Orion Software Solutions Ltd.

Internal Docupedia - Simulated Corporate Knowledge Base

Document classification: Internal (Simulated) | **Version:** 1.0 | **Effective date:** 2026-01-20

Purpose: Provide a realistic, end-to-end Docupedia source for software platform project testing, including people, projects, processes, and policies.

Disclaimer: All names, projects, systems, figures, and policies in this document are fictitious and intended solely for test and demonstration purposes.

1. Company Overview

Orion Software Solutions Ltd. is a mid-sized European software development company founded in 2016. The company builds and operates long-lived platforms for enterprise and regulated clients, prioritizing reliability, compliance, and sustainable delivery.

Primary service lines: (a) SaaS platform development and operation, (b) enterprise modernization programs, (c) applied AI automation, (d) product engineering for regulated digital services.

Delivery model: cross-functional product teams, each responsible for a bounded domain, end-to-end (build-run-own).

Locations (simulated): Sofia (HQ), Plovdiv (engineering hub), Berlin (customer success), Vienna (sales), remote employees across the EU.

Core metrics (simulated): 145 employees, 6 product teams, 3 shared services teams, 99.92% average monthly platform uptime across production systems.

Company values: ownership, clarity, pragmatism, learning, and customer trust.

1.1 Executive Leadership (Simulated)

Role	Name	Responsibilities	Decision Scope
CEO	Mila Vankova	Company strategy, revenue, partnerships, risk acceptance	Strategic and commercial decisions
CTO	Dr. Petar Dimitrov	Technology strategy, architecture governance, engineering productivity	Technical strategy and standards
COO	Rumen Iliev	Delivery operations, resource planning, incident governance	Operational and delivery decisions
Head of People & Culture	Nadia Petrova	Hiring, performance framework, policies, culture programs	People policies and escalation
Head of Security & Compliance	Todor Hristov	Security program, audits, data protection, vendor risk	Security exceptions and controls

1.2 How to Use This Docupedia

This Docupedia is structured for fast retrieval and operational use. Each section includes: purpose, scope, ownership, procedures, templates, and escalation paths.

Update expectation: If you discover incorrect or outdated content, you must create a Docupedia ticket within 24 hours, referencing the section number and proposing a correction.

Ownership: Each section has an assigned owner. Owners review their content quarterly, or sooner if triggered by incidents, audit findings, or major organizational changes.

2. Organizational Structure

Orion uses a matrix model: employees belong to a functional discipline (for standards and development) and to a delivery team (for product outcomes).

Delivery units: product teams (Atlas, Helios, Nova, Aurora, Meridian, Sentinel) and shared services (Platform Engineering, Security, Internal Tools).

Functional chapters: Backend Engineering, Frontend Engineering, Mobile, QA, DevOps/SRE, Data/ML, UX, Product.

2.1 Teams and Primary Responsibilities

Team	Primary Domain	Typical Outputs	Key Interfaces
Atlas	Manufacturing ERP	Modules, integrations, reporting packs	Platform Eng, Security, Customer Success
Helios	AI Support Automation	Models, inference APIs, workflows	Security, Data Governance, Support Ops
Nova	Fintech Mobile Platform	Mobile apps, APIs, compliance artifacts	Legal, Compliance, Security, SRE
Aurora	Identity & Access	SSO, RBAC, audit trails	All product teams
Meridian	Billing & Subscriptions	Billing engine, invoicing, pricing rules	Finance, Customer Success, Legal
Sentinel	Observability & Reliability	SLIs/SLOs, incident tooling, runbooks	All product teams, COO office

2.2 Key Roles (Definitions)

Product Owner (PO): Owns product backlog, acceptance criteria, and stakeholder alignment. Accountable for scope and value.

Engineering Lead (EL): Owns technical delivery, code quality, architecture decisions within team boundaries, and engineering execution risk.

Delivery Manager (DM): Owns sprint operations, cross-team dependencies, release readiness and reporting.

SRE: Owns reliability posture, observability, on-call practices, and production readiness reviews.

3. Engineering Principles and Standards

Engineering standards exist to reduce variance, prevent avoidable failures, and improve cross-team mobility.

