Security policy for Video-surveillance
TABLE OF CONTENTS

1. SCOPE ................................................................................................................................. 34
2. STAKEHOLDERS .................................................................................................................. 34
3. CCTV SYSTEM POLICY STATEMENTS ............................................................................. 34
4. AVAILABILITY MEASURES IMPLEMENTED ........................................................................ 45
5. OLAF CCTV APPLICATIVE ACCESS RIGHTS .................................................................... 45
1. **Scope**

This document describes the measures that have been put in place in order to protect the CCTV system from unauthorized access.

The CCTV system at OLAF is composed of 51 video cameras, 5 Cisco network switches and 1 server.

The video cameras monitor all the accesses to

- the OLAF perimeter (main lifts hall, the exits of the OLAF lift in the extension at +1, +3 and +4 floors, the fences in the emergency staircases, the SASs)
- the network technical rooms called Local Répartiteur d'Etage (LRE's),
- the computer rooms,
- the corridors giving access to the archive rooms at -4 floor and protected by an intrusion detection system at the 3rd floor.

The system and the data protection issues are described in the notification DPO-137 and the in opinion from the EDPS case 2007-634.

2. **Stakeholders**

The following stakeholders play a role in this policy:

- **OLAF LSO**: the Local Security Officer(s), or deputy(ies) nominated by OLAF as foreseen in Commission Decision 844/2001.

- **OLAF Security Management Team**: OLAF officials, security cleared, in charge of network and servers’ management and operation of OLAF physical access control system.

- **OLAF Security Permanency**: OLAF staff nominated to organise a 24/7 security permanency for OLAF.

3. **CCTV System Policy Statements**

(1) All equipment in the solution - network switches, video server and video cameras must be managed by the OLAF Security Management team.

(2) All equipment in the solution network switches, video server and video cameras must be password protected. A password management system must be in place for safekeeping these passwords.

(3) Rooms where equipment for the CCTV solution is installed must be protected and monitored. The technical rooms (LRE) must be protected by the access control system and the CCTV systems itself. The server room must have an intrusion detection system in addition to the normal controls.

(4) Servers in the computer room must be installed in special security computer racks with an independent access control system. All accesses to the computer racks are monitored and
logged. Access to the rack hosting the CCTV system must be limited to the OLAF security management team.

(5) The OLAF Physical Security Management Team is in charge of the rack access management system. The system is described and notified to the DPO in OLAF DPO-84).

(6) The physical security network must be logically isolated and monitored; the equipment for this is exclusively managed by the OLAF Physical Security Management Team. The firewall management solution is described and notified to the DPO in OLAF DPO-83.

(7) The CCTV and physical access control servers must be stand alone servers that cannot be part of an overall logical grouping of computers. The servers must be managed by the OLAF Security Management Team only.

(8) The live video is accessible to the OLAF Security Permanency, LSO and the OLAF security management team.

(9) The right to access recorded footage is described in the document “Physical Access Control System: Access Policy to Security Events” and controlled by the LSO.

(10) For maintenance purposes, the video footage and live video are accessible to the OLAF Physical Security Management Team.

(11) All persons dealing with these systems must be vetted by their national authorities.

(12) External personnel should not have access to the recorded data.

(13) Any breach or suspicion of a security breach must be reported to the LSO and the DPO.

4. AVAILABILITY MEASURES IMPLEMENTED

(1) The video server and physical security network equipments is considered sensitive. The system is therefore powered by two independent power sources.

(2) The video server's operating system and data must be protected against hard drive failures. A RAID configuration has been put in place in accordance with the RAID configuration guideline used in the Commission.

(3) In case of system crash, the OLAF team should be able to rebuild a new working video server in a short time. The system is therefore backed up on a daily basis. The system is backed up to disks in order to avoid tape loss or theft.

5. OLAF CCTV APPLICATIVE ACCESS RIGHTS
<table>
<thead>
<tr>
<th>Role</th>
<th>User</th>
<th>Global user rights</th>
<th>User rights for cameras</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>View</td>
<td>Live</td>
<td>Browse</td>
</tr>
<tr>
<td>OLAF Permanency</td>
<td>Angelo NICOSIA</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Edouard DEPUTTER</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>LSO</td>
<td>Joël HUBIN</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>OLAF Physical Security</td>
<td>Torben FORSLUND</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Management</td>
<td>Franco PECORARO</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Kristof rumors</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Luc SAPART</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Browse = ability to review recorded videos
Setup = ability to add/remove/modify views
PTZ = Ability to use the Remote Client's or Smart Client's navigation features for PTZ (Pan/Tilt/Zoom) cameras. (only the digital zoom is available)
Output = ability to remotely control external device from the camera (not used)
Events = ability to automatically trigger actions (not used)
Database export = ability to generate and export evidence in database format
Sequences = Ability to use the Sequences feature for browsing images from a selected camera
Smart search = Ability to use the Smart Client's Smart Search feature, with which users are able to search for motion in one or more selected areas of images from the selected camera