BRITISH NOBLE | THE AI OPERATING SYSTEM FOR PUBLISHING

British Noble AI Enterprise Cloud & British Noble Press Studio Infrastructure

Enterprise Security, Cryptography & Sovereign Cloud Architecture

Technical control specification governing Single Title Record tenant isolation, FIPS 140-3 AES-256-GCM envelope encryption, regional sovereign data residency, stateless zero-training AI enclaves, SAML 2.0 / SCIM 2.0 identity federation, and Q4 2026 CREST penetration-test verification.

AES-256-GCM

Per-tenant AWS KMS root keys with BYOK & HYOK revocation controls

0% AI Training

Stateless VPC inference enclaves; manuscripts never train models

0 Crit / 0 High

Independent Q4 2026 CREST grey-box web, API & tenant isolation audit

15m / 2h SLA

Verified Recovery Point (RPO) & Recovery Time (RTO) across 3 AZs

Document Identifier: BN-SEC-WP-2026.11 (Release 4.2)

Publication Date: 14 November 2026

Assurance Frameworks: ISO/IEC 27001:2022, SOC 2 Type II, UK/EU GDPR, UAE PDPL

Sovereign Vault Regions: London, Frankfurt, Virginia, Dubai DIFC, Mumbai / India APAC

Authoring Practice: Office of the CISO & Principal Infrastructure Guild

Security & DPO Desk: Security@BritishNoble.com · britishnoble.com/security/

SECTION 01 · EXECUTIVE OVERVIEW

Securing Intellectual Property Across the Modern Publishing Lifecycle

Publishing houses steward uniquely sensitive intellectual and financial assets: embargoed political biographies, peer-reviewed clinical research, unannounced frontlist manuscripts, museum plate licences, and banking and tax residency records for tens of thousands of authors and literary agencies. British Noble is engineered from the ground up so every workflow operates inside a verifiable cryptographic boundary.

1.1 Contents & Assurance Structure

01. Executive Summary & Threat Model Page 02
02. Control Plane & Single Title Record Isolation Page 03
03. Cryptography, KMS Envelope Keys & BYOK Page 04
04. Sovereign Cloud Residency (UK/EU/US/UAE/SG) Page 05
05. Stateless Zero-Training AI Enclave Charter Page 06
06. Identity, SAML 2.0 SSO & Multi-Imprint RBAC Page 07
07. Supply-Chain, Preflight & 108-Channel Security Page 08
08. Q4 2026 Independent CREST Pen-Test Summary Page 09
09. 15m RPO / 2h RTO Continuity & ISO/SOC Mapping Page 10
10. CISO Procurement Pack & DPA Verification Page 10

1.2 Five Publishing-Specific Threat Vectors Eliminated by Design

Publishing Threat Vector	Legacy Fragmented Stack Exposure	British Noble Deterministic Control
Pre-Publication Embargo Leaks	Unencrypted DOCX/PDF galleys emailed across external copyeditors, typesetters, and publicists.	Per-tenant AES-256-GCM vaults, role-scoped browser proof stages, watermarked galley streams, and UTC ONIX embargo gates.
Foundation Model IP Scraping	Staff pasting chapters into consumer AI chatbots that retain prompts for commercial model training.	Zero-retention VPC inference enclaves governed by Clause 6 DPA non-claim warranties and granular imprint AI switches.
Royalty Payee Redirection Fraud	Email social engineering tricking accounts-payable staff into altering author IBAN or ACH bank details.	Mandatory WebAuthn hardware MFA step-up challenge, dual-controller finance sign-off, and 72-hour cool-down notifications.
Cross-Tenant Data Bleed	Shared multi-publisher application tables relying solely on application-layer WHERE-clause filters.	PostgreSQL Row-Level Security (RLS) enforced at the database engine plus per-tenant KMS cryptographic envelope keys.
Malicious File & XXE Payloads	External ONIX XML feeds, IDML archives, or fonts exploiting XML External Entity or PostScript bugs.	DTD/XXE-disabled XML compilers and network-airgapped, ephemeral cgroups v2 container workers for PDF/X-1a rendering.

