# Content

# Summary

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

- Data
- Applications (Business)
- Integrations
- Middleware
- Infrastructure
- 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:

B **Business goals**
This is a state or capability according to strategic direction(s)

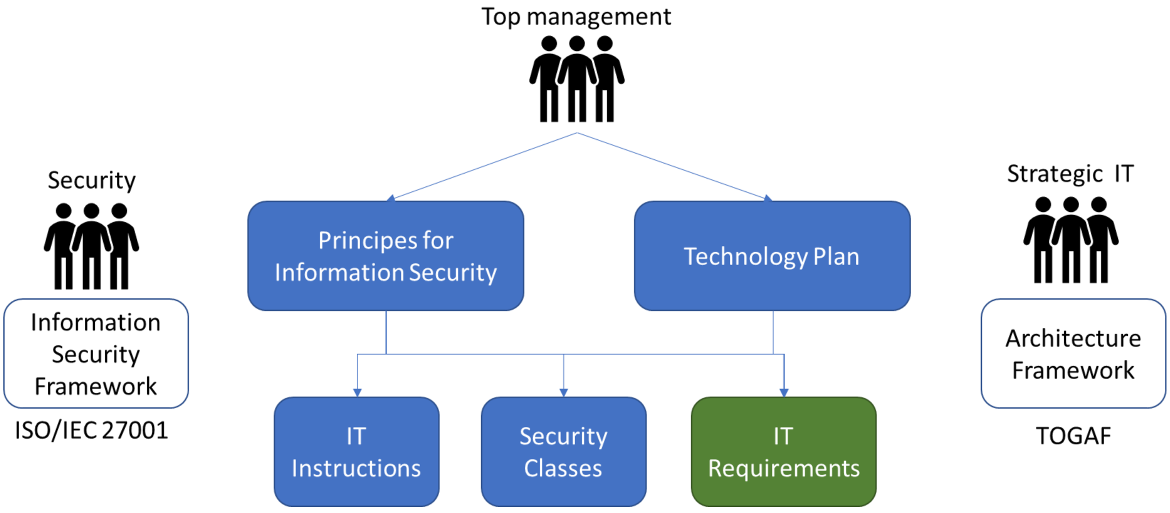
P **Principle**
This is a direction necessary to reach the business goal(s)

R **Requirement**
This is a hard requirement to ensure compliance with the business goal(s)

# Business goals and principles from NRK top management

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

In 2018 the department for security and readiness, together with the new Chief Information Security Officer (CISO), developed the document "Principles for information security". This document is also approved by NRK top management.



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

The "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

These strategic directions have been derived to the following business goals (future state and capabilities):

B NRK has an efficient and less complex system portfolio as possible

B NRK's systems use standardized technology that is open and integrable

B NRK's technology facilitates coordinated, efficient and innovative interaction in NRK and with external parties

B NRK applies automation and artificial intelligence to streamline and improve the entire business

B NRK concentrates resources on core business and is capable to outsource services to external actors

B NRK's architecture and control mechanisms support the efficient and secure sharing of information between internal systems, cloud services and external partners

B NRK has APIs (Application Programming Interface) exposed for all external usage of NRK services

B NRK has secure access to all relevant services, regardless of location and platform, and meets the requirements for information security and privacy

The business goals have been derived to the following principles for sourcing:

P Anything that is not NRK's core business should be considered for outsourcing

P Outsource whole areas or domains

P Purchasing of services is preferred. Rent is preferred before purchase of standard solution

P Self-development should only be chosen when it gives NRK a clear differentiated position, and there are no commercially solutions available

P All sourcing should be scalable in functionality and in costs

The business goals have also been derived to the following principles for governance:

P All investments should result in increased value to the audience, directly or indirectly

P Solutions should be good enough to meet defined needs. High-end solutions should only be used when providing significantly increased value to the audience

P Technology procurement should emphasize user perspectives and have user involvement in the development / acquisition of systems

P Efficiency and standardization of workflows should always be considered as part of technology decisions and acquisitions

P We should adapt to standard systems, use the systems fully and not have overlapping systems for the same task

P All integrations should use common integration standards and platforms

P Open standards and open source code should be evaluated when choosing technology

P All new systems within production and publishing must support Sami character set

All business goals and guidelines are derived into local principles and requirements for each architecture domain.

