Appendix 3, to the tender for the video solution, IT Security Requirements, ISO/IEC 27002 – Supplier Compliance

It is essential that the solution complies with satisfactory IT security requirements, as the solution may process GDPR related data, se appendix 5.

The supplier must provide a clear account of the current level of compliance within the IT security domain, including which security requirements are applicable, which have been partially implemented, and which have been fully implemented.

The supplier shall be subject to audit in relation to cf. Section 7 of the agreement.

The IT security requirements do not form part of the weighted evaluation criteria in the tender process. However, the document must be duly completed and submitted as part of the tender material.

Questions for Suppliers

Response scale (default):
0 = Not implemented
1 = Partially implemented / Inadequately documented
2 = Fully implemented and documented or not applicable (note why)
Responses shall be supported by documentation upon request.

The following security topics will form part of the contractual requirements.

Topic	Score (0, 1 or 2)
Management and Organization	
1. Do you have an approved IT security policy?	
2. Are roles and responsibilities for IT security formally described?	
3. Are risk assessments conducted regularly?	
4. Is IT security integrated into the software development and deployment process?	
Supplier and Subcontractor Management	
5. Do you have procedures for evaluating subcontractors?	
6. Are IT security requirements imposed on subcontractors?	
7. Is the security level of subcontractors monitored continuously?	
8. Do you inform customers about important changes in the supply chain?	
Classification and Data Handling	
9. Do you classify data and information?	
10. Do you have guidelines for the handling of confidential data?	
11. Is customer data secured according to the classification agreed?	
Access Control	
12. Is the principle of least privilege applied?	
13. Is MFA used for administrative or critical access?	

14. Are there rules for creating and deleting user accesses?	
15. Are regular access reviews carried out?	
Technical Security	
16. Are systems protected by malware protection?	
17. Is patch management used?	
18. Are security-relevant events logged, monitored, and retained for an appropriate period?	
19. Are production, test, and development environments separated and appropriately protected?	
20. Are vulnerability scans or penetration tests performed?	
Cryptography and Backup	
21. Is data encrypted in transit?	
22. Is data encrypted at rest?	
23. Is data backed up regularly, encrypted and tested?	
Event Handling	
24. Do you have documented incident handling procedures?	
25. Are there fixed deadlines for customer notification?	
26. Is root-cause analysis performed after serious incidents?	
Continuity and Readiness	
27. Do you have a BCP?	
28. Do you have a disaster recovery plan?	
29. Are these tested regularly?	
30. Are RTO (max downtime after an outage) and RPO (max amount of data tolerated after an outage – measured in time since the last backup) described?	
Compliance and audit	
31. Do you comply with data protection legislation and other relevant laws?	
32. Are data processing agreements in place (if relevant)?	
33. Can you document compliance (ISO 27001, ISAE 3000 or similar)?	
34. Do you accept customer or third-party audit?	
The partnership ends	
35. Do you ensure the deletion or return of customer data at the end of the partnership?	
36. Is all access closed when the agreement expires?	
Total score	

Critical minimum requirements

The total score must be at least 60.

These 9 questions should score greater than or equal to 1:

- 1 (security policy)
- 12-14 (access control)
- 21-22 (encryption)
- 24-25 (event handling)
- 31 (data protection law/data processing agreement)

If the provider does not meet the minimum requirements, it will be considered a non-approved provider, regardless of the overall score.

The supplier must be prepared to ensure that all 36 controls achieve a level 2 rating within one year of the agreement entering into force.

2. Mapping to ISO/IEC 27002:2022

Question	ISO 27002-control
1–4	5.1, 5.2, 5.4, 5.7
5–8	5.19–5.23
9–11	5.12, 5.13
12–15	5.15–5.18
16–20	8.7, 8.8, 8.16, 8.20
21–23	8.24–8.28
24–26	5.24–5.26
27–30	5.29–5.30
31–34	5.31–5.36
35–36	5.11, 5.20