidelines, Section 6.5), meaning that the CCTV cameras are located and installed in a way to face only the entrance points of the Agency building but not the surroundings of it (as indicated in the description above).

## 4. Type and purpose of the surveillance

### 4.1 Summary description and detailed technical specifications for the system

The Agency video-surveillance system (as described in chapter 3 above) is a conventional system. It records digital images and is equipped with motion detection. It records any movement detected by the cameras in the area under surveillance, together with time, date and location. All cameras operate daily, as described under point 3 'Areas under surveillance' above. The image quality normally allows identifications of persons recorded within the camera's area of coverage. The cameras are all fixed in a way that they cannot be used by the operators to follow individuals around.



The Agency does not use high-tech or intelligent video-surveillance technology, does not interconnect its system with other systems nor engages in covert surveillance, using sound recording or "talking CCTV" (Guidelines, Section 6.12). The technical specifications for the cameras and for the video-surveillance system as a whole (including any software and hardware) are included in Attachment 3.

## 4.2 Purpose of the surveillance

The Agency uses its video-surveillance system for the sole purposes of security and access control. The video-surveillance system helps control access to the Agency building and helps ensure the security of the building, the safety of the staff and visitors, as well as property and information located or stored on the premises. It complements other physical security systems such as access control systems and physical intrusion control systems. It forms part of the measures to support Agency's broader security policies and helps prevent, deter, and if necessary, investigate unauthorised physical access, including unauthorised access to secure premises and protected rooms, IT infrastructure, or operational information. In addition, video-surveillance helps prevent, detect and investigate theft of equipment or assets owned by the Agency, visitors or staff, and threats to the safety of visitors or personnel working at the office (e.g. fire, physical assault).

## 4.3 Purpose limitation

The system is not used for any other purpose, for example, it is not used to monitor the work of employees or to monitor attendance. Neither is the system used as an investigative tool for purposes other than investigating physical security incidents such as thefts or unauthorised access. It is only in exceptional circumstances that the images may be transferred to investigatory bodies in the framework of a formal disciplinary or criminal investigation.

## 4.4 Ad hoc surveillance foreseen

At present the Agency does not foresee *ad hoc* surveillance operations which would need special planning (Guidelines, Section 3.5).

## 4.5 Webcams

There are no webcams located in the Agency premises.

## 4.6 Special categories of data collected

The Agency does not collect special categories of data.

# 5. Legal basis of the video-surveillance

The use of our video-surveillance system is necessary for the management and functioning of the Agency (for the security and access control purpose described in Section 4.2 above). Therefore, the Agency has a lawful ground for the video-surveillance (Guidelines, Section 5.2). A more detailed and specific legal basis for the video-surveillance is provided in these Video-Surveillance Rules (paragraph 1.2 above). These Rules form part of the Security Rules adopted by the Agency.

# 6. Access and disclosure of information

## 6.1 In-house security staff and outsourced security-guards

Recorded video footage is accessible to the in-house security staff only. Live video footage is also accessible to security guards on duty. These security guards work for a licensed security company, contracted by the Agency. A copy of the contract with this security company is included in Attachment 4.



## 6.2 Access rights

These Rules for Video-Surveillance specify who has access to the video-surveillance footage and/or the technical architecture of the video-surveillance system, for what purpose and what those access rights consist of. In particular, the right to:

- view the footage real-time,
- view the recorded footage, or
- copy,
- download,
- delete, or
- alter any footage.

## 6.3 Data protection training

All personnel with access rights, including the security guards, are given data protection training. Training is provided for each new member of the staff and periodic workshops on data protection compliance issues are carried out at least once every two years for all staff with access rights.

## 6.4 Confidentiality undertakings

After the training each staff member with access rights also signs a confidentiality undertaking. This undertaking was also signed by the contracted security company. Templates of these confidentiality undertakings are attached as Attachment 5.

## 6.5 Transfers and disclosures of information

All transfers and disclosures of information outside the responsible personnel are documented and subject to a rigorous assessment of the necessity of such transfer and the compatibility of the purposes of the transfer with the initial security and access control purpose of the processing. The register of retention and transfers is included in Attachment 6. The DPO of the Agency is consulted in each case thereof. No access is given to management or human resources.

Local police may be given access if needed to investigate or prosecute criminal offences. The the Agency Security Officer shall be responsible to give authorisation to provide information and/or images to the local police. Every occasion of a request and provided authorisation shall be documented based on the template Disclosure Request Form, Attachment 8 to these Rules.

Under exceptional circumstances, access may also be given to

- the European Anti-fraud Office ("OLAF") in the framework of an investigation carried out by OLAF,
- the Commission's Investigation and Disciplinary Office ("IDOC") in the framework of a disciplinary investigation, under the rules set forth in Annex IX of the Staff Regulations of Officials of the European Communities, or
- those carrying out a formal internal investigation or disciplinary procedure within the Agency, provided that it can be reasonably expected that the transfers may help investigation or prosecution of a sufficiently serious disciplinary offence or a criminal offence.

# 7. Protection and safeguarding of the information

In order to protect the security of the video-surveillance system, including personal data, a number of technical and organisational measures have been put in place.

Among others, the following measures are taken:

- Secure premises, protected by physical security measures, host the servers storing the images recorded; network firewalls protect the logic perimeter of the IT infrastructure and the main computer systems holding the data are security hardened.

- Administrative measures include the obligation of all contractors' personnel having access to the system (including those maintaining the equipment and the systems) to have relevant security documentation under national law.
- All staff (external and internal) with access rights signs confidentiality undertakings.
- Access rights to users are granted to only those resources which are strictly necessary to carry out their jobs.
- Only the system administrator specifically appointed by the controller for this purpose is able to grant, alter or annul any access rights of any persons. Any provision, alteration or annulment of access rights is made pursuant to the criteria established in the Agency rules and mechanisms in place.