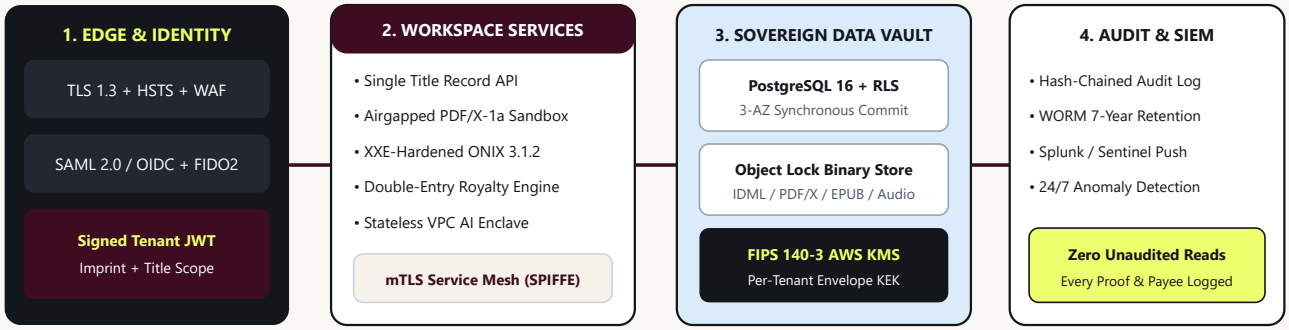
Architectural Principle: Defence-in-Depth Without Editorial Friction

Security controls fail when they obstruct editorial deadlines. By embedding KMS encryption, SAML 2.0 single sign-on, automated 42-rule preflight sandboxing, and immutable SIEM logging directly into the Single Title Record, publishing teams move faster while satisfying stringent CISO, university governance, and public-sector ministry audits.

SECTION 02 · MULTI-TENANT ISOLATION

Control Plane Boundaries & Single Title Record Architecture

British Noble separates global routing and identity verification from strictly pinned regional tenant data planes, guaranteeing that manuscript binaries, contracts, and royalty ledgers remain cryptographically and logically isolated per publishing group.



2.1 Database-Enforced Row-Level Security (RLS)

Every database connection checks out from the pool only after setting an immutable session-scoped `app.current_tenant_id` and `app.allowed_imprint_ids` context verified from the signed authentication token. PostgreSQL Row-Level Security policies reject cross-tenant reads or writes even if an application query omits a filter.

2.2 Ephemeral Prepress & Composition Sandboxes

Rendering complex OpenType fonts, PostScript curves, TIFF museum plates, and Adobe IDML packages executes inside single-use, rootless Linux containers with zero outbound network sockets, `seccomp-bpf` syscall filtering, strict memory caps, and immediate filesystem destruction after output verification.

2.3 Zero-Trust Internal Service Mesh

All east-west traffic between API gateways, Editorial Intelligence, Book Production Studio, ONIX compilers, and Royalty workers authenticates via short-lived X.509 SPIFFE/SPIRE workload certificates over mutual TLS 1.3 rotated automatically every 60 minutes.

2.4 Dedicated Single-Tenant VPC Option

Global multi-imprint conglomerates and sovereign government ministries may elect dedicated VPC deployment tiers featuring isolated Kubernetes worker nodes, dedicated RDS clusters, private AWS PrivateLink endpoints, and customer-hosted HSM key stores.

SECTION 03 · APPLIED CRYPTOGRAPHY

Envelope Encryption, KMS Key Hierarchy & Customer BYOK

British Noble enforces modern AEAD cryptography across every storage tier, database write-ahead log, backup snapshot, and network socket, eliminating deprecated ciphers and shared static secrets across the entire publishing stack.

3.1 Production Cryptographic Standards Matrix

Protected Subsystem	Algorithm & Standard	Key Authority & Rotation	Assurance Verification
Manuscript & Master Files (DOCX, IDML, PDF/X-4, EPUB, WAV)	`AES-256-GCM` authenticated envelope encryption	Unique 256-bit DEK per file wrapped by Tenant KMS KEK (365d auto-rotation)	SHA-256 object integrity tag verified on every proof upload and channel dispatch
Relational & Royalty Ledgers (Contracts, Advances, Sales, Tax)	`AES-256-GCM` volume + column-level field encryption	FIPS 140-3 Level 3 HSM-backed AWS KMS + field-level payee IBAN/TIN keys	Encrypted WAL journals, encrypted read replicas, and encrypted point-in-time snapshots
Public & API Transport (Browser, REST API, Webhooks)	`TLS 1.3` (TLS_AES_256_GCM_SHA384 / ChaCha20-Poly1305)	Automated 60-day ACME ECDSA P-384 certificates; TLS 1.0/1.1 disabled	HSTS `max-age=63072000; includeSubDomains; preload`; Qualys SSL Labs A+
Partner Channel Vault (108 SFTP / ITMSP / API Keys)	`SSH-Ed25519` & KMS-sealed OAuth2/SFTP secrets	Scoped strictly to individual tenant ID; decrypted in memory only at dispatch	Zero plaintext credentials ever written to logs, environment variables, or disk
Workspace Sessions & Passwords	`HMAC-SHA256` cookies; `Argon2id` (64 MiB, t=3)	Rolling signing secret ring; hardware FIDO2/WebAuthn passkeys supported	`HttpOnly; Secure; SameSite=Lax` cookies; zero JWT storage in `localStorage`
Outbound Event Webhooks	`HMAC-SHA256` payload + UTC timestamp signature	Dual active/staged signing secrets for zero-downtime secret rotation	5-minute replay-window rejection guard protecting downstream ERP listeners