## Information security principles

The "Principles for information security" (2018), based on ISO/IEC 27001, contain the following principles to ensure NRK's information assets are secured in a systematic and satisfactory manner:

P Information security goals shall be included in the design for all IT change or transition projects

P Risk and security assessment must be done early in every IT project to identify necessary classifications and actions to reduce the risks. Risk reducing actions must be included in the project deliveries

P Information security must be part of all IT project phases

P All IT services must have an owner, be classified and be in NRK architecture repository

P All IT services shall be secured according to NRK security classes. This includes architecture, solutions, governance and procedures to ensure confidentiality, integrity and availability

P NRK security shall be involved in the procurement process of all cloud services

P NRK must for all cloud services have a data processing agreement

P All cloud services containing confidential or strictly confidential data must adhere to Cloud Security Alliance (CSA) Cloud Control Matrix in addition to the Norwegian policies for data storage location

P Shared users shall only be permitted if required for business or operational reasons, and shall be approved by NRK security and documented

P All IT services user accesses must be managed by NRK's solution for identity and access management (IAM)

P 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

P IT service owners must ensure updated and available operational documentation, including life cycle management, configuration, backup, dependencies to processes, data and other IT services, incident management, operational contact persons, monitoring and procedures to restart

P The clock in all NRK's IT infrastructure must be synchronized with NRK's central NTP server

P NRK shall organize all major platform upgrades of operating systems and middleware in projects and ensure that notification of changes is given in time to allow appropriate tests and assessments to take place before implementation

P All infrastructure and middleware must be configured according to NRK's Safe Configuration Guide

P IT services must be developed in accordance with NRK's guidelines for safe development

P All IT services developed by NRK shall undergo safety testing before they are deployed into production to reveal any vulnerabilities and error configuration

P 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

P The environments for development, testing and production should be separate to reduce the risks of unauthorized access to or changes in the production environment

## Data domain

Relevant high-level business goals and principles from the technology plan and information security for the data domain:

B Information is registered once, reused in associated workflows, and is available to those who need it

B NRK's system architecture and control mechanisms support the efficient and secure sharing of information between internal systems, cloud services and external partners

B NRK has secure access to all relevant services, regardless of location and platform, and meets the requirements for information security and privacy

P Open standards and open source code should be evaluated when choosing technology

P All new systems within production and publishing must support Sami character set

P Shared IDs shall only be permitted if required for business or operational reasons, and shall be approved by NRK security and documented

P 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

Derived principles and requirements for the data domain:

P When registering data, the quality and availability must be on a level good enough for all use and reuse in associated workflows and systems

P Data should have a defined source and the source should be source for all

P Data structures and models should be according to open, de facto standards and best practices

P All primary keys should be unique and not contain any functional logic

R All data protocols, types and formats must support UTF-8 character set

R All data must be classified, managed and secured according to NRK security classes

R All data storage, transport and management must be compliant to Norwegian policies

R All data must be documented, and quality breaches should be corrected

R All use of data must be well documented, including all processes and systems using them

R All primary keys should be random or sequential generated

R Additional nick names/codes, with functional logic, should be used when humans are involved.

R All codes shall have an id, name and description. Only ids should be referenced.

R All relevant primary keys should follow the content/transactions down the whole value chain (necessary to ensure quality, and insight and analytics across the value chain)

R Creation and change of data shall be time stamped and by whom to ensure traceability

### Content data and transactions

P Content metadata for content planning, production, distribution and publishing should be according to the EBU Class Conceptual Data Model (EBU CCDM)

### Master and reference data

P Master data should have right quality and availability for all workflows and systems using them

P All master data should have an owner responsible for quality and life cycle management

### Configuration data

P Configuration data should have right quality and relevant for life cycle management, part of the system documentation and be versioned

### Unstructured data (empty)

P Unstructured data should be avoided (if possible)

## Application domain (business applications)

### General

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

B NRK has an efficient and less complex system portfolio as possible

B NRK's systems use standardized technology that is open and integrable

B NRK concentrates resources on core business and is capable to outsource services to external actors