## 8. Storing of the data

The procedure for retention of images is in accordance with Regulation (EC) No 45/2001. The retention time complies with the applicable Portuguese legislation which requires data storage of 30 days, after which images are deleted automatically.

If any image needs to be stored to further investigate or evidence a security incident, they may be retained as necessary. Their retention is rigorously documented and the need for retention is periodically reviewed. A copy of the register of retention and transfers is included in Attachment 6.

The system is also monitored live by the security guard in the downstairs building reception 24 hours a day.

## 9. Provision of information to the public

### 9.1 Multi-layer approach

The Agency provides information to the public about the video-surveillance in an effective and comprehensive manner. It presents a multi-layer approach, which consists of a combination of the following methods:

- on-the-spot notices to alert the public to the fact that monitoring takes place and provide them with essential information about the processing,
- These Video-Surveillance Rules are made available on Agency's intranet and also on its internet sites. For purposes of confidentiality and protection of the legitimate interests certain attachments are not publicly disclosed. ;
- Print-outs of these Video-Surveillance Rules are also available from Agency's Security Officer upon request;
- A phone number and an email address are provided for further enquiries (general the Agency contact points).

The Agency also provides on-the-spot notice adjacent to the areas monitored. Notices are placed near the main entrance, the elevator entrances and in the parking garage within the Agency parking area and at the entry to the parking garage.

The Agency's on-the-spot data protection notice is included as Attachment 7.

### 9.2 Specific individual notice

In addition, individuals must also be given individual notice if they were identified on camera (for example, by security staff in a security investigation) provided that one or more of the following conditions also apply:

- their identity is noted in any files/records,
- the video recording is used against the individual,
- kept beyond the regular retention period,
- transferred outside the A.2 unit, or
- if the identity of the individual is disclosed to anyone else but the Security Officer.

Provision of notice may sometimes be delayed temporarily, for example, if it is necessary for the prevention, investigation, detection and prosecution of criminal offences. The Agency DPO is consulted in all such cases to ensure that the individual's rights are respected



## 10. Verification, modification or deletion of information

Members of the public have the right to access their personal data the Agency holds on them and to correct and complete such data. Any request for access, rectification, blocking and/or erasing of personal data should be directed to the Agency Security Officer. The Security Officer may also be contacted in case of any other questions relating to the processing of personal data via the video surveillance system.

Whenever possible, the Security Officer responds to an enquiry in substance within 15 calendar days. If this is not possible, the applicant is informed of the next steps and the reason for the delay within 15 days. Even in the most complex of cases access must be granted or a final reasoned response must be provided rejecting the request within three months at the latest. The Unit A.2 shall make its best efforts to respond earlier, especially if the applicant establishes the urgency of the request.

If specifically requested, a viewing of the images may be arranged or the applicant may obtain a copy of the recorded images on a DVD or other media. In case of such a request, the applicants must indicate their identity beyond doubt (e.g. they should bring identity cards when attending the viewing) and, whenever possible, also designate the date, time, location and circumstances when they were caught on cameras. They shall also provide a recent photograph of themselves that allows the security staff to identify them from the images reviewed.

At this time, the Agency does not charge applicants for requesting a viewing or a copy of their recorded images. However, the Agency reserves the right to charge a reasonable amount in case the number of such access requests increases.

An access request may be refused when an exemption under Article 20(1) of Regulation 45/2001 applies in a specific case. For example, when restricting access may be necessary to safeguard the investigation of a criminal offence. A restriction may also be necessary to protect the rights and freedoms of others, for example, when unrelated people are also present on the images, and it is not possible to acquire their consent to the disclosure of their personal data or to use image-editing to remedy the lack of consent.

## 11. Right of recourse

Every individual has the right of recourse to the European Data Protection Supervisor ([edps@edps.europa.eu](mailto:edps@edps.europa.eu)) if they consider that their rights under Regulation 45/2001 have been infringed as a result of the processing of their personal data by the Agency. Before doing so, it is recommended that individuals first try to obtain recourse by contacting:

- the Security Officer ([security@emsa.europa.eu](mailto:security@emsa.europa.eu)) and/or
- the Data Protection Officer of the Agency.

Staff members may also request a review from their appointing authority under Article 90 of the Staff Regulation.

## 12. Final provision

EMSA Guidelines on Video surveillance in of 29th June 2010 are replaced by these Rules.

## 13. List of Attachments

- Attachment 1 - the audit report and periodic reviews (*not publicly available*)
- Attachment 2 - map with the locations of the cameras (*not publicly available*)
- Attachment 3 –the technical specifications for the cameras and for the video-surveillance system as a whole (including any software and hardware) (*not publicly available*)



- Attachment 4 - the contract with the outsourced security company (*not publicly available*)
- Attachment 5 - template of the confidentiality undertaking;
- Attachment 6 - the template of register of retention and transfers;
- Attachment 7 - the Agency's on-the-spot data protection notice ;
- Attachment 8 - the Disclosure Request Form.

**European Maritime Safety Agency**





Praça Europa 4  
1249-206 Lisbon, Portugal  
Tel +351 21 1209 200  
Fax +351 21 1209 210  
[emsa.europa.eu](http://emsa.europa.eu)

