

PROCESSING REGULATIONS REGARDING VIDEO SURVEILLANCE AT BACHEM AG

1. Scope

These regulations define guidelines for the lawful use and operation of image and video surveillance systems (visual surveillance using optical-electronic systems, hereinafter collectively referred to as "video surveillance systems") at BACHEM AG, Bubendorf.

2. Purpose

2.1. Video surveillance serves the following purposes:

- Protection of visitors and employees
- Protection of infrastructure and property
- Preservation of evidence
- Right to keep out trespassers
- Prevention and solving of criminal offences
- Operation of the parking management system
- Visitor management

3. Proportionality

3.1. Image and video recordings with video surveillance systems may only be collected, processed and used if they are suitable and necessary for achieving the purpose pursued in accordance with the above section 2 and if there are no indications that the legitimate interests of the individuals concerned outweigh them.

3.2. Surveillance of third-party properties and public spaces is not permitted.

4. Responsibility

4.1. The management is responsible for the use of video surveillance systems in accordance with these regulations.

4.2. The Group Leader Electrotechnics at Bachem AG (hereinafter referred to as "the Representative") ensures that the installation and operation of video surveillance systems complies with the law and the provisions of these regulations.

4.3. The Representative may further specify the installation and operation of video surveillance systems in compliance with the provisions of these regulations.

4.4. The Representative may, in compliance with legal requirements, entrust third parties with the installation and operation of video surveillance systems. These third parties must be contractually obliged to comply with the statutory requirements and the provisions of these regulations.

5. Scope and type of video surveillance

- 5.1. Video surveillance is generally carried out 24 hours a day, 7 days a week. It is carried out both actively (real-time monitoring in the form of live images) and passively (video recording with evaluation in the event of an incident). Video recordings are only be evaluated if there is reasonable suspicion and in accordance with the provisions of these regulations. If necessary, an evaluation can also be carried out as part of the operation of the parking management system and the digital visitor management system.
- 5.2. Real-time monitoring of employees' work activities is only permitted if it is necessary for their protection. Such real-time monitoring is limited to the minimum necessary and is not recorded. The employees affected will be transparently informed in advance and consulted. Such personalised real-time monitoring can take place in clean rooms in particular.
- 5.3. There is no further video surveillance of employees.

6. Access

- 6.1. The images from real-time surveillance are available live to security and reception employees.
- 6.2. Video recordings may only be viewed in the event of an incident, only by the Representative and only with the consent of their supervisor. An event is defined as any occurrence in which the assertion of civil or criminal claims must be examined.
- 6.3. Information from the parking management system (in particular the number plates of vehicles entering and leaving) is also accessible to technical service employees at any time, insofar as this is necessary to ensure operations.
- 6.4. The Representative is permitted to evaluate information from the visitor management system (in particular information about the data subject) insofar as this is necessary to ensure identity verification and access management and to achieve the purposes set out in section 2 above.
- 6.5. Access must be verifiably documented (except for the purpose of operating the car park management system).
- 6.6. If the data collected in the context of video surveillance is assigned to a specific person, that person must be informed in advance about the data processing, but at the latest as soon as the purpose defined in the preceding section 2 permits.
- 6.7. If a suspected case involves a person entrusted with video surveillance, or if that person appears to be biased, the management must determine who will carry out the inspection.

7. Use of video recordings

- 7.1. Video recordings may only be used to assert civil or criminal claims.
- 7.2. Any copies or extracts of the video recordings required for this purpose may only be made at the request of the Representative and with the approval of their supervisor. They must be documented.

8. Storage and data deletion

- 8.1. Video recordings will be stored for a maximum of 35 days. Thereafter, they will be erased or overwritten automatically.
- 8.2. Personal data collected as part of visitor management must be deleted no later than one year after the last visit. Visitor photos extracted from identity documents must be deleted immediately after checkout. Photos taken during check-in must be deleted no later than 30 days after the last visit.
- 8.3. The right to longer storage within the scope of the above section 7 remains reserved. In such cases, image and video recordings may be stored for as long as this is required in order to assert claims under civil or criminal law.

9. Security measures

- 9.1. The Representative must take and document appropriate technical and organisational measures to protect the video recordings and video surveillance systems from access by unauthorised third parties.
- 9.2. The following security measures shall be implemented to the extent possible:
 - Encrypted storage
 - Remote storage
 - Access to servers with password protection
 - Access to IT rooms via an access control system
 - Remote access only possible with VPN
 - Logging of monitoring times (logs are stored for 1 year and then automatically deleted)
 - Access to log data must be authorised and documented by the Representative.
 - Privacy filters
 - Pixelation
 - Masking bar
- 9.3. Any transfer of image and video recordings to authorised third parties may only be carried out in encrypted form. Any further distribution or publication of video recordings is not permitted.

10. Information

- 10.1. A clearly visible notice must be displayed on every video surveillance system to indicate that video surveillance is in operation.
- 10.2. In addition to the information board, at least the following information must also be made easily accessible by means of appropriate measures:
 - Responsible body for video surveillance
 - Purpose of video surveillance
 - Storage period
 - Rights of affected persons and contact point for affected persons
 - Categories of recipients to whom the video recordings may be disclosed
 - When disclosing personal data abroad: Recipient countries and any guarantees given or exemptions claimed

10.3. The locations of the video surveillance systems must be documented.

10.4. The information provided to the persons concerned within the scope of visitor management is provided separately and in conjunction with a declaration of consent.

11. Integral parts of these regulations

11.1. The following documents, in their current versions, form an integral part of these regulations:

- Information sheet for video security systems
- Information sheet for cyber security systems
- Configuration report
- Operating log for video surveillance systems
- Area overview CCTV Bachem AG
- Building surveillance (indoor CCTV) Bachem AG (as per detailed plans)



12. Commencement of the Regulations

These regulations enter into force on 01.12.2025. It replaces the regulations dated 01.04.2024.

Place/Date: Bubendorf Dec 22, 2025

Frank Dettner, Site Manager BBU

DocuSigned by:
Frank Dettner
CF09EECC9FDE43F...

Sven Burger, Site Security Manager

DocuSigned by:
Sven Burger
C8A8414A80604B1...

Matthias Schindler, Group Leader Electrotechnics

DocuSigned by:
Matthias Schindler
AFBE91B2E570414...