Non-negotiables: peer review, automated testing, vulnerability scanning, documented runbooks for production services, and measurable SLIs/SLOs.

Architectural style: modular monoliths where appropriate; microservices only when justified by scaling, isolation, or compliance constraints.

3.1 Definition of Done (DoD)

Dimension	Minimum Requirement
Code Quality	1+ approving review; no critical lint issues; style guide compliance
Tests	Unit tests for logic; integration tests for external boundaries; CI green
Security	No high/critical vulnerabilities; secrets managed via vault; access scopes validated
Observability	Structured logs, metrics, and alerts; dashboard link in README
Docs	Updated ADRs/runbooks; release notes drafted if user-facing change

Ops	Rollback plan confirmed; capacity impact considered

3.2 Coding and Review Practices

Code reviews focus on correctness, maintainability, and operational risks. Reviewers must challenge unclear naming, missing tests, hidden coupling, and unsafe defaults.

Required review depth: risk-based. Payments, identity, and PII flows require senior review and security sign-off.

Commit conventions: Conventional Commits (feat/fix/chore/docs) with ticket reference (e.g., NOVA-412).

4. Active Projects Overview

Orion currently operates six active product domains. Each project page summarizes business goal, architecture, technology stack, delivery status, team, and onboarding path.

4.1 Project Atlas (Manufacturing ERP)

Objective: Provide modular ERP capabilities for mid-sized manufacturing clients with configurable workflows and audit-grade reporting.

Key modules: Finance (GL/AP/AR), Inventory, Production Planning, Quality Management, Reporting, Integrations (EDI, SAP exports).

Tech stack: Java 21, Spring Boot, PostgreSQL, React, Kafka, Kubernetes (EKS), Helm, Prometheus/Grafana, OpenTelemetry.

Current status (simulated): 68% complete; 3 customers live on Finance + Inventory; production planning in pilot; next quarter focus on analytics and EDI connectors.

Known risks: EDI connector variability across clients; data migration throughput; report performance under peak load.

Team: Ivan Petrov (EL), Violeta Stancheva (PO), Dimitar Rusev (DM), Maria Koleva, Stefan Ivanov, Georgi Dimitrov (Backend), Elena Markova, Petar Angelov (Frontend), Nikolay Stoyanov (QA), Radoslav Georgiev (DevOps).

4.2 Project Helios (AI Support Automation)

Objective: Reduce customer support time-to-resolution by automated classification, summarization, and recommended response drafts, with human-in-the-loop controls.

Core capabilities: ticket ingestion, language detection, routing, sentiment scoring, response suggestion, feedback loop retraining.

Tech stack: Python, FastAPI, PyTorch, Redis, OpenSearch, S3, AWS ECS, feature store (Feast), batch jobs (Airflow).

Current status (simulated): 42% complete; model v0.7 in evaluation; inference API in internal beta; privacy controls under review.

Constraints: PII redaction, retention rules, audit logs for model outputs, explainability summaries for regulated customers.

Team: Daniela Hristova (ML Lead), Nikolay Marinov (PO), Kaloyan Marinov, Vasil Petkov, Yoana Ilieva (ML Eng), Teodora Mileva (Backend), Martin Bonev (QA).

4.3 Project Nova (Fintech Mobile Platform)

Objective: Deliver a mobile-first banking platform for EU SMEs with strong compliance controls and a modern UX.

Key features: accounts, cards, payments, expense categorization, invoice scanning, approvals, audit trails, and Open Banking connectivity.

Tech stack: Kotlin (Android), Swift (iOS), shared UI components (Flutter module), Node.js (BFF), MongoDB, PostgreSQL (ledger), OAuth2/OIDC, HSM integration for signing.

Current status (simulated): 83% complete; security testing and regulatory audit underway; launch readiness gated by penetration test remediation.

Team: Desislava Todorova (PO), Hristo Angelov (EL), Borislav Kolev (Mobile), Irena Stoimenova (Mobile), Simeon Rachev (Backend), Antonia Georgieva (Compliance), Milen Atanasov (SRE), Yana Pavlova (QA).

4.4 Project Aurora (Identity & Access)

Objective: Centralized identity platform for all Orion products: SSO, RBAC, audit logs, and customer tenant management.