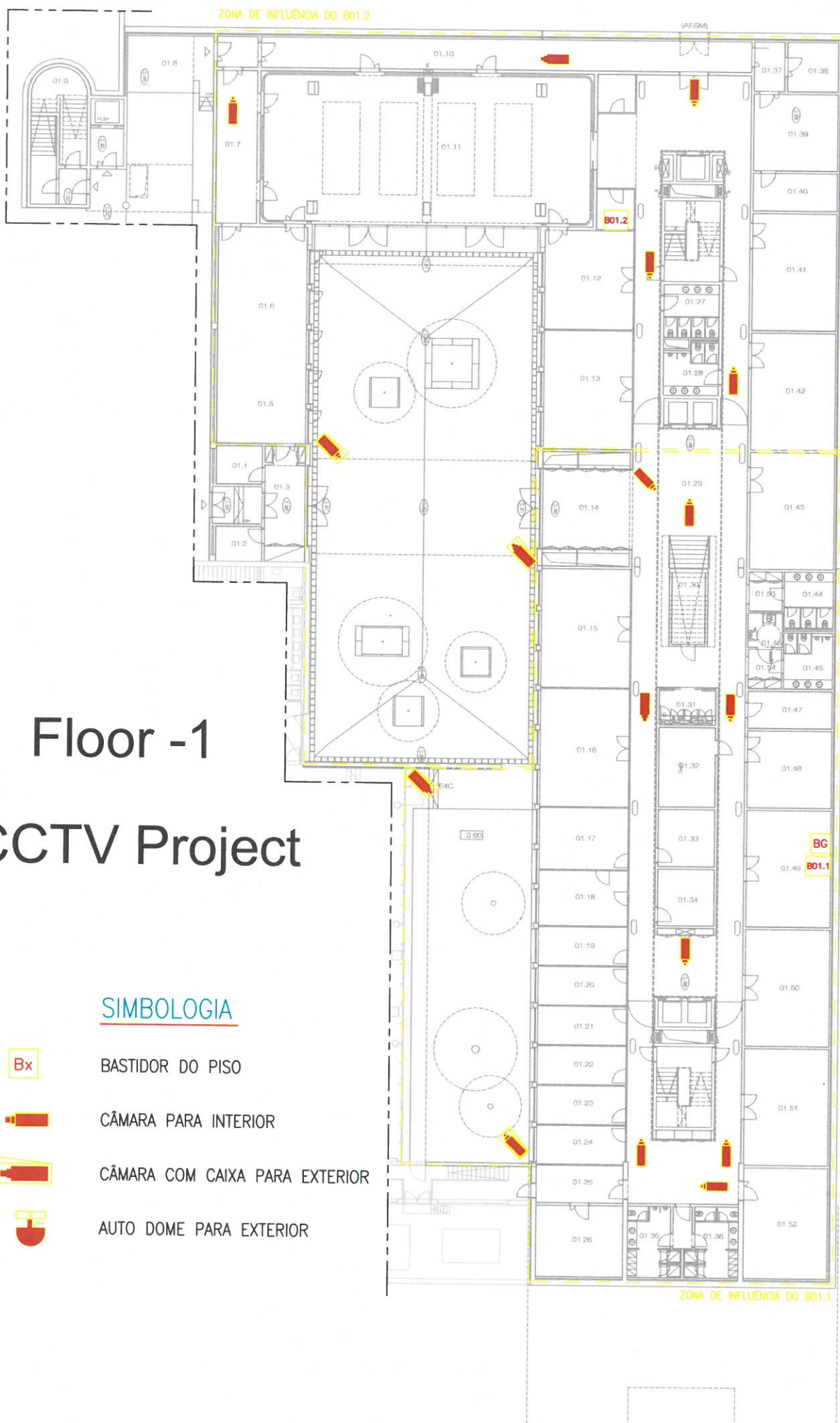


# Floor -1

## CCTV Project

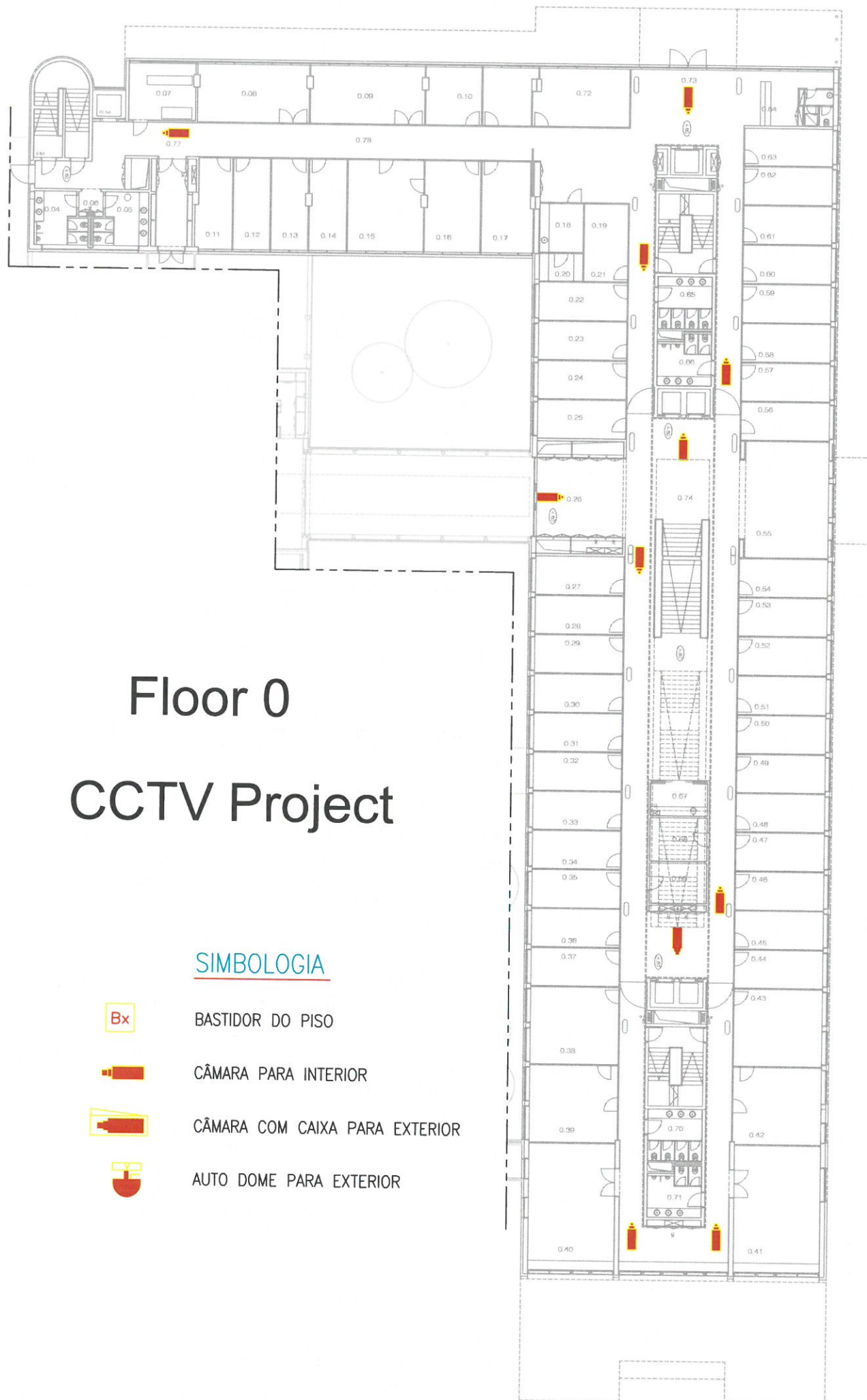
### SIMBOLOGIA

-  BASTIDOR DO PISO
-  CÂMARA PARA INTERIOR
-  CÂMARA COM CAIXA PARA EXTERIOR
-  AUTO DOME PARA EXTERIOR



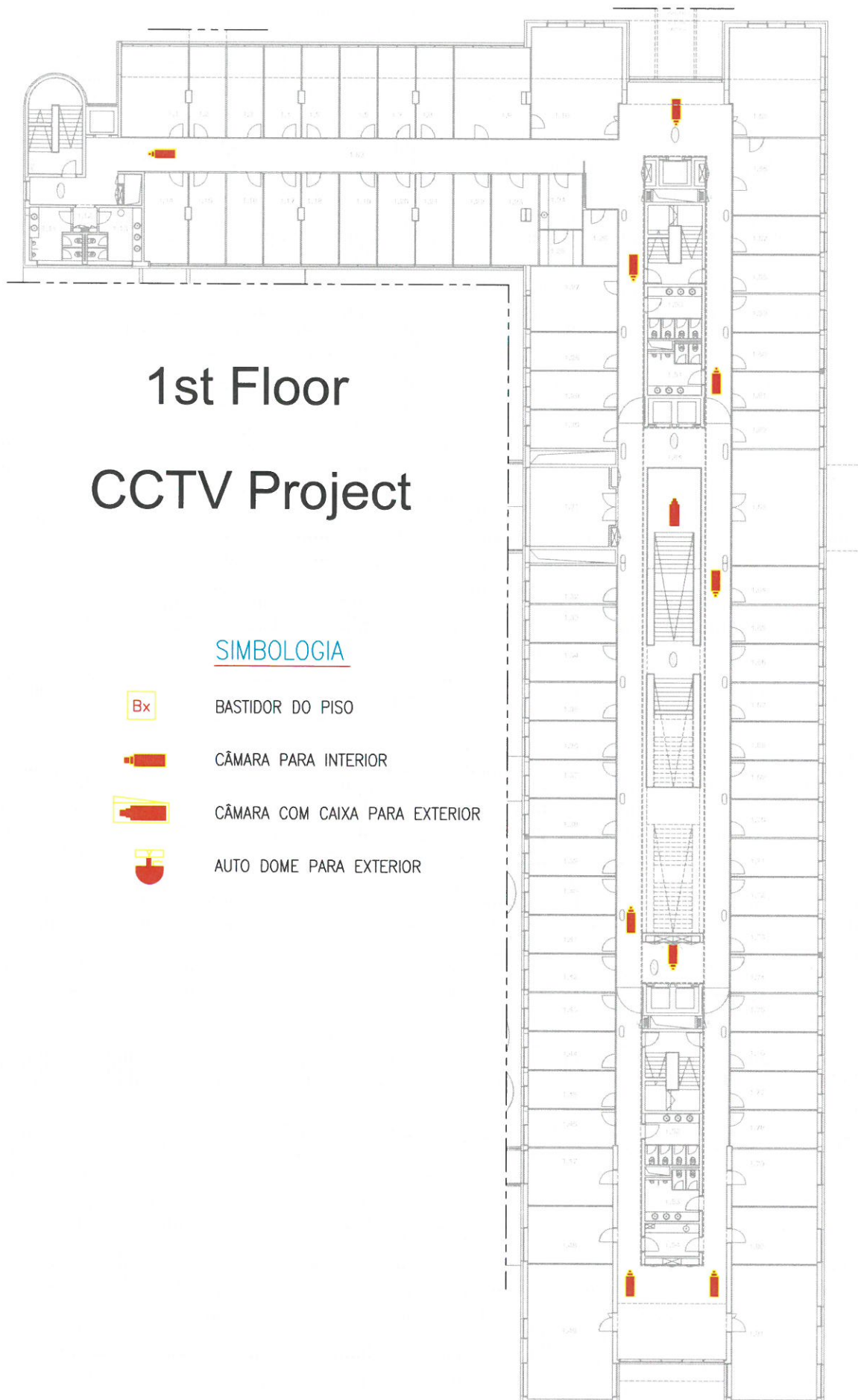




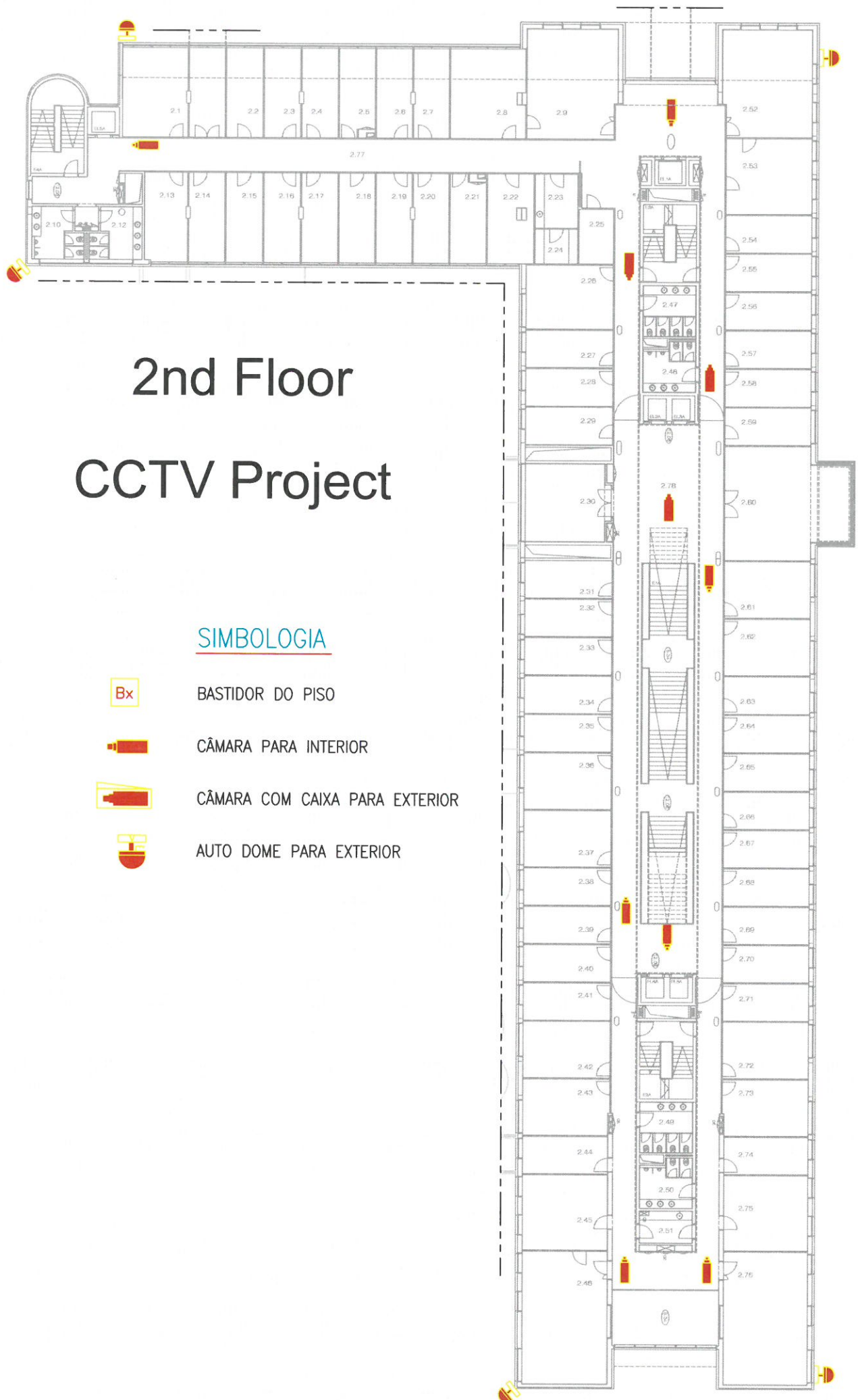












# 2nd Floor

## CCTV Project

### SIMBOLOGIA

Bx

BASTIDOR DO PISO



CÂMARA PARA INTERIOR



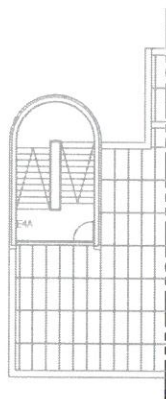
CÂMARA COM CAIXA PARA EXTERIOR



