TLP:AMBER Limited distribution — share within your organisation on a need-to-know basis. Do not share externally without authorisation. TLP: https://www.first.org/tlp/ | DK: https://www.cfcs.dk/da/handelser/traffic-light-protocol/

Defencia.dk

Solution Design Document
SDD

[Project / System Name]

Project Name	*[Full project / system name]*
Document Title	Solution Design Document (SDD)
System / Product	*[System or product being designed]*
Author(s)	*[Name(s), Role(s)]*
Date	*[Date of this revision]*
Revision	X.X
Status	*[Draft / Under Review / Approved / Superseded]*
Classification	TLP:AMBER — Internal use. Do not distribute externally without authorisation.

TEMPLATE GUIDANCE *This template covers all standard sections of an enterprise SDD. Adapt depth and detail to the complexity of the system. Simple systems may collapse sections; complex systems should expand them. Remove TEMPLATE GUIDANCE boxes before publishing. This document is for internal use and should be stored in the CMDB / document management system. xleb@defecia.dk.*

Revision History

Version	Date	Author	Change Type	Description
1.0			Initial draft	

Request and Approval

GOVERNANCE This document requires sign-off from both the Requester and the Approving Manager before the solution moves to implementation. Security and Privacy review sign-off is mandatory for systems processing personal data or classified as business-critical.

Name	Role	Action (Req/Approv)	Date	Signature
	Requester			
	Technical Reviewer			
	Security Reviewer			
	CISO / ISSO			
	Approving Manager			

1. Introduction

1.1 Purpose

TEMPLATE GUIDANCE *State clearly what this document is for and what decision or action it supports. Who is the intended audience? (Architects, developers, security team, management, auditors?)*

[Describe the purpose of this Solution Design Document. What system or solution does it describe? What stage is the project at? What decisions does this document support?]

1.2 Scope

This section defines what is in scope and what is explicitly out of scope for this solution design.

In scope	*[List components, services, integrations, and user groups included in this design]*
Out of scope	*[List what is explicitly excluded, and why]*
Assumptions boundary	*[What assumptions define the scope boundary?]*

1.3 References

TEMPLATE GUIDANCE *List all documents, standards, and policies this SDD depends on or references. Include version numbers and document IDs where available.*

Ref	Document Title	Version / Date	Location / Link
R1	Business Requirements Document (BRD)		
R2	Information Security Policy		
R3	Risk Register		

R4	Data Protection Impact Assessment (DPIA)		
R5	Business Impact Analysis (BIA)		
R6	CMDB entry for this system		

2. System Overview

2.1 System Description

TEMPLATE GUIDANCE

Provide a high-level description of the system: what it does, who uses it, and what business problem it solves. If this is an 'as-is' documentation of an existing system, describe the current state and any delta from the target state.

[Describe the system: its primary function, intended user base, business context, and relationship to other systems. If documenting an existing ('as-is') system, describe current state and known gaps.]

2.2 Business Impact Assessment (BIA)

Classify the business impact of this system across the CIA triad. This drives security controls, SLA requirements, and recovery objectives.

Dimension	Rating (H/M/L)	Score (1–5)	Justification
Confidentiality			
Integrity			
Availability			

Additional BIA considerations:

GDPR relevance	*[Does this system process personal data? Categories? Number of data subjects? Lawful basis?]*
NIS2 relevance	*[Is this system in scope for NIS2 as an essential or important entity? Which sector? Which service?]*
Regulatory / compliance	*[Other applicable regulations: PCI-DSS, ISO 27001, DORA, sector-specific requirements]*
Data classification	*[What is the highest data classification this system handles? Public / Internal / Confidential / Restricted]*

2.3 Service Level Agreement (SLA)

Define the service levels this system must meet. These must be agreed with the business owner before design is finalised.

Service / Function	Target Uptime	RTO	RPO

RTO & RPO	RTO (Recovery Time Objective) = maximum acceptable time the system can be unavailable. RPO (Recovery Point Objective) = maximum acceptable data loss measured in time. Both must be set by the business owner, not IT alone.