Tech stack: Go, PostgreSQL, Keycloak extensions, OIDC/SAML connectors, Terraform, Vault, Kubernetes.

Status (simulated): 55% complete; RBAC v1 shipped; SAML connectors in progress; audit logging standardized.

Team: Georgi Velikov (EL), Plamen Yordanov (Backend), Daria Hristova (Backend), Ivana Koleva (QA), Todor Hristov (Security oversight).

4.5 Project Meridian (Billing & Subscriptions)

Objective: Subscription, billing, invoicing, and pricing rule engine for all SaaS products, including EU VAT handling.

Tech stack: .NET 8, PostgreSQL, RabbitMQ, React admin console, PDF generation service, Stripe/Adyen connectors (simulated).

Status (simulated): 61% complete; invoicing live for internal use; tax rules expanding; dunning workflow in design.

Team: Stoyan Ivanchev (EL), Lina Karadzhova (PO), Krasimir Petrov (Backend), Petya Nikolova (Frontend), Ivan Valchev (QA).

4.6 Project Sentinel (Observability & Reliability)

Objective: Improve MTTR and reliability through standardized dashboards, alerts, incident tooling, and operational readiness practices.

Tech stack: OpenTelemetry, Prometheus, Grafana, Loki, Tempo, PagerDuty equivalent (simulated), runbook repository.

Status (simulated): Ongoing; 90% of services instrumented; SLOs defined for critical paths; on-call playbooks adopted by all teams.

Team: Milen Atanasov (SRE Lead), Ralitsa Ganeva (SRE), Dimitar H. Petrov (Platform Eng), with rotating representatives from each product team.

5. Employee Onboarding

Onboarding is a managed process with explicit outcomes. The goal is to reach safe independent delivery by the end of week 4 and reliable on-call participation (where relevant) by the end of month 3.

5.1 Day 0-5: Setup and Orientation

IT provisioning: laptop enrollment, MFA, password manager, VPN, device encryption, endpoint protection.

Accounts: email, chat, issue tracker, source control, CI/CD, observability, HR portal.

Mandatory training: security basics, data protection, secure coding, workplace conduct, and incident reporting.

Outcome: environment builds successfully, first documentation contribution submitted (small but real).

5.2 Week 2-4: Project Integration

New hires are assigned a mentor and a 30-day plan. The plan includes: architecture tour, codebase navigation, service ownership boundaries, and first deliverable.

Expected deliverables: (1) at least one low-risk change merged, (2) one test added or improved, (3) one runbook update, (4) demo of delivered work at sprint review.

Mobility design: internal docs must be sufficient for a qualified engineer to become productive in 2 weeks without tribal knowledge.

5.3 Project-Specific Onboarding (Template)

Checklist Item	Description	Owner
Architecture Tour	System context, data flows, boundaries, key failure modes	Engineering Lead
Local Setup	Run services locally or via dev cluster; seeded test data	Mentor
Access Review	Least privilege; confirm required repos and environments	IT + Security
First Task	Small change with tests and deploy to staging	Mentor + DM
Operational Readiness	Understand alerts, dashboards, and incident procedure	SRE

6. Vacation and Time-Off Policy

Annual leave: 25 working days per calendar year (simulated default), prorated for partial-year employment.

Carryover: up to 5 days may be carried to Q1 of the next year with manager approval.

Minimum notice: 10 working days for vacations longer than 3 days; 2 working days for 1-2 day requests.

6.1 How to Request Vacation

1) Submit request in HR portal (Time Off -> New Request). 2) Add coverage plan in the request notes. 3) Inform your team in the weekly planning meeting. 4) Wait for manager approval.

Coverage plan must include: ownership of active tickets, on-call swap if applicable, and any customer deadlines impacted.

Approval SLA: managers approve or reject within 3 business days. If not addressed, escalate to Delivery Manager.

6.2 Sick Leave and Unplanned Absence

Report sick leave to your manager and team channel before 10:00 local time. For absences longer than 2 consecutive days, provide documentation per local legal requirements (simulated).

If you are on-call and become unavailable, you must request an on-call handover immediately to avoid coverage gaps.