AUTO DOME PARA EXTERIOR







# 3rd Floor CCTV Project

## SIMBOLOGIA



BASTIDOR DO PISO



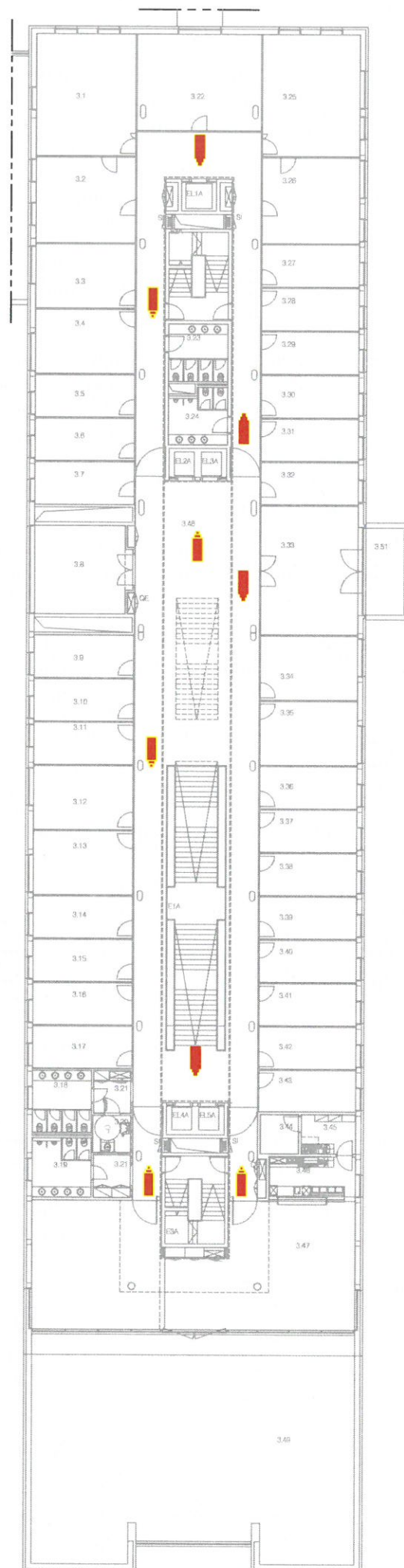
CÂMARA PARA INTERIOR



CÂMARA COM CAIXA PARA EXTERIOR



AUTO DOME PARA EXTERIOR







Video | DiBos IP Recorder Software (EMEA/APR)

# DiBos IP Recorder Software (EMEA/APR)

[www.boschsecurity.com](http://www.boschsecurity.com)



**BOSCH**

Invented for life



- ▶ Recording Software for Bosch MPEG-4 and JPEG video sources
- ▶ Connect up to 32 IP video sources
- ▶ View/record video at CIF/2CIF/4CIF/Megapixel resolution
- ▶ Connect to other DiBos recorders
- ▶ Web-browser remote access and viewing

DiBos IP Recorder Software uses Bosch's proven state of the art digital recording and communications technology and takes video surveillance to a new level. It is an integral part of overall security solutions for a wide range of applications – including banks, large retailers, railway stations, airports, city centers, industrial facilities, and office buildings.