P We should adapt to standard systems, use the systems fully and not have overlapping systems for the same task

P Open standards and open source code should be evaluated when choosing technology (when no standard solution is available or adequate)

P IT services must be developed in accordance with NRK's guidelines for safe development

Derived guidelines and requirements for the application domain:

P Applications should be secured according to the data sensitivity, integrity and service availability (NRK system security classification matrix)

P Accesses to applications should be controlled by the IAM-solution

P Select SaaS when that is an option

P Applications should be able to be delivered in the cloud if SaaS is not an option

P Applications should preferable be installed/packaged as a container over a service running on a VM

P Applications should be developed according to DevSecOps (Secure DevOps) aligned with the guidelines and best practices from OWASP (Open Web Application Security Project)

P Application sourcing should be scalable in functionality and in costs

P Applications should be easy to operate and maintain

P Applications should be able to utilize marked leading, standard and de facto middleware and infrastructure solutions and services

P All applications should support UTF-8 character set

## Applications on workstations

P Browser based applications (web/thin) are preferred (easy to manage)

P Thick client applications should support thin workstations through application or desktop virtualization

P Thick client applications handling big sets of data should be able to do this in a separate drive (locally or cloud solution)

P All windows client applications should be programmed in accordance with Microsoft's requirements for Windows client applications, e.g.:

- Users should not need administrative privileges to run any application
- Applications should be installed under Program Files
- Applications should be programmed to run on our workstation requirements
- Applications should be updated/patched to always be supported

~~P~~ Thick client applications should be able to be distributed to client computers using industry standard management service or software

~~P~~ The installation and upgrades/updates/patches should run silent (as a background process)

P 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

P Domain authentication is preferably done using Kerberos. More modern authentication methods such as OAuth 2.0 is an option

P Programs running on client computers should be able to run on a standard model that meets hardware requirements set by the software/hardware manufacturer

P 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

P Web applications must support the following web-browsers:

- Chrome (last 3 builds)

P Thick client applications must support IPv4 and IPv6.

P Thick client applications must support DNS

P Applications must comply with NRK security zone model

P IT services must be developed in accordance with NRK's guidelines for safe development

### Applications on middleware (empty)

### Applications (apps) on mobiles and tablets

P Applications should be programmed to run on our mobile and tablet requirements

P Applications must be updated/patched to always be supported

P Applications should not require more resources than necessary

P Applications must be downloaded from Google Play or Appstore.

### Applications on servers

P All applications running on servers should be running as services. Programs must not be dependent upon having a specific user logged on to the server.

P Local user accounts must not be used. Service accounts, which systems depend upon, must all reside in Active Directory. All user accounts must be able to use strong passwords.

P Authentication towards the domain is preferably done using Kerberos.

### Software as a Service

R All SaaS containing confidential or strictly confidential data must adhere to CSA Cloud Control Matrix

## Integration domain

### General

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

B NRK has an efficient and less complex system portfolio as possible

B NRK's systems use standardized technology that is open and integrable

B Information is registered once, reused in associated workflows, and is available to those who need it

B NRK has APIs (Application Programming Interface) exposed for all external usage of NRK services

P All integrations should use common integration standards and platforms

Derived principles and requirements for the integration domain:

P Distribution of master data and content meta data should be done from the source system, and not through other systems (except the integration middleware)

P Business data mapping between different data models should be available for business users to manage and correct

P We should adapt to standard integration technologies and not have overlapping technologies for the same task/ techniques

P Integrations should use the best technique and technology for the purpose/use case

## Middleware domain

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

B NRK has an efficient and less complex system portfolio as possible

B NRK's systems use standardized technology that is open and integratable

B NRK's technology facilitates coordinated, efficient and innovative interaction in NRK and with external

Derived principles and requirements for the integration domain:

R All middleware must comply with NRK security zone model

### Middleware on workstations

R Oracle client version 11

The same requirements apply here as those listed under applications running on workstations.

### Middleware on mobiles and tablets

The same requirements as applications running on mobiles and tablets.

### Middleware in cloud

P Cloud middleware is preferred over internal

P Managed databases should be used including PostgreSql, MySQL, Microsoft SQL Server.