7. Remote Work and Home Office

Orion operates a hybrid work model. Default expectation is 2 days/week in-office for teams with on-site collaboration needs; otherwise flexible within agreed team norms.

Eligibility: all roles by default, except positions requiring on-site lab access or regulated customer constraints.

7.1 Home Office Request Process

Submit request in HR portal (Remote Work -> Request). Include date(s), reason category (personal logistics, deep work, travel), and any meetings impacted.

Approval criteria: no critical on-site dependencies, coverage maintained, security conditions met (private workspace, no unauthorized recording, no public Wi-Fi without VPN).

Default limit: up to 3 remote days/week unless otherwise agreed with the manager.

7.2 Remote Security Requirements

Use company VPN for all access. Lock your screen when away. Never print confidential content at home. Do not store customer data locally unless explicitly approved and encrypted.

Video calls must be taken in a non-public environment when discussing confidential information.

8. Incident Management

Incident management is standardized to reduce mean time to detect (MTTD) and mean time to restore (MTTR). The process is owned by the Sentinel team and enforced by the COO office.

8.1 Severity Levels and Targets

Severity	Definition	Response Target	Update Cadence	Postmortem
SEV-1	Full outage or critical regulatory exposure; major customer impact	15 minutes	Every 30 minutes	Required within 72 hours
SEV-2	Partial outage or major degradation; limited customer set	30 minutes	Every 60 minutes	Required within 5 business days

SEV-3	Non-critical degradation; workaround exists	4 hours	Daily until resolved	Optional; required if recurring
SEV-4	Minor defect; no immediate customer impact	2 business days	Weekly	Not required

8.2 Incident Roles

Incident Commander (IC): coordinates response, owns timeline, and decides when to escalate or declare resolved.

Operations Lead: executes mitigation steps, coordinates deployments and rollbacks.

Communications Lead: posts internal updates and customer-facing status messages if required.

Scribe: records timeline, decisions, and action items for postmortem.

8.3 Standard Incident Flow

1) Detect (alert, customer report, monitoring). 2) Triage (severity assignment, initial hypothesis). 3) Mitigate (rollback, feature flag, capacity change). 4) Restore service. 5) Verify and monitor. 6) Postmortem and corrective actions.

Rules: No blame, but clear accountability. If unsure, reduce blast radius first.

9. Team Building and Culture

Orion treats culture as an operational asset: it reduces coordination cost and improves execution under pressure.

9.1 Past Team Building Highlights (Simulated)

2024 Q3 - Rhodope retreat: 3-day offsite with cross-team workshops and a customer simulation exercise focused on incident response and stakeholder communication.

2025 Q1 - Internal hack week: 52 prototypes built, including automated release notes generator and a runbook linter; 9 prototypes moved to production tools.

2025 Q4 - Berlin customer visit: mixed team attended a customer onsite to validate workflows; output included prioritized UX debt backlog and a revised onboarding guide.

9.2 Future Plans

2026 Q2 - International offsite: focus on cross-team architecture alignment and product strategy deep dives.

Quarterly: innovation days (one business day), wellness stipend pilot, and chapter-led learning sessions.

10. Career Development and Promotions

Career development is managed through two tracks: Individual Contributor (IC) and Management. Employees may switch tracks based on demonstrated skills and business needs.

10.1 Career Levels (IC Track - Summary)

Level	Title	Typical Scope	Promotion Signals
IC1	Software Engineer	Small tasks, guided delivery	Consistent delivery; quality basics; learning velocity
IC2	Software Engineer II	Features end-to-end within a team	Owns small areas; strong tests; reliable estimates
IC3	Senior Engineer	Subsystem ownership; mentors others	Designs solutions; improves reliability; reduces risk
IC4	Staff Engineer	Cross-team technical leadership	Drives standards; resolves complex incidents; architecture
IC5	Principal Engineer	Company-wide technical strategy	Creates leverage; aligns teams; measurable platform impact

10.2 Promotion Process

Promotions occur in April and October (simulated). Candidates submit a promotion packet including impact summary, evidence artifacts (PRs, ADRs, incident leadership), and peer feedback.

