

DISPATCHER PROCEDURAL PROTOCOL

ARTIFICIAL INTELLIGENCE-BASED PERIMETER PROTECTION

1. Receiving the Alarm

1.1. In the event of fence-proximate movement or an intrusion attempt detected by artificial intelligence, the incident management software (MONITORINGBOOK PRO) notifies the dispatcher with an alarm.

1.2. The alarm contains the following information:

- Timestamp (date, exact time)
- Camera ID / location
- Type of alarm event (e.g., motion detection, suspected climbing, etc.)
- Video recording and/or live image from the time of the alarm



2. Event Identification and Visual Verification

2.1. The dispatcher **opens the live image and/or replayable recording related to the alarm within** the incident management software interface.

2.2. Examination criteria:

- Is a human figure, suspicious movement, or action visible?
- Was there an intentional approach to the fence?
- Can an animal or other factor causing a false alarm be detected?

2.3. The dispatcher **validates the alarm**:

-  **Genuine alarm** (e.g., intrusion attempt, suspicious person)
-  **False alarm** (e.g., bird, animal, moving tree branch, shadow, weather)

3. Measures in Case of a Genuine Alarm

3.1. After validating the alarm, the dispatcher **logs the following** in the incident management system:

- “Suspected genuine intrusion”
- A brief description of the recorded event
- Time of initiation of the intervention

3.2. Immediate response:

- The dispatcher switches on the floodlights in the camera zone concerned (if lighting control is integrated)
- Through the outdoor **loudspeaker system, the dispatcher addresses the intruder**, e.g.:

“Attention! You have entered a guarded area! Your activity has been recorded. Leave the area immediately!”

- Repeat if necessary, with increasing firmness, and include identifying details for visual confirmation of the intruder, e.g.: “You in the red T-shirt with the blue cap.”

3.3. Further measures:

- If the intruder does not leave or poses a threat:
- Notify **the on-site security response unit**
- Notify the **police** (112), provided the client has authorized this and site protection requires it

4. Event Documentation

4.1. Following the intervention, the dispatcher sets the alarm status to “**closed**” in the incident management system.

4.2. The following data are recorded:

- Type of event (genuine/false)
- Time and type of intervention (e.g., light, loudspeaker, external notification)
- Behavior of the intruder (e.g., left, returned, stopped)
- Affected camera zone
- Final comment and closing statement

4.3. Archiving video recordings:

- Due to GDPR, the incident management system does not archive video material belonging to the alarm, only saves the access path (link) to the bookmarked recording

stored on the network video system, in accordance with the regulations, on the intervention worksheet.

5. Handling a False Alarm

5.1. If the dispatcher determines that no unauthorized intrusion has occurred:

- Log the false alarm in the incident management system:
 - “False alarm – reason: [animal/moving vegetation/weather, etc.]”
 - Close the event
-

6. Feedback and System Maintenance

6.1. Regular feedback (e.g., based on a weekly report) is exchanged between the system operator and the remote monitoring service provider on the number and causes of false alarms.

6.2. If false alarms are frequent in a given zone, recalibration of the analytics or adjustment of the camera position may be necessary.



Closing Statement

- The dispatcher handles all events strictly in accordance with GDPR and data protection policies.
- Use of loudspeaker warnings and lighting devices is permitted exclusively in case of a genuine alarm.