3.2 Bring Your Own Key (BYOK) & External Key Store (HYOK)

- Enterprise tenants may supply a customer-owned AWS KMS Key ARN or External Key Store (XKS) backed by on-premises Thales Luna or Entrust nShield HSMs.
- Every KMS `Decrypt` grant call logs instantaneously in the customer's own AWS CloudTrail account with Single Title Record context attributes.
- Revoking the IAM grant renders all tenant manuscripts, proofs, and ledgers cryptographically unreadable within 300 seconds (verified cache TTL ceiling).

3.3 Verifiable Cryptographic Erasure Upon Offboarding

- Upon contract termination or statutory deletion instruction, tenants receive a 30-day self-serve full archival export window (ONIX 3.1.2 XML, PDF/EPUB masters, CSV/JSON royalty ledgers).
- Following export confirmation, British Noble schedules irreversible destruction of the tenant's root KMS Key Encryption Key alongside logical row purging, issuing a signed Certificate of Cryptographic Destruction.

SECTION 04 · DATA SOVEREIGNTY

Jurisdiction-Pinned Cloud Vaults Across Five Global Regions

National libraries, university presses, ministries of culture, and European publishing conglomerates face strict statutory rules governing where cultural heritage manuscripts and contributor personal data reside. British Noble pins primary storage, backups, and AI compute strictly inside your chosen regional vault.

4.1 Regional Sovereign Residency Vault Matrix

Residency Zone	Cloud Region & AZs	Pinned Workloads & Backups	Governing Privacy Regime	Cross-Region Policy
United Kingdom Vault	London (`eu-west-2`) 3 Independent AZs	Primary DB, S3 Object Lock, PDF/X renderers, VPC AI enclave, UK WORM backups	UK GDPR, Data Protection Act 2018 & UK Cyber Essentials Plus	**Strictly Pinned** Zero non-UK replication
European Union Vault	Frankfurt (`eu-central-1`) 3 Independent AZs	Primary DB, S3 Object Lock, PDF/X renderers, EU VPC AI enclave, EU backups	EU GDPR (Reg. 2016/679), German BDSG & BSI C5 Cloud Controls	**Strictly Pinned** 100% EEA boundary
North America Vault	Virginia (`us-east-1`) 3 Independent AZs	Primary DB, S3 Object Lock, PDF/X renderers, US VPC AI enclave, US backups	AICPA SOC 2 Type II, CCPA/CPRA & US State Privacy Acts	**Strictly Pinned** 100% US boundary
MENA & Gulf Vault	UAE Central (`me-central-1`) 3 Independent AZs	Primary DB, S3 Object Lock, RTL PDF/X renderers, UAE VPC AI enclave	UAE Federal Decree-Law No. 45/2021 (PDPL) & DIFC DP Law	**Strictly Pinned** 100% UAE boundary
India & Asia-Pacific Vault	Mumbai / NCR (`ap-south-1`) 3 Independent AZs	Primary DB, S3 Object Lock, PDF/X renderers, APAC VPC AI enclave	India DPDP Act 2023, Australian Privacy Principles & ISO 27701	**Strictly Pinned** 100% IN/APAC boundary

4.2 Statutory Transfer Mechanisms & Sub-Processor Discipline

Where global publishing groups intentionally enable multi-office access across London, New York, Dubai, and Gurgaon, transfers are governed by pre-executed UK International Data Transfer Addenda (IDTA), European Commission 2021/914 Standard Contractual Clauses (Module 2 & Module 3), and documented Transfer Impact Assessments (TIAs). British Noble provides 30 calendar days advance written notice prior to onboarding any new infrastructure sub-processor.