2.4 CMDB Reference

CMDB record ID	*[Configuration Item (CI) ID in the CMDB]*
System owner	*[Name, role, and contact of the system owner]*
Technical owner	*[Name, role, and contact of the technical owner]*
Production approval reference	*[Reference to system approval / production sign-off documentation]*
Environment	*[Production / Staging / Development / DR]*

3. Design Considerations

3.1 Assumptions

TEMPLATE GUIDANCE *Document all assumptions made during the design process. If any assumption proves incorrect, this section identifies what parts of the design may need to be revisited.*

[List all assumptions. Example: 'It is assumed that the existing Active Directory infrastructure will be used for authentication.' 'It is assumed that the target environment is AWS EU (Ireland).']

3.2 Constraints

Design constraints limit the solution space. Document them explicitly.

Technology constraints	*[Mandated or excluded technologies, platforms, or frameworks]*
Budget constraints	*[Budget ceiling and its impact on design choices]*
Time constraints	*[Delivery deadline and its impact on scope or approach]*
Legal / regulatory constraints	*[GDPR, NIS2, data residency requirements, export controls]*
Organisational constraints	*[Skills available, team size, existing vendor relationships]*

3.3 Goals and Design Principles

- Security by design: security controls are built in, not bolted on
- Privacy by design: GDPR principles applied from the outset (Art. 25)
- Least privilege: every component and user account has the minimum permissions required
- Defence in depth: multiple layers of security controls
- Resilience: the system degrades gracefully under failure conditions
- Observability: the system produces sufficient logs and metrics to support operations and incident response
- Portability: avoid unnecessary vendor lock-in; prefer open standards

[Add or modify design principles specific to this project]

3.4 Risks, Risk Acceptance, and Exceptions

RISK vs EXCEPTION

A RISK is a known uncertainty that has been assessed and mitigated where possible. Residual risks must be accepted by management. An EXCEPTION is a temporary deviation from policy or standard — time-limited (max 6 months) and requires documented approval. Both must be recorded in the organisational risk register.

#	Risk / Exception Description	Type	Likelihood	Impact	Owner / Acceptance
1		*Risk / Exception*	*H/M/L*	*H/M/L*	
2		*Risk / Exception*	*H/M/L*	*H/M/L*	
3		*Risk / Exception*	*H/M/L*	*H/M/L*	

4. Architecture and System Design

4.1 High-Level Architecture

TEMPLATE GUIDANCE

Include architecture diagrams here. Recommended: (1) Context diagram showing the system boundary and external actors, (2) Component diagram showing internal services and their relationships, (3) Network diagram showing network zones, firewall boundaries, and data flows. Diagrams can be inserted as images or referenced from a linked draw.io / Visio / Miro file.

DIAGRAMS

Insert architecture diagrams as images, or reference the linked design file. For cloud systems: include the cloud provider's native architecture diagram. Always include a network zone diagram showing trust boundaries and firewall segmentation.

[Insert or reference high-level architecture diagram here. Describe the main components, their relationships, and the overall system boundary.]

4.2 Component Design

TEMPLATE GUIDANCE

Describe each major component or service in the system. For each: name, purpose, technology stack, scaling approach, dependencies, and owner.

Component	Technology	Hosted On	Dependencies	Notes / Owner

4.3 Database Design

TEMPLATE GUIDANCE *Describe the data model: primary databases, their type (relational/NoSQL/graph), schema overview, key entities and relationships. Reference ER diagrams or schema documents. Note any data classification and retention requirements.*

Database technology	*[e.g. PostgreSQL 15, Azure SQL, MongoDB, DynamoDB]*
Hosted / managed by	*[Cloud provider, on-premise, managed service]*
Data classification	*[What is the highest classification of data stored?]*
Retention policy	*[How long is data retained? Deletion / archival process?]*
Backup strategy	*[Frequency, location, encryption, retention of backups]*

[Describe database schema overview, key entities, and relationships. Reference linked ER diagrams or data model documentation.]

4.4 User Interface Design

TEMPLATE GUIDANCE *Reference mockups, wireframes, or design system documentation. Describe key user flows. Note accessibility requirements (WCAG 2.1 AA or higher).*

[Reference UI mockups or wireframes. Describe key user journeys. Note accessibility requirements and design system used.]