A promotion committee (CTO, chapter leads, HR) reviews packets using calibrated rubric. Decisions are documented for transparency.

11. Security and Compliance

Security and compliance are baseline requirements. Orion follows a control framework aligned with common standards (e.g., ISO 27001 concepts) without claiming certification in this simulated document.

11.1 Access Control

Access is granted by least privilege and time-bounded where possible. Elevated access (production write, admin consoles) requires manager approval and security ticket.

Quarterly access reviews are mandatory. Unreviewed access is removed automatically after 30 days of inactivity (simulated control).

11.2 Secure Development Requirements

Secrets must never be committed to source control. Use Vault-managed secrets. Third-party dependencies are scanned; high/critical findings must be remediated before release.

For PII flows, implement: encryption in transit and at rest, data minimization, audit logs, and retention controls.

12. Appendices

Appendices provide templates, reference checklists, and operational artifacts used across teams.

12.1 Template Index

Template	Use Case	Location (Simulated)

ADR Template	Architectural decisions and rationale	Docupedia/Engineering/ADRs
Incident Postmortem	Standard postmortem format	Docupedia/Operations/Incidents
Onboarding Plan	30-day plan for new hires	Docupedia/People/Onboarding
Release Checklist	Production release readiness	Docupedia/Engineering/Releases
RACI Matrix	Role clarity for initiatives	Docupedia/Governance/RACI

13. Internal Tooling and Systems

Orion standardizes tooling to reduce friction and make cross-team collaboration predictable.

13.1 Tooling Stack (Simulated)

Category	System	Primary Purpose	Owner
Issue Tracking	Jira-like Tracker	Backlog, sprint planning, incident tickets	COO office
Source Control	GitHub Enterprise-like	Repositories, PR reviews, permissions	Platform Eng
CI/CD	Buildkite-like + ArgoCD-like	Build/test/deploy automation	Platform Eng
Observability	Grafana + Prometheus + Loki	Dashboards, alerting, logs	Sentinel
Docs	Confluence-like Wiki	Docupedia pages, knowledge sharing	CTO office
Secrets	Vault-like	Secrets management, rotations	Security

13.2 Access Requests

Tool access is requested via IT ticket with business justification and role. Security-sensitive systems require security approval and time-limited access where possible.

14. Quality Assurance and Testing

Quality is treated as a lifecycle practice, not a phase. Teams own quality outcomes and partner with QA to design effective coverage.

14.1 Testing Strategy

Unit tests: cover business logic and edge cases. **Integration tests:** cover boundaries with databases, message brokers, and external APIs. **E2E tests:** cover critical user journeys.

Test failures blocking main branch must be fixed immediately. Flaky tests are treated as production risk and prioritized accordingly.

14.2 Test Data and Environments

Dev and staging environments use sanitized datasets. Production-like data is restricted and requires explicit security approval for testing in isolated environments.

15. Release Management

Release management ensures predictable delivery with traceability, safe rollbacks, and clear communication.

15.1 Release Cadence

Default cadence: weekly releases for non-regulated products, bi-weekly for regulated products. Critical fixes may be hotfixed with full documentation.

Releases require: change summary, risk assessment, backout plan, monitoring plan, and sign-offs where required.

15.2 Release Checklist (Summary)

Checklist includes: CI green, security scan passed, database migrations reviewed, feature flags configured, runbooks updated, dashboards prepared, customer communication drafted if needed.

16. Knowledge Sharing and Documentation

Documentation is a deliverable. If it is not documented, it is not done.

16.1 Documentation Standards

Docs are written for a new engineer joining tomorrow. Avoid tribal knowledge. Include diagrams, key failure modes, and operational runbooks.

Architecture decisions are captured in ADRs. Each ADR includes context, decision, alternatives, and consequences.

16.2 Knowledge Sharing Rituals

Each team runs a monthly tech talk. Chapters run quarterly deep-dive sessions. Major incidents trigger a postmortem review session shared across teams.

17. Performance Management

Performance management exists to align effort to outcomes and to make expectations explicit.

17.1 Goal Setting

Employees define semi-annual objectives using a simple structure: objective, success metrics, evidence artifacts, risks, and alignment to team goals.