With DiBos customers can retrieve vital images and share information faster than ever before. They can better assess critical situations and take action immediately. Whether they are on site or at a remote network location, authorized personnel have quick, convenient access to information so they can operate more effectively and efficiently.

DiBos supports live viewing and recording at resolutions up to 2048 x 1536 pixels (3 Megapixel) and frame rates up to 30/25 ips. Users can connect up to 32 IP video sources. This includes support for Bosch MPEG-4 IP cameras (Dinion IP, FlexiDome IP and AutoDome IP), Bosch MPEG-4 video encoders (VideoJet and VIP X Series), Bosch Megapixel cameras, as well as JPEG images from numerous IP camera manufacturers.

The system offers advanced features for viewing and a very high flexibility in recording and image access. The real power of DiBos is fast, convenient accessibility to images and information. If required, accessibility to images and information is possible round the clock

and everywhere all over the world. Communication and access to DiBos is possible via private or public networks. For these purposes the system can be connected to a variety of peripheral devices and systems.

The unique, scalable GUI allows live and recorded images from multiple remote systems to be viewed from a single PC or another DiBos. With this powerful tool, security managers can monitor and supervise various locations simultaneously.

Cameras and viewing modes can be programmed or selected manually. Each camera offers in-window pan/tilt/zoom functionality from local or remote facilities. Images are displayed with date/time, location, camera name and status of connected devices such as detectors and sensors. DiBos can be programmed to respond to specific situations and events automatically. Minimal human intervention is necessary.

In response to alarms, the system can be programmed to transmit images or messages to security personnel or the security control center.

Playback is easy thanks to familiar search and navigation functions in a tree structure. Images can be accessed locally or remotely via a company network or the Internet. The customer can select multiple different views from up to 30 cameras. Fast, powerful image search functions eliminate time consuming



manual searches. Functions include search for image changes (Smart Motion Search), search for criteria such as camera number and recording date/time. To ensure high security, all access is controlled by user authorization. Profiles are assigned by the system administrator. Events, such as login, logoff, status changes, image transmission, and system shutdown are stored in a database. Video authentication is built in to ensure that DiBos images are not altered in any way.

Various storage devices – such as external disk arrays, RAID and NAS devices, and external disk drives – may be used for export and backup of images.

The configuration wizard makes installation quick and easy. DiBos can connect to Bosch alarm panels and Allegiant matrices via the RS232 serial port.

### Technical Specifications

Maximum recording rate (analog and IP)	50 Mbit per second
Recording resolution (IP inputs - Bosch IP devices)	PAL: 704 x 576 (4CIF/D1), 704 x 288 (2CIF), 464 x 576 (2/3 D1), 352 x 576 (1/2 D1), 352 x 288 (CIF), 176 x 144 (QCIF) NTSC: 704 x 480 (4CIF/D1), 704 x 240 (2CIF), 464 x 480 (2/3 D1), 352 x 480 (1/2 D1), 352 x 240 (CIF), 176 x 120 (QCIF)
Recording rates per channel (video inputs IP)	PAL: 0.5; 1; 2; 3; 4; 5; 6; 8; 12.5; 25 ips NTSC: 0.5; 1; 2; 3; 5; 6; 7.5; 10; 15; 30 ips
Supported single channel encoders Bosch VideoJet Series and Bosch VIP Series	VideoJet 10S, VideoJet 1000 VideoJet X10 VIP X1, VIP 10
Supported multi channel encoders Bosch VideoJet Series and Bosch VIP Series	VideoJet 8004, VideoJet 8004A VideoJet 8008, VideoJet 8008A VideoJet X20, VideoJet X40 VIP X2, VIP X2A, VIP X1600
Supported Bosch IP cameras	Dinion IP, AutoDome IP, FlexiDome IP, Megapixel IP
JPEG protocol	JPEG image request via HTTP
Supported JPEG cameras from other manufacturers	IP cameras from Axis, Sony and Mobotix. For further information please contact Bosch Security Systems

### Minimum requirements for computer with DiBos Receiver Software/IP Recorder Software (in brackets recommended requirements)

Operating system	Windows XP Professional, 32-bit versions;
------------------	---

	Windows Vista, 32-bit versions
CPU	Pentium 4, 3 GHz with Hyper Threading, (Core 2 Duo CPU)
RAM	1024 MB (2048 MB)
VGA card	32-Bit color depth (DirectX 9 Hardware Support, no shared memory)
Recording partition	Dedicated partition for recording
Network adapter	1000 Base-T, Gbit

Windows XP and Windows Vista are registered trademarks of Microsoft Corporation

### Ordering Information

#### DB SR 042 IP Recorder Software

DiBos IP recorder software, recording of up to 4 IP devices.

Order number **DBSR042**

#### DB SR 082 IP Recorder Software

DiBos IP recorder software, recording of up to 8 IP devices.

Order number **DBSR082**

#### DB SR 162 IP Recorder Software

DiBos IP recorder software, recording of up to 16 IP devices.

Order number **DBSR162**

#### DB SR 322 IP Recorder Software

DiBos IP recorder software, recording of up to 32 IP devices (not expandable).