5. Integration and Data Flows

5.1 System Integrations

TEMPLATE GUIDANCE

Document every integration point: what system sends/receives data, what protocol is used, what authentication method, what data is exchanged, and who owns each side.

Source System	Target System	Protocol	Auth Method	Data Exchanged	Owner
		HTTPS/REST SFTP API	*OAuth 2.0 API Key MTLS*		
		HTTPS/REST SFTP API	*OAuth 2.0 API Key MTLS*		
		HTTPS/REST SFTP API	*OAuth 2.0 API Key MTLS*		

5.2 Data Flow Diagrams

TEMPLATE GUIDANCE

Insert or reference data flow diagrams (DFDs) here. At minimum: (1) Level 0 context DFD showing system boundary and external entities, (2) Level 1 DFD showing internal processes and data stores. For GDPR compliance, data flows involving personal data must map to the Record of Processing Activities (RoPA).

[Insert or reference data flow diagrams. For each flow involving personal data, note the data category, transfer mechanism, and legal basis under GDPR.]

6. Testing Strategy

6.1 Testing Overview

The following testing phases apply to this solution. Each phase must be completed and signed off before progression to the next.

Test Phase	Description	Responsible	Status
Unit Testing	Individual component / function testing by developers	Development Team	
Integration Testing	End-to-end testing of integration points and APIs	Development / QA	
System Testing	Full system testing against functional requirements	QA Team	
User Acceptance Testing (UAT)	Business validation that the solution meets requirements	Business Owner / Users	
Security Testing	Vulnerability assessment and/or penetration test by IT Security	IT Security	
Performance Testing	Load and stress testing to validate SLA targets	QA / IT Ops	
Disaster Recovery Test	Validation of RTO/RPO targets	IT Ops	

6.2 Sample Test Cases

TC#	Test Description	Expected Result	Actual Result	Pass/Fail
1				
2				
3				
4				
5				

7. Deployment Plan

7.1 Deployment Strategy

Deployment approach	*[Blue-green / Canary / Rolling / Big-bang / Phased rollout]*
Target environment	*[Cloud provider + region / On-premise data centre / Hybrid]*
Deployment pipeline	*[CI/CD tool: GitHub Actions / Azure DevOps / Jenkins / GitLab CI]*
IaC (Infrastructure as Code)	*[Terraform / Bicep / CloudFormation / Ansible / None]*
Rollback procedure	*[Describe how to roll back if deployment fails. Maximum rollback time?]*
Change management reference	*[Change ticket number or change advisory board (CAB) reference]*

[Describe the deployment plan in detail: sequence of steps, environment progression (dev → staging → production), go/no-go criteria, and communication plan for stakeholders.]

7.2 Maintenance and Operational Support

Operating team	*[Who is responsible for day-to-day operations after go-live?]*
Monitoring and alerting	*[Tools: Datadog / Azure Monitor / Grafana / Prometheus / Splunk / SIEM]*
On-call / support hours	*[24/7 / Business hours / Best effort]*
Patch management	*[Critical patches within 48h / Monthly patch cycle / vendor-managed]*
End of life (EOL) plan	*[When is EOL expected? What is the decommission / replacement plan?]*

8. Cloud Deployment

TEMPLATE GUIDANCE

Complete this section if any part of the solution is hosted on a public or private cloud platform. If on-premise only, mark as N/A. Cloud deployments have specific requirements for shared responsibility, data residency, exit strategy, and key management.

