REQUIREMENTS FOR SAAS IT-SYSTEMS USED AT NRK

V.3.0.5

Instructions to suppliers of equipment or software affected by the requirements listed below:

If you comply with the requirements relevant to your delivery to NRK, you should only quote “Read and understood” at the bottom of this list of section 2. NRK will then regard this as an acceptance of the relevant requirements or at least as a confirmation that the Supplier will comply with the requirements at the time of delivery

Content

Summary

This document contains business goals, principles and requirements for the architecture domains:

- Data
- Applications (Business)
- Integrations
- Network

The business goals, guidelines and requirements are valid both for internal (NRK) and external IT service providers and developers.

The document uses the following notation and hierarchy:

Abbreviation	Requirement type	Note
Hard	Hard requirement	A hard requirement should be followed. If it is broken it should be clearly documented and approved in NRK
Requirement	Normal requirement	A requirement should be followed. It is possible to break as long as it is documented. Unlike a hard requirement it does not need any approval.
Guideline	Guideline for that NRK considers a best practice.	A guideline is a rule of what NRK want. However, it is not needed documented or having any decision to break. It might get rewarded in different processes or acquisition or development if they are followed.

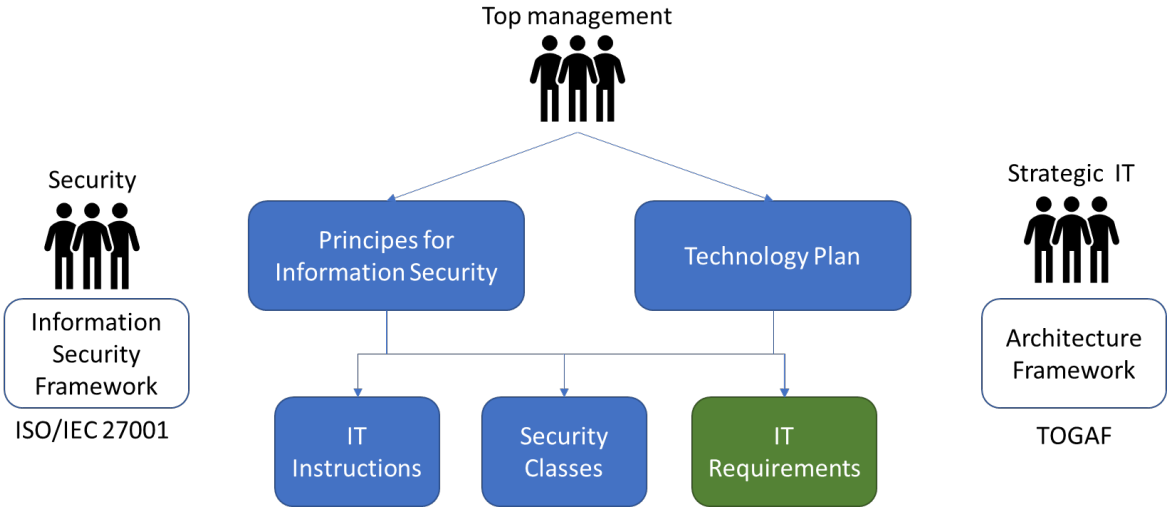
Purpose of this document

The purpose of this document is to present the requirements from IT. It has been compiled a list of requirements for the IT domain. In this document it is condensed to contain the relevant areas. This document should ensure:

1. Present the IT-Requirements in a consistent, precise and understandable document.
2. Governance of IT-Requirements should be simplified.
3. Consistent requirements towards vendors and other parties.
4. Requirements are not left out.
5. Differentiation in how important the requirements are. How important / strict are they in NRK.

Business goals and principles from NRKs Strategies

In 2016 and 2017 NRK had a technology plan project. This project resulted in the technology plan document, containing the strategic directions, business goals and principles for the technology domain.