Order number **DBSR322**

### Software Options

#### DB SR 002-B DiBos 8 Receiver SW Burning License

Order number **DBSR002-B**

#### DB SR 042 EXP IP Recorder

DiBos IP expansion, 4 IP devices (maximum 32 IP devices)

Order number **DBSR042EXP**

#### DB SE 016 DiBos ATM POS Bridge License

Software interface via TCP/IP to Bosch ATM/POS bridge.

Order number **DBSE016**

#### DB SE 017 DiBos IP Software License

Software interface via TCP/IP socket connection to IP server providing POS, ATM or other data.

Order number **DBSE017**

## SAFETY PRECAUTIONS

TYPENUMBERS NWC 0445-10P NWC 0445-20P NWC 0445-10P NWC 0445-20P

### Danger

The lightning flash with unswitched symbol, within an equilateral triangle, is intended to alert the user to the presence of unswitched live parts which may be of sufficient magnitude to constitute a risk to persons.

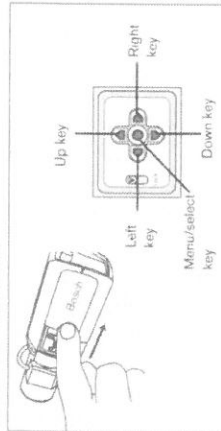
### Warning

The exclamation mark within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (warning) instructions in the literature accompanying the appliance.

### Important Safeguards

- Read these instructions.
- Keep these instructions.
- Comply with all warnings.
- Follow all instructions.
- Do not use this equipment near water.
- Do not use this equipment near dry cloth.
- Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
- Do not install near any heat source such as radiators, heat registers, stoves, or other equipment (including amplifiers) that produce heat.
- Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding-type plug has two blades and a third grounding prong. Both the wide blade and the third prong are provided for safety. If the supplied plug does not fit into your outlet, consult an electrician for advice.
- Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the equipment.
- Only use attachments/accessories specified by the manufacturer.

## Quick set-up menu



Press the menu select key to access the menus or to move to the next or previous menu.

Press the menu/select key for approximately 1.5 seconds to open the Installer menu.

Use the up or down keys to scroll through a menu.

Use the left or right keys to move through options or to set parameters.

When in a menu, quickly pressing the menu/select key twice restores the selected item to its factory default.

To close all menus, select the Exit item and hold down the menu select key until the menu display disappears.

### Defaults

To restore all parameters (including IP address) to the factory defaults, press and hold the Up navigation key for at least 10 seconds and then confirm. Allow a few seconds for the camera to optimize the picture after a made reset.

- Unplug this equipment during lightning storms or when unused for long periods of time.
- Rider all servicing to qualified service personnel. Servicing is required when the equipment has been damaged in any way, such as when power supply cord or plug is damaged, liquid has been spilled or objects have fallen into the equipment, the equipment has been exposed to rain or moisture, does not operate normally, or has been dropped.
- An all-pole mains switch with a contact separation of at least 3mm in each pole shall be incorporated in the electrical installation of the building.

### Warning

To reduce the risk of electric shock, do not remove covers. No user-serviceable parts inside. Refer servicing to qualified service personnel.

### Warning

To reduce the risk of fire or electric shock, this equipment should not be exposed to rain or moisture and objects shall with liquids, such as water, should not be placed on this apparatus.

### Caution

The Low Voltage power supply unit must comply with EN60950-1 (Safety Extra Low Voltage - Limited Power Source) IECEN60950-1 compliant power sources are SELV devices by default.

INSTALLATION MANUAL (full version) is available on enclosed CD-ROM and can be viewed and printed with Acrobat Reader which is also available on enclosed CD-ROM.

## Install menu

Function	Selection	Description
Lens Wizard	Select submenu	Optimize camera/lens combination
Network	Select submenu	Set the camera IP address
Exit		Exit the menu

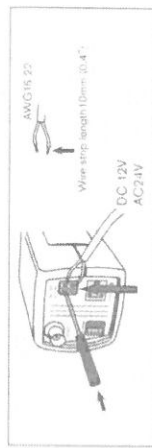
### Install lens wizard submenu

Function	Selection	Description
Lens Type	Auto, Manual, DC Irs, Video	Auto detects the type of lens used
Detected		If Auto, the detected lens type is shown
Set Back Focus Now		Select to force lens to its maximum opening
Set LVL (Video iris lenses only)		Set indicator to the center by adjusting the level potentiometer on the lens
Exit		Return to the Install menu

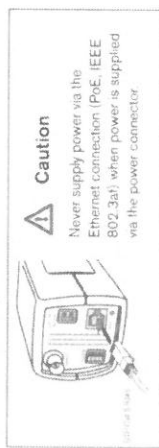
### Install IP address submenu

Function	Selection	Description
IP Address		Enter an IP address for the camera (default 192.168.0.1)
Subnet Mask		Enter subnet mask (default 255.255.0.0)
Gateway		Enter a Gateway address
Exit		Return to the Install menu

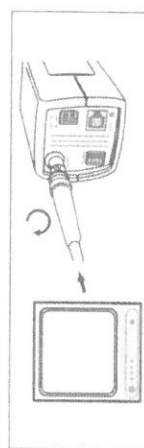
## Power



## Network (and power)



## Video service monitor



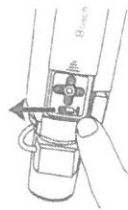
## Back focus adjustment

When back focusing vari focus lenses, adjust to obtain a sharp picture in both wide-angle and tele positions for both far and near focus.

When back focusing zoom lenses, ensure the object of interest remains in focus throughout the entire zoom range of the lens.

