Vendor Security Requirements

Document Level	4
Version	1.2
Date	18.01.2023
Approved By	NRK CSO
Document Owner	NRK CISO
Classification	NRK Public
Scope	Vendors

1. Introduction

1.1	Description	Vendors are expected to maintain the minimum information security requirements. This document is based on ISO 27001 controls and EBU R143 *Cybersecurity Recommendation for Media Vendors' Systems, Software & Services*.
1.2	Scope	Section 2 must be completed by vendors that process, access, hold or transmit data for NRK. The same applies to vendors that have access to NRK's physical sites. Both section 2 and 3 must be completed by vendors that providing software, middleware, hardware, platforms or other systems/components, which are integrated with NRK's information technology environment.

2. Organisational Requirements

Please respond to the following requirements with either Y=Yes, No=N or N/A=Not applicable and provide an explanation for each answer.

Requirements	Y	N	N/A	Explanation
2.1 Security Governance The vendor has a security policy that is regularly evaluated and updated.				
2.2 Risk Management The vendor identifies risks associated with its services and provides mitigating measures.				
2.3 Data Transfer NRK's data is stored and processed only within the European Economic Area (EEA).				
2.4 Personnel Security Background checks, such as identity and credential verification, are conducted on all personnel that are involved in the assignment.				
2.5 Supply Chain The vendor takes responsibility for the security of its supply chain.				

3. Technical Requirements

Please respond to the following requirements with either Y=Yes, No=N or N/A=Not applicable and provide an explanation for each answer.

Requirements	Y	N	N/A	Explanation
3.1 Vulnerability Management The vendor has a process in place to identify, track and address vulnerabilities.				
3.2 Security Testing The vendor conducts regular technical security analysis, such as penetration or vulnerability testing.				
3.3 Incident Response Management The vendor has an incident response procedure implemented.				
3.4 Incident Reporting The vendor has a procedure in place to notify NRK of data breaches or major incidents.				
3.5 Data Recovery The vendor has appropriate backup procedures and recovery plans in place and has tested them.				
3.6 Access Control The vendor ensures that their services support role-based access control and Azure AD SSO.				
3.7 Data Encryption The vendor has an established method of encrypting sensitive data when necessary, both for data at rest and in transit.				
3.8 Change Management The vendor ensures that changes of the service are controlled through a formal documented process.				
3.9 Separation of Environments The vendor ensures that production and test environments are kept separate.				
3.10 Segregation of Customer Data The vendor has an appropriate segregation of customer data in place, if stored in a multi-tenanted environment.				
3.11 Physical Security The vendor has access control and physical security of its premises.				