Objectives are reviewed mid-cycle to adjust for changing priorities.

17.2 Feedback

Feedback is continuous. Managers are expected to provide actionable feedback within one week of observing material behavior, positive or negative.

18. Compensation and Benefits

Compensation is benchmarked annually against relevant markets and adjusted based on performance, scope, and company results (simulated).

18.1 Benefits (Simulated)

Standard benefits include private health insurance, learning budget (EUR 1,000/year), ergonomic home office stipend, and annual wellbeing allowance.

Travel and conference participation is approved based on role relevance and expected business impact.

18.2 Compensation Changes

Out-of-cycle adjustments may occur for promotions, scope changes, or retention risk, and require approval from People & Culture and the responsible executive.

19. Legal and Compliance Framework

Legal and compliance requirements vary by product domain and customer. Compliance artifacts are treated as deliverables and are stored in controlled repositories.

19.1 Contractual Commitments

Teams must understand contractual SLAs and security requirements before committing to timelines. If a contract implies operational constraints (e.g., RTO), it must be reflected in engineering plans.

19.2 Regulatory Readiness (Fintech Example)

For fintech products, maintain audit logs, change management evidence, access reviews, vulnerability remediation records, and incident reports as required by customers or regulators.

20. Risk Management

Risks are tracked as first-class work. A risk is any credible event that could materially impact delivery, security, compliance, or customer trust.

20.1 Risk Register (Example)

Risk	Likelihood	Impact	Owner	Mitigation
EDI connector variability in Atlas	Medium	High	Atlas EL	Connector framework with client-specific adapters; staged rollouts and contract tests per client

PII leakage in Helios datasets	Low	Critical	ML Lead + Security	Automated redaction pipeline; dataset access controls; quarterly audits; synthetic data for development
Regulatory audit delays for Nova	Medium	High	Nova PO	Early audit preparation; remediation sprints; buffer for external assessor; weekly compliance sync

20.2 Escalation

High-impact risks must be escalated to the COO and logged with mitigation and review cadence. Unowned risks are unacceptable.

21. Business Continuity and Disaster Recovery

Business continuity ensures that Orion can operate under disruption. Disaster recovery focuses on restoring systems after major failures.

21.1 Backup Policy (Simulated)

Production databases are backed up daily with encrypted storage and a 30-day retention window. Critical systems have hourly incremental backups.

Backup restoration is tested quarterly for critical services and annually for all services.

21.2 Recovery Objectives

System Type	RTO (Target)	RPO (Target)	Notes
Identity (Aurora)	2 hours	15 minutes	Required for all other systems to operate; prioritize auth and tenant resolution
Payments/Ledger (Nova)	1 hour	5 minutes	Regulated; highest priority; validated via quarterly restoration drill
ERP Core (Atlas)	4 hours	60 minutes	Customer-specific downtime constraints; may use degraded mode for reporting
Observability (Sentinel)	8 hours	4 hours	Fallback to cloud provider logs and minimal alerting during outage

22. Code of Conduct and Ethics

Employees must act professionally and ethically. Orion maintains a zero-tolerance stance toward harassment, discrimination, retaliation, and deliberate policy violations.

22.1 Conflicts of Interest

Employees must disclose conflicts of interest (e.g., working for a competitor, vendor relationships, or financial stakes) to People & Culture. Undisclosed conflicts may result in disciplinary action.

22.2 Reporting Concerns

Concerns may be reported to your manager, People & Culture, or via a confidential reporting channel. Reports are investigated with confidentiality and anti-retaliation protections (simulated).

23. Docupedia Governance

Docupedia governance ensures content quality, ownership, and consistency.

23.1 Governance Board (Simulated)

Board members: CTO (chair), COO, Head of Security, Chapter Leads, and a rotating representative from each product team.

The board meets monthly to approve major changes, resolve conflicts, and drive documentation quality initiatives.

23.2 Change Control

Minor edits may be made directly by owners. Major changes (policy changes, security controls, legal commitments) require governance review and an approved ticket.

24. Decision-Making Framework

Decision-making at Orion is explicit and time-bounded. The goal is to avoid decision paralysis and ensure accountability.