### Middleware on servers

R Databases supported at NRK are PostgreSql, MySQL, Microsoft SQL Server. MySQL is an option on Linux servers only.

R Internet servers supported at NRK are Internet Information Server (IIS) and Apache. Apache is an option on Linux servers only.

Else the same requirements as applications running on servers.

### Platform as a Service

R All PaaS containing confidential or strictly confidential data must adhere to CSA Cloud Control Matrix

## Infrastructure domain

### General

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

B NRK has an efficient and less complex system portfolio as possible

B NRK's systems use standardized technology that is open and integratable

B NRK's technology facilitates coordinated, efficient and innovative interaction in NRK and with external

Derived principles and requirements for the infrastructure domain:

R All infrastructure must comply with NRK security zone model

## Workstations

R Operating Systems:
  - Microsoft Windows 10 64-bit (last 3 builds)
  - Latest Mac OS (latest build)

R Operation system language must be Norwegian (preferred) or English

R All workstations must be member of Active Directory domain and/or Azure AD.

R All workstations must run the latest version of NRKs antivirus and malware software (Symantec Endpoint Protection)

R All operating systems must be patched up to date. All systems must accept new patches continuously

R All workstations must run drive encryption:
  - MacOSX filevault 2
  - Windows 10: bitlocker

## Mobiles and tablets

R Operating Systems:
  - IOS (latest version of iOS)
  - Android (latest 3 versions)

R All mobile devices must be a member of NRK's preferred MDM system
  - IOS devices shall be enrolled through the Apple Device enrollment program (DEP)
  - Android devices shall support Android Enterprise or Samsung Knox

## Container technology

P Deployments on NRK Kubernetes expose a healthcheck endpoint according to NRK standard for monitoring

P Deployments on NRK Kubernetes expose a metrics endpoint for monitoring

P Deployments are scaled according to deployment requirements and tuned

P Deployments must be designed to run on multiple hosts

## Servers

R Operating systems:
  - Windows Server 2016
  - Windows Server 2012 R2 (current Microsoft standard)
  - Ubuntu LTS

R OS installations are preferably done by NRK, using standardized installation method and setup. NRK's Windows server installation includes latest versions of .NET, Windows Installer and Internet Explorer. If installation is done by the supplier, NRK must be able to adjust the installation to NRK's specifications.

R All Windows servers are members of an Active Directory domain (function level 2012).

R All Windows servers must run latest version of Microsoft System Center Endpoint Protection.

R All Windows servers are patched up to date. All systems must accept new security patches for OS and HW continuously.

R All Linux servers are patched up to date. All systems must accept new patches continuously.

R All servers must be able to be monitored with NRK's monitoring system, Microsoft System Center Operations Manager (Current Build), either by installation of agent software, agentless monitoring supported by our monitoring systems or SNMP support.

R All Windows servers must be able to be managed by NRK's management software, Microsoft System Center Configuration manager (Current Build).

R All servers must support IPv4 and IPv6.

R All servers must support DNS.

R NRK has standardized on VMware vSphere 6.5 (VMX version 11 or newer), and use virtual servers as default on new installations. Virtual servers are an absolute requirement from all vendors and any reason for not virtualizing should be very well documented and tested. If virtualization is not possible, NRK will preferably purchase all standard server hardware required for new systems on our own agreements.

R These are the standard NRK models in prioritized order:

- Virtual (VMWare ESXi /vSphere 6.5 or newer)
- Blade (HP c-class or Dell M-series)
- Rack mounted server (HP ProLiant DL3xx or Dell R-series)

### Infrastructure as a Service (IaaS)

P All IaaS containing confidential or strictly confidential data must adhere to CSA Cloud Control Matrix

### Internet of Things (IoT) (empty)

## Network

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

B NRK has an efficient and less complex system portfolio as possible

B NRK's systems use standardized technology that is open and integratable

B NRK's technology facilitates coordinated, efficient and innovative interaction in NRK and with external

Derived principles and requirements for the network domain:

R SQL and other database protocols are only allowed from cleared security zones

R All network infrastructure and applications must support IPv4 and IPv6.