Unified Compliance & Contractual Documentation Pack (Sample)

Organization: HeliosOne Global Services Ltd.
Industry: Enterprise Cloud & Data Analytics
Geographic Presence: EU, UK, US, APAC
Purpose: This multi-document PDF is a **synthetic but realistic** sample created to test document ingestion, classification, RAG, and compliance analysis pipelines.

SECTION A — MASTER SERVICE AGREEMENT (MSA)

This Master Service Agreement (MSA) governs the provision of services by HeliosOne Global Services Ltd. to its customers.

1. Scope of Services

HeliosOne shall provide cloud-hosted analytics, data processing, and reporting services as defined in applicable Statements of Work (SOW).

2. Data Ownership

All customer data remains the sole property of the Customer. HeliosOne shall act as a data processor.

3. Confidentiality

Each party shall protect Confidential Information using reasonable security measures. However, encryption requirements are not explicitly mandated for all data classes.

4. Liability & Indemnification

Liability is capped at 12 months of fees. Cybersecurity incidents are partially excluded from indemnification.

SECTION B — SERVICE LEVEL AGREEMENT (SLA)

1. Availability

The Services shall be available 99.5% of the time, measured monthly. Planned maintenance may exceed 8 hours per month.

2. Incident Response

Critical incidents will be acknowledged within 4 hours and resolved on a best-effort basis.

3. Service Credits

Service credits are provided only after customer request and are capped at 5% of monthly fees.

Severity	Response Time	Resolution Target
Critical	4 hours	Best effort
High	8 hours	72 hours
Medium	24 hours	5 business days

SECTION C — SOC 2 TYPE II SUMMARY

This section summarizes controls aligned with the AICPA Trust Services Criteria.

Security

Logical access is enforced using role-based access control. Multi-factor authentication is implemented only for administrative users.

Availability

Backups are performed daily; restoration testing is conducted annually.

Confidentiality

Confidential data is encrypted at rest in production systems. Non-production systems are excluded.

Incident Management

Incident response procedures exist but are not formally tested on a scheduled basis.

SECTION D — ISO/IEC 27001:2022 CONTROL STATEMENT

A.5 Information Security Policies

Information security policies are documented but not reviewed annually.

A.8 Asset Management

Asset inventory exists but does not include ephemeral cloud resources.

A.9 Access Control

User access reviews are conducted annually instead of quarterly.

A.12 Operations Security

Logging is enabled; however, log retention is limited to 30 days.

SECTION E — GDPR & DATA PROTECTION POLICY

1. Lawful Basis of Processing

Personal data is processed primarily under contractual necessity and legitimate interest.

2. Data Subject Rights

Requests for access, rectification, and erasure are handled within 45 days.

3. Breach Notification

Supervisory authorities will be notified of personal data breaches within 96 hours where feasible.

4. International Transfers

Standard Contractual Clauses (SCCs) are used; Transfer Impact Assessments are not consistently documented.

DOCUMENT METADATA & TESTING NOTES

- Document Types Included: Contract, SLA, SOC 2, ISO 27001, GDPR
- Risk Posture: Mixed / Medium-High Risk
- Intended Use: Testing document classification, page-level evidence extraction, framework mapping, and risk scoring in RAG-based analyzers.