24.1 Decision Types

Strategic: product portfolio, major investments, market direction (owned by CEO/Exec).

Tactical: roadmap scope, resourcing, major architectural direction within products (owned by PO/EL with CTO oversight).

Operational: implementation details, sprint commitments, defect prioritization (owned by teams within constraints).

24.2 Decision Record

Material decisions must be recorded as ADRs or decision notes including: context, options, decision, owner, date, and follow-up actions.

25. RACI and Ownership Model

Major initiatives require clear ownership. Orion uses RACI to eliminate hidden work and prevent dropped responsibilities.

25.1 When RACI is Required

RACI is mandatory for: cross-team projects, compliance programs, major releases, vendor onboarding, and customer escalations.

25.2 Example RACI - Production Release for Nova

Activity	Responsible	Accountable	Consulted	Informed
Release readiness review	Nova DM	Nova EL	SRE, Security	COO office
Pen-test remediation sign-off	Security Eng	Head of Security	Nova EL	CTO, PO
Customer communication	Customer Success	PO	Legal	CEO (if SEV-1)

26. Financial Awareness and Cost Responsibility

Engineering decisions have financial consequences. Teams must understand and control their cost drivers.

26.1 Common Cost Drivers

Infrastructure (compute, storage, data transfer), managed services (search, queues), licenses, contractor time, and operational overhead from incidents and manual processes.

Teams are expected to identify cost hotspots and propose optimizations quarterly.

26.2 Spend Controls (Simulated)

Any recurring expense above EUR 500/month requires a cost justification and approval from the COO office. Annual licenses above EUR 5,000 require CFO sign-off (simulated).

27. Vendor and Third-Party Management

Third-party vendors introduce operational and security risk. Vendor onboarding is controlled and documented.

27.1 Vendor Onboarding Steps

1) Business justification. 2) Security questionnaire. 3) Data processing assessment. 4) Contract review. 5) Trial in non-production. 6) Production approval.

Vendors handling confidential or restricted data require explicit approval from Security and Legal.

27.2 Annual Review

Vendor relationships are reviewed annually for cost, service quality, security posture, and alternatives. Decommission plans are created for high-risk or low-value vendors.

28. Intellectual Property Management

All work produced in the course of employment is company IP unless otherwise agreed in writing. This includes code, documentation, designs, models, and internal tools.

28.1 Open Source Use

Open-source components must comply with license policies. Copyleft licenses that impose distribution obligations require legal approval before use.

28.2 Open Source Contributions

Employees may contribute to open source only with manager approval and after confirming no customer confidential information or internal IP is disclosed.

29. Data Governance and Classification

Data governance ensures consistent handling of data based on sensitivity, legal obligations, and customer commitments.

29.1 Classification Levels

Classification	Examples	Handling Requirements
Public	Marketing pages, published blog posts	No restrictions beyond standard professionalism
Internal	Internal docs, non-sensitive process notes	Access limited to employees and approved contractors
Confidential	Customer tickets, contracts, non-public roadmaps	Need-to-know; encrypted storage; no external sharing
Restricted	PII, financial identifiers, credentials, regulated datasets	Strict access control; logging; encryption; retention rules; security approval for transfers

29.2 Data Retention (Simulated)

Customer support content: 18 months retention unless contractual requirements differ. PII: minimum necessary retention, reviewed quarterly. Logs: 30 days hot storage, 180 days cold storage for audit needs where required.

30. Company Exit and Offboarding

Offboarding ensures continuity, protects company assets, and enables learning from departures.

30.1 Offboarding Checklist (Summary)

Item	Owner	Due
Access revocation (email, repos, CI/CD, VPN)	IT Ops	Last working day
Device return / wipe confirmation	IT Ops	Last working day
Knowledge transfer session and handover notes	Manager + Employee	Within last 5 days
Project ownership reassignment in tracker	Delivery Manager	Before departure

Exit interview and feedback capture	People & Culture	Last 10 days

30.2 Knowledge Transfer Expectations

Departing employees must provide: current work status, key architectural context, open risks, operational insights, and contacts. Handover notes must be stored in the team knowledge base and linked from the relevant project page.