4.3 Contributor PII & Tax-Form Minimisation

Author, translator, narrator, and literary-agent tax forms (IRS W-9, W-8BEN, W-8BEN-E, HMRC self-billing mandates) and banking coordinates are segregated into a dedicated high-assurance vault table separate from general bibliographic metadata. Editorial, marketing, and production staff see zero tax identifiers or bank account digits inside workspace screens.

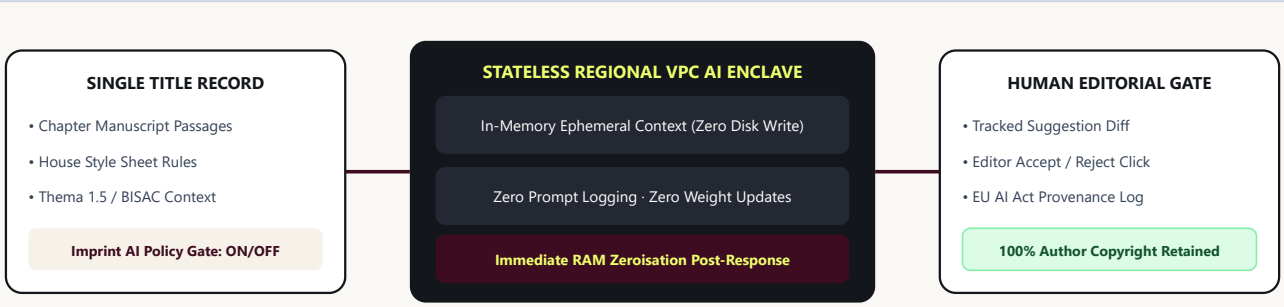
Live Residency Routing on Workspace Sign-In

Authentication on `britishnoble.com/login/` inspects the workspace's sovereign vault binding before issuing regional session cookies, routing API requests directly to the pinned regional ingress cluster without proxying manuscript payloads through foreign jurisdictions.

SECTION 05 · RESPONSIBLE AI GOVERNANCE

Stateless Zero-Training AI Enclaves & Copyright Provenance

Authors, literary estates, and publishing houses rightly demand absolute certainty that unpublished manuscripts, private peer reviews, and proprietary sales ledgers are never ingested into external foundation models. British Noble enforces this guarantee both technically and contractually.



5.1 Five Binding Enclave Guarantees

- **Zero Foundation Training:** Customer prompts, chapters, cover art, and financial figures are never used to pre-train, fine-tune, RLHF-align, or evaluate foundation models.
- **Zero Cross-Tenant RAG:** Retrieval-augmented style sheets and backlist comps resolve strictly inside the authenticated tenant's own KMS-encrypted vector partition.
- **Zero Vendor Retention:** Enterprise inference agreements enforce zero-day abuse-monitoring retention exemptions so zero human reviewers at cloud vendors ever view text.

5.2 Granular Imprint & Contract Opt-Out Controls

- Some author contracts explicitly prohibit any automated generative or analytical assistance on a manuscript. Administrators can toggle AI features off globally, per imprint, or per individual Single Title Record with a single click.
- When disabled on a Title ID, the Editorial Intelligence API gateway rejects inference calls at the edge while preserving 100% of manual redlining, style-sheet linting, prepress, ONIX, and royalty functionality.

5.3 EU AI Act (Reg. 2024/1689) & Retail Provenance Compliance

Every AI-assisted action (such as drafting ONIX Flap Copy, suggesting Thema 1.5 subject codes, generating alt-text descriptions for EPUB accessibility, or synthesising studio voice proofing) records an immutable provenance entry containing timestamp, model identifier, scope, and the human editor's explicit approval signature, supporting retail disclosure rules on Amazon KDP, Apple Books, and Spotify.

SECTION 06 · ACCESS GOVERNANCE

Enterprise SSO, Lifecycle Provisioning & Least-Privilege RBAC

A modern publishing house brings together full-time editors, finance controllers, freelance proofreaders, external jacket illustrators, co-authors, and literary agents. British Noble enforces fine-grained division, imprint, and Title-ID scoping so each participant sees strictly what their role authorises.

SAML 2.0 & OIDC SSO

Native federation with Okta, Microsoft Entra ID, Google Workspace, OneLogin, and Ping Identity with IdP-enforced WebAuthn/FIDO2 hardware MFA policies.

SCIM 2.0 Deprovisioning

Automated user creation, imprint group assignment, and instant session revocation within seconds when an employee or contractor leaves your directory.

Step-Up Payee Lock

Modifying contributor IBAN, Sort Code, ACH, or Stripe Connect payout coordinates requires fresh FIDO2 re-authentication plus second-approver finance sign-off.