8.1 Cloud Deployment Design

Cloud provider(s)	*[AWS / Azure / GCP / OVHcloud / Other — specify region(s)]*
Data residency	*[Data must remain in EU/EEA. Confirm region. Schrems II compliance if US services used.]*
Shared responsibility model	*[Document which security responsibilities are cloud provider's and which are ours]*
Identity and Access Management	*[IAM design: roles, service accounts, MFA for console access, break-glass procedure]*
Network design	*[VPC/VNet design, subnet segmentation, security groups / NSGs, private endpoints]*
Logging & monitoring	*[CloudTrail / Azure Activity Log / GCP Audit Logs — sent to SIEM?]*

8.2 Encryption

Data at rest	*[AES-256. Provider-managed key (PMK) or Customer-managed key (CMK)? Key rotation policy?]*
Data in transit	*[TLS 1.2 minimum, TLS 1.3 preferred. Certificate authority and rotation.]*
Database encryption	*[Transparent Data Encryption (TDE) / column-level encryption for sensitive fields?]*
Key management	*[AWS KMS / Azure Key Vault / GCP KMS. Who controls the keys? Can the organisation recover without the vendor?]*

KEY CONTROL

If the cloud vendor controls encryption keys and the organisation cannot access data without vendor cooperation, this represents a concentration risk. Document and accept (or mitigate) this risk explicitly, referencing the Risk Register.

8.3 Exit Strategy

VENDOR LOCK-IN	Every cloud deployment must have a documented exit strategy. The organisation must be able to export all data and migrate to an alternative platform within an acceptable timeframe. Define this before deployment, not after.

Data export format	*[How can all data be exported? Format? Tool? Completeness?]*
Estimated migration time	*[How long would a full platform migration take? What is the target?]*
Contractual exit rights	*[What notice period applies? What data deletion certification is provided?]*
Alternative platform identified	*[Has a fallback platform been identified? What is the migration path?]*

9. Security

9.1 General Data Protection

- Access control: Role-Based Access Control (RBAC) — document roles and permissions matrix
- Authentication: MFA mandatory for all users with access to production systems or sensitive data
- Privileged access: Privileged Access Management (PAM) for administrator accounts. Just-in-time (JIT) access preferred
- Session management: session timeout, concurrent session limits, session token security
- Audit logging: all authentication events, privilege escalations, data access, and configuration changes logged. Logs retained for minimum [12 months]
- Log protection: logs must be tamper-evident and stored in a separate, secured log management system (SIEM)

[Describe additional security controls specific to this system's threat model and data classification]

9.2 Endpoint and Network Protection

- Network segmentation: system components in appropriate network zones (DMZ / internal / restricted). No direct internet exposure of internal services
- Firewall rules: document all required firewall rules. Default deny; explicit allow only
- Web Application Firewall (WAF): required for any internet-facing web application
- Intrusion Detection / Prevention (IDS/IPS): deployed at network perimeter
- Endpoint protection: EDR deployed on all servers. Automatic threat containment enabled
- Vulnerability management: systems scanned monthly. Critical CVEs patched within 48h. High within 14 days

9.3 Supply Chain Security and Vendor Breach Notification

NIS2 SUPPLY CHAIN NIS2 Article 21(2)(d) requires organisations to address security risks in supply chains. For each third-party component or service in this system, document how you will be notified of a breach on the vendor's side, and what your response process is.

Vendor / Component	Service Provided	Breach Notification SLA	Our Response Process
		[Hours to notification]	
		[Hours to notification]	
		[Hours to notification]	

10. Privacy

10.1 GDPR Compliance

TEMPLATE GUIDANCE

Complete this section for any system that processes personal data. If no personal data is processed, state this explicitly and provide justification. For high-risk processing, a Data Protection Impact Assessment (DPIA) is mandatory under GDPR Article 35.

Personal data processed	*[Describe categories: names, emails, IP addresses, health data, financial data, etc.]*
Data subjects	*[Who are the data subjects? Employees / customers / public?]*
Lawful basis	*[GDPR Art. 6: Consent / Contract / Legal obligation / Vital interests / Public task / Legitimate interests]*
Special category data	*[Art. 9: Health, biometric, racial/ethnic, political, religious, sexual orientation? If yes: Art. 9(2) basis?]*
Data retention	*[How long is personal data retained? Automated deletion process?]*
Data subject rights	*[How are access, rectification, erasure, portability, and objection requests handled?]*
Data transfers outside EEA	*[Are data transfers to non-EEA countries involved? Mechanism: SCCs / Adequacy decision / BCRs?]*
DPIA required?	*[Yes / No / Screened. If yes: reference DPIA document ID]*
DPO consulted?	*[Name of DPO and date of consultation]*
RoPA entry	*[Record of Processing Activities: reference entry ID]*

