SUPPLIER SECURITY REQUIREMENTS

Version	0.9
Issued	14.09.2022
Classification	NRK Public

Contents

1 INTRODUCTION

This document establishes minimum security standard required for suppliers to meet appropriate organisational and technical measures, to help ensure the confidentiality, integrity, and accessibility of NRK's data and information technology environment.

All requirements are based on ISO/IEC 27001:2018 *Information Security Management Systems*, and *Cybersecurity for Media Vendor Systems, Software & Services*, which is a standard (R 143, 2020) developed by the European Broadcasting Union (EBU).

2 SCOPE

The scope of this document includes any suppliers that process or have access to NRK's data. This includes, but not limited to:

- Suppliers that process, access, hold or transmit data for NRK.
- Suppliers that have access to NRK's physical sites or IT systems.

Suppliers must demonstrate compliance with each of the requirements below in Section 3 *Organisational measures*.

Suppliers providing software, middleware, hardware, platforms, or other systems and/or components integrated with, or connected to, NRK's information technology environment, must also comply with Sections 4 *Technical Measures* of this document.

3 ORGANISATIONAL MEASURES

#	Description	Fully meets	Partially meets	Don´t support	Comment
1	**Security Governance** The supplier must have a security policy that is regularly evaluated and updated.				
2	**Risk Management** The supplier must identify risks that are caused by its services and provide mitigating measures.				
3	**Personnel Security** The supplier must ensure that all personnel who will have access to any of NRK's sites or data, are screened prior to engagement.				
4	**Supply Chain** The supplier must ensure that their subcontractors is compliant with the measures in this document.				

4 TECHNICAL MEASURES

#	Description	Fully meets	Partially meets	Don´t support	Comment
5	**Vulnerability Management** The supplier must ensure that a vulnerability management process is in place to keep track of identified vulnerabilities and patches that may fix them.				
6	**Security Testing** The supplier must perform regular technical security analysis such as penetration or vulnerability testing of the service.				
7	**Incident Management** The supplier must have an incident response procedure implemented. To collect security events, technical controls must be established.				
8	**Incident Reporting** The supplier must have a documented process in place to notify NRK when a security incident occurs.				
9	**Disaster Recovery** The supplier must have appropriate backup procedures implemented, and recovery plans that are tested.				
10	**Access Control** The supplier must ensure that their services support role-based access control and NRK's Single Sign On (SSO).				
11	**Data Encryption** The suppliers must have an established method of encrypting sensitive data in storage and in transit following industry best practice.				
12	**Change Management** The supplier must ensure that changes of the services are controlled and authorised through a formal, documented process.				
13	**Separation of Environments** The supplier must ensure that production, test, and development environments are kept separate.				
14	**Segregation of Customer Data**				

	The supplier must have in place appropriate segregation of customer data where it is being stored or processed in a multi-tenanted environment.				
15	**Physical Security** The supplier must have established access control and necessary physical security of its premises.				
16	**Personal Data** The supplier must disclose if personal data is being processed outside of the EEA.				