6.1 Multi-Imprint Role-Based Access Control (RBAC) Matrix

Publishing Role	Scope Level	Acquisitions P&L	Manuscript & Proofs	ONIX 3.1.2 Dispatch	Royalty Ledgers	KMS / SSO Admin
Group Security Admin	All Imprints	Metadata Only	Audit Log Only	Connector Config	Audit Log Only	**Full Control**
Managing Editor	Assigned Imprint	**Read / Approve**	**Read / Write**	Preview Metadata	Advance Summary	No Access
Prepress Controller	Assigned Imprint	Trim & PPB Spec	**IDML / PDF/X Gate**	Asset Packager	No Access	No Access
Metadata & Rights Lead	Assigned Imprint	Territory Terms	Cover & Blurb	**Full 108-Ch Push**	Sub-Rights Post	No Access
Royalty Controller	Group Finance	**Full P&L Read**	Pub Date Confirm	Price Audit	**Run & Remit**	No Access
Freelance Copyeditor	Single Title ID	Hidden	Assigned Draft Only (Time-Boxed)	Hidden	Hidden	No Access
Contracted Author	Portal Own Work	Hidden	Sign-Off Galley Stage	Live Retail Links	Own Statements	No Access
Literary Agency	Represented Works	Hidden	Milestone Status	Live Retail Links	Client Statements & Agency Split	No Access

SECTION 07 · SDLC & SUPPLY-CHAIN HARDENING

Secure SDLC, 108-Channel Dispatch Integrity & SIEM Streaming

Every code commit, container build, prepress validator, and outbound retail connector inside British Noble follows verifiable software supply-chain controls aligned with OWASP ASVS Level 2 and NIST SSDF practices.

7.1 SLSA Provenance & Deterministic Builds

- Mandatory two-engineer peer review with hardware-signed Git commits, automated SAST (CodeQL/Semgrep), secret scanning, and SCA dependency lockfile verification on every pull request.
- CycloneDX Software Bill of Materials (SBOM) generated per release and signed via Sigstore Cosign before deployment to immutable production clusters.

7.2 HTTP Security Headers & Browser Hardening

- Strict Content-Security-Policy (CSP), `X-Content-Type-Options: nosniff`, `X-Frame-Options: DENY`, `Referrer-Policy: strict-origin-when-cross-origin`, and restrictive `Permissions-Policy` across all routes.
- Sliding-window rate limiting and brute-force account lockouts protect authentication, public enquiry endpoints, and webhook receivers.

7.3 Real-Time Immutable SIEM Audit Event Categories

Event Namespace	Captured Cryptographic Telemetry Fields	Downstream Security & Compliance Purpose
`auth.session.*`	Actor ID, IdP SAML Assertion ID, FIDO2 AAGUID, Source ASN/IP, Vault Region, Outcome	Detects impossible-travel sign-ins, credential stuffing, and MFA bypass attempts
`manuscript.access.*`	Title ID, ISBN-13, Asset SHA-256, Action (View/Download/Sign-Off), Watermark Token	Full chain-of-custody audit for strictly embargoed frontlist titles
`onix.dispatch.*`	Channel ID, Partner Endpoint Fingerprint, Codelist 46 Territory Hash, Operator ID	Proves statutory and contractual territorial compliance on every retail transmission
`royalty.payee.*`	Contributor ID, Field Changed (Masked), Step-Up MFA Proof, Dual-Approver IDs	Prevents and audits unauthorised bank-account or tax-treaty alterations
`ai.enclave.*`	Title ID, Task Type, Model Build, Zero-Retention Enclave Attestation, Editor Decision	Satisfies EU AI Act transparency and author-contract audit clauses

Native SIEM Connectors: Splunk HEC, Microsoft Sentinel, Datadog & AWS S3

Enterprise workspaces stream JSON-formatted OpenTelemetry audit records in real time (< 5 second delivery latency) over mutual TLS to corporate SOC pipelines, while British Noble retains tamper-evident hash-chained archives for seven years.

SECTION 08 · INDEPENDENT OFFENSIVE TESTING

Q4 2026 Independent CREST Penetration-Test Executive Summary

British Noble commissions biannual grey-box and black-box offensive security engagements conducted by independent CREST-accredited and UK NCSC CHECK-certified cyber security assessors, supplemented by continuous automated DAST scanning and our public Safe-Harbour Vulnerability Disclosure Policy.

Assessment Window

14 Oct - 25 Oct