From these two documents, three documents have been derived:

- **IT instructions**
  Instructions for employees and others working for NRK, using and producing NRK information assets
- **Security Classes**
  Sheet with instructions and requirements for security and architecture based on classification of the three core elements of security:
  - Confidentiality
    Data must not made available or disclosed to unauthorized individuals, entities, or processes
  - Integrity
    The consistency, accuracy, and trustworthiness of data over its entire life cycle
  - Availability
    Information must be available when it is needed
- **IT Requirements**
  This document, deriving the principles into the different architecture domains

Strategic directions, business goals and principles

Our current technology strategy (currently Technology Plan, 2017) contains the following strategic directions to **reduce complexity** and **increase efficiency**:

- Concentrate resources and expertise within content production and publishing
- Increase cooperation
- Focus on analysis and insight
- Operate flexibly and cost-effectively
- Increase conversion capacity and reduce investment horizon
- Compliance (GDPR, Data handling agreements and similar)

Software as a Service (SaaS)

Storage of information on the cloud is restricted by laws and regulations in both EU and in Norway. Being on the cloud the information is outside of the facilities of NRK and as such has different security aspect. This means that there are requirements from law and NRK that need to be in place.

- Agreement on how/where data is stored
- Exit strategy if service is shut down or changing vendor
- Predictable storage location and regulations
- Predictable security including information security, network security and similar
- Predictable handling of scalability and failure of the service

Information security requirements

The following principles and rules as based on ISO/IEC 27001 and the European Broadcasting Union's (EBU) standards for vendor management. They are meant to ensure that NRK's information assets are secured in a systematic and satisfactory manner.

Req #	ReqType	Requirement	Vendor reply
1.1.24	Principal	Information security must be part of the entire IT project	
1.1.26	Principal	All IT services shall be secured following a risk-based approach, ensuring the necessary confidentiality, integrity and availability in architecture, solutions, governance and procedures.	
1.1.163	Rule	All vendors of IT services shall have a documented Cyber Security Policy (or set of policies) in place that are aligned to or certified against recognized security standards and frameworks and approved by senior management.	
1.1.164	Rule	All vendors of IT services regularly perform enterprise risk assessments and specific risk assessments for the provided IT service.	
1.1.166	Rule	If requested by NRK, vendors of IT services shall be prepared to make available any relevant documentation, such as external audits, certifications, security incident information, and results from regularly performed risk assessments, vulnerability and penetration tests.	

2.1.167	Rule	Appropriate segregation of customer data is in place where it is being stored or processed in a multi-tenanted environment.	
1.1.168	Rule	Cloud services allow default passwords to be changed for built-in accounts; do not have global hidden accounts (such as maintenance accounts) with the same password for all product units and customers; and supports implementation of NRK's password policy	
1.1.169	Rule	All vendors of IT services have a documented incident response and crisis management process/procedure in place, which is regularly reviewed and kept up to date.	
1.1.170	Rule	All vendors of IT services have a business continuity and/or disaster recovery plan in place, which is tested, reviewed at regular intervals, and includes immediate notification to NRK.	
1.1.28	Rule	NRK must for all cloud services have a data processing agreement	
1.1.171	Rule	Cloud services must support enhanced authentication mechanisms in internet-facing interfaces, such as Multi-Factor Authentication (MFA).	
1.1.29	Rule	All cloud services containing confidential or strictly confidential data should adhere to Cloud Security Alliance (CSA) Cloud Control Matrix and must adhere to the Norwegian policies for data storage location	
1.1.30	Rule	Shared users shall only be permitted if required for business or operational purposes, and shall be approved by NRK security and documented	
1.1.31	Rule	All IT services user accesses must be managed by NRK's solutions for identity and access management. That is integrate with NRK Azure AD or on-prem AD (ADFS)	
1.1.32	Rule	Allocation and use of privileged administrator access shall be limited and controlled through a formal	