10.2 Encryption (Privacy Perspective)

Data at rest	*[AES-256. CMK or PMK? Key holder? Annual key rotation?]*
Data in transit	*[TLS 1.3 preferred, TLS 1.2 minimum. HSTS enabled for web services.]*
Database encryption	*[TDE enabled? Column-level encryption for PII fields (e.g. national ID, health data)?]*
Backup encryption	*[All backups encrypted with same or higher standard as production data?]*
Personal data	*[Is pseudonymisation or anonymisation applied where possible? Technique*

pseudonymisation	*used?]*

11. Supply Obligations and NIS2

NIS2	The NIS2 Directive (EU 2022/2555) requires essential and important entities to implement cybersecurity risk management measures across their supply chain. If your organisation is subject to NIS2, this section is mandatory. If not subject to NIS2, document this explicitly and keep the section for awareness.

11.1 NIS2 Applicability

NIS2 classification	*[Essential entity / Important entity / Not subject to NIS2]*
Sector	*[Energy / Transport / Banking / Health / Digital Infrastructure / ICT / Other]*
Competent authority	*[Which national authority is responsible? (DK: CFCS / Digitaliseringsstyrelsen)]*
Incident reporting obligation	*[Art. 23: Early warning within 24h. Full notification within 72h. Final report within 1 month.]*

11.2 NIS2 Security Measures for This System

The following NIS2 Article 21 security measures apply to this system. Document compliance or planned compliance for each:

NIS2 Art. 21 Measure	Compliant?	How Addressed in This Design
Policies on risk analysis and IS	*Yes / Partial / No*	
Incident handling	*Yes / Partial / No*	
Business continuity and crisis management	*Yes / Partial / No*	
Supply chain security	*Yes / Partial / No*	
Secure acquisition, development, and maintenance	*Yes / Partial / No*	
Policies to assess effectiveness of cybersecurity measures	*Yes / Partial / No*	
Cyber hygiene practices and training	*Yes / Partial / No*	
Cryptography and encryption policies	*Yes / Partial / No*	
Human resources security and access control	*Yes / Partial / No*	
MFA or continuous authentication	*Yes / Partial / No*	

A. Appendix

Appendix A — Glossary

Term	Definition
BIA	Business Impact Analysis — assessment of the impact of system unavailability on the organisation
CIA	Confidentiality, Integrity, Availability — the three pillars of information security
CMDB	Configuration Management Database — authoritative record of IT assets
CMK	Customer-Managed Key — encryption key controlled by the organisation, not the cloud provider
DPIA	Data Protection Impact Assessment — mandatory under GDPR Art. 35 for high-risk processing
IaC	Infrastructure as Code — managing infrastructure through version-controlled configuration files
JIT	Just-In-Time access — temporary, on-demand privileged access granted only when needed
PAM	Privileged Access Management — controls and audit of administrator and privileged accounts
RoPA	Record of Processing Activities — GDPR Art. 30 mandatory register of data processing activities
RPO	Recovery Point Objective — maximum acceptable data loss in time
RTO	Recovery Time Objective — maximum acceptable system downtime
SDD	Solution Design Document — this document
SLA	Service Level Agreement — agreed performance and availability targets
TDE	Transparent Data Encryption — database-level encryption at rest
TLP	Traffic Light Protocol — information sharing classification system
WAF	Web Application Firewall — protects web applications from common attacks

Appendix B — Additional Technical Specifications

[Include detailed technical specifications, code snippets, API contracts, configuration examples, or expanded diagrams that are too detailed for the main body.]

Appendix C — Final Approval Sign-off

The undersigned confirm that they have reviewed and approved this Solution Design Document for implementation.

Name	Role	Action (Req/Approv)	Date	Signature
	Requester			
	Technical Reviewer			
	Security Reviewer			
	CISO / ISSO			
	Approving Manager			

A design document that is not kept current is worse than no design document — it creates false confidence. Update this SDD with every significant change and store it alongside the CMDB entry.