### Adjustment procedure Manual-iris Lens

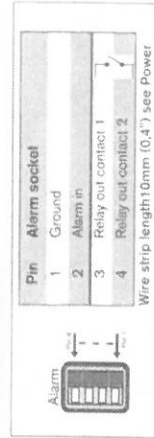
- Unlock the back focus locking button



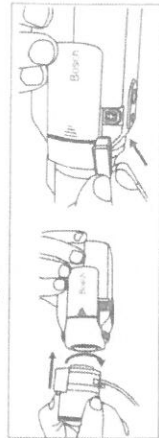
- Adjust the lens to the maximum lens opening.
- Turn the back focus adjustment as required.



## Alarm connector



## Lens mounting

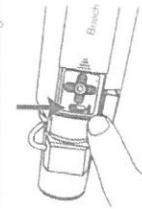


The camera accepts CS mount lenses with a lens protrusion of up to 5mm. CS mount lenses are mounted using a lens adapter ring.

## Mounting the camera



## Lock the back focus locking button



### Adjustment procedure DC-iris Lens

- Unlock the back focus locking button.
- Access the Lens Wizard menu.
- Set Back Focus Now is highlighted in the menu.
- Turn the back focus adjustment as required.
- Lock the back focus locking button.
- Exit the menu.

### Adjustment procedure Video-iris Lens

- Unlock the back focus locking button.
- Access the Lens Wizard menu.
- Set Back Focus Now is highlighted in the menu.
- Turn the back focus adjustment as required.
- Lock the back focus locking button.
- Select Set LVL in the menu, the Level bar appears.
- Point the camera at the scene it will be mostly viewing.
- Adjust the level potentiometer located on the lens until the Level bar is in the central position.
- Exit the menu.







From	Product Management	Telephone	Nuremberg
STVC/PRM		+49 911 93456 0	18.09.2006

## Release Letter

Product:	<b><i>Configuration Manager</i></b>
Version:	<b><i>1.51.0009</i></b>

This letter contains latest information about the above mentioned software.

### 1. General

Configuration Manager is a generic configuration tool for all Bosch IP Network Video Products, both software modules and hardware devices.

It is used for licensing and configuration of the various products where it is included on the product CD.

Make sure to always use the latest released version.

### 2. Added Features

- VIP X1/X2/XD, VIP X1600 and Dinion IP cameras with firmware 2.0 are supported.
- Configuration and licensing of IVMD 1.0, available with firmware version 2.0 for the products VIP X1, VIP X2, VIP X1600 and Dinion IP are supported.
- Access may be password protected.



From	Product Management	Telephone	Nuremberg
STVC/PRM		+49 911 93456 0	18.09.2006

### 3. Restrictions; Known Issues

- Audio functions in VIP X and VideoJet 800x with firmware 1.5 are not supported.
- VGA settings for VIP XD are not available in this Configuration Manager version. Must be set up via the product's web site.
- For Display Stamping the setting of XY position is not possible. Must be set up via the product's web site.

### 4. System Requirements

Hardware	Personal Computer
CPU	Pentium IV, 2.0 GHz or better
RAM	min. 256 MB
OS	Windows XP Home/XP Professional, Windows 2003 Server
Graphic Card	NVIDIA GeForce 6600, NVIDIA Quadro FX 1400, ATI RADEON X600/X800 or better
Ethernet Card	100 Mbps
Sound Card	Recommended
Software	DirectX 9.0c
Free Memory (Installation)	45 MB (.NET environment, Configuration Manager)



## Attachment 5

### Confidentiality undertaking

#### [Template]

I, [insert name and title of signatory of this declaration], the undersigned,

☐ in my own name (for a natural person)

or

☐ representative of (for a request made on behalf of a legal person)

[insert name in full of the legal person, official address in full]

Being provided with access to the video-surveillance footage and/or the technical architecture of the video-surveillance system established by EMSA, hereby confirm:

- the rights to view the footage real-time, view the recorded footage, or copy, download, delete, or alter any footage acquired by the aforementioned video-surveillance system are provided to me within the framework of my function and duties which I perform for the Agency.
- I am [and the entity that I represent and the staff proposed are] not subject to a conflict of interest in the context of the aforementioned functions and duties; a conflict of interest could arise in particular as a result of economic interests, political or national affinities, family or emotional ties, or any other relevant connection or shared interest;
- that I will inform EMSA, without delay, of any situation constituting a conflict of interest or which could give rise to a conflict of interest;
- that I will not communicate any confidential information that is revealed to me or that I have discovered. I will not make any adverse use of information given to me.
- that I will keep the footage file entrusted to me confidential. I will not disclose such a file nor the information contained in the file to any party. I will use the footage only for the purposes of my immediate function and duties in accordance with the provisions of Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data and EMSA Video-Surveillance Rules

- that I [the organisation that I represent and its staff] have not sought and will not seek, have not attempted and will not attempt to obtain, and have not accepted and will not accept, any advantage, financial or in kind, from any party whatsoever, where such advantage constitutes an illegal practice or involves corruption, either directly or indirectly, inasmuch as it is an incentive or reward relating to the access rights to the video-surveillance footage and/or the technical architecture of the video-surveillance system established by EMSA.
- that I am aware that EMSA reserves the right to check this information, and I realise the possible consequences that may arise from any false declaration.

Full name and signature:

Date:

## Attachment 6

### Register of retention and transfers

Number	Date and Time	Entity requesting the disclosure	Brief description	Justification	Deadline for EMSA copy to be destroyed	Authorised by	Signature





## Attachment 7

### EMSA on-the-spot data protection notice





## Attachment 8

### Disclosure Request Form

<b>Event description</b>		
Date and Time:	Location:	Report Reference:
Event type		
Theft <input type="checkbox"/> Accident <input type="checkbox"/> Violence/Physical aggression <input type="checkbox"/> Other <input type="checkbox"/> (describe)		
Brief description		
Entity requesting the disclosure		
Police <input type="checkbox"/> SIS <input type="checkbox"/> Other <input type="checkbox"/>		
Justification		
EMSA copy to be destroyed in [days]:		
Authorised by:		
Signature:		
Requested by:		
Date	Name	Signature