		authorization process where access shall only be granted after approval by the IT service owner	
1.1.34	Rule	The clock in all NRK's IT infrastructure must be synchronized with an NTP server, preferably with NRK's central NTP server	
1.1.37	Rule	IT services must be developed in accordance with NRK's guidelines for safe development	
1.1.39	Rule	Test data must be carefully selected and protected. Use of data from production containing personally identifiable information or other confidential information for test purposes should be avoided	
1.1.40	Rule	The environments for development, testing and production should be separate to reduce the risks of unauthorized access to or changes in the production environment	
7.1.172	Rule	Communications must be encrypted when transmitted across networks so as to protect against eavesdropping of network traffic by unauthorized users. The following protocols should be used: • HTTPS • SFTP • FTPS • SCP • SSHv2 • SNMPv3 The following protocols should be avoided: • HTTP • FTP • TELNET • SNMPv1 • SNMPv2 • SSHv1 • VNC	

1.1.173	Rule	All vendors of IT services apply the same level of security control assessment procedure to its own suppliers.	

Data domain

Req #	ReqType	Requirements
2.2.52	Rule	All data protocols, types and formats must support UTF-8 character set . This means the API must support UTF-8 but data in the system mush handle special characters like Sami alphabet.
2.1.46	Principal	Shared IDs shall only be permitted if required for business or operational reasons, and shall be approved by NRK security and documented
2.2.48	Principal	When registering data, the quality and availability must be on a level good enough for all use and reuse in associated workflows and systems
2.2.51	Principal	All primary keys should be unique and not contain any functional logic
2.2.54	Rule	All data storage, transport and management must be compliant to Norwegian policies (GDPR, Norwegian laws and legislations)
2.2.59	Rule	All codes shall have an id, name and description. Only ids should be referenced.
2.2.61	Rule	Creation and change of data shall be time stamped and by whom to ensure traceability
4.5.65	Principal	Configuration data should have right quality and relevant for life cycle management, part of the system documentation and be versioned
5.6.66	Principal	Unstructured data should be avoided (if possible)

Application domain (business applications)

Req #	ReqType	Requirement
6.2.79	Principal	Application sourcing should be scalable in functionality and in costs
6.2.80	Principal	Applications should be easy to operate and maintain
6.2.81	Principal	Applications should be able to utilize marked leading, standard and de facto middleware and infrastructure solutions and services
6.3.83	Principal	Browser based applications (web/thin) are preferred
6.3.84	Principal	Thick client applications should support thin workstations through application or desktop virtualization

6.3.88	Principal	The installation and upgrades/updates/patches should run silent (as a background process)
6.3.89	Principal	Local user accounts should not be used. Service accounts, which systems depend upon, should all reside in Active Directory. All user accounts should be able to use strong passwords in accordance to Microsoft's recommendation
6.3.91	Principal	Programs running on client computers should be able to run on a standard model that meets hardware requirements set by the software/hardware manufacturer
6.3.92	Principal	MS Office 2013/2016/365 and is the preferred communication and office software on NRK's workstations. Applications should be compatible with these versions and later versions whenever NRK decides to upgrade company wide
6.3.93	Principal	Web applications must at least support the following web-browsers: o Chrome (last 3 builds)
6.3.96	Principal	Applications must comply with NRK security zone model
6.5.100	Principal	Applications must be updated/patched to always be supported
6.5.102	Principal	Applications must be downloaded from Google Play or Appstore.
6.8.106	Rule	All SaaS containing confidential or strictly confidential data must adhere to CSA Cloud Control Matrix

Integration domain

Req #	ReqType	Requirement
7.2.111	Principal	All integrations should use common integration standards and platforms
7.2.113	Principal	Business data mapping between different data models should be available for business users to manage and correct
7.2.114	Principal	We should adapt to standard integration technologies and not have overlapping technologies for the same task/ techniques

Network

Relevant business goals and principles from the technology plan and information security for the network domain

Req #	ReqType	Requirement
10.2.161	Rule	SQL and other database protocols are only allowed from cleared security zones
10.2.162	Rule	All network infrastructure and applications must support IPv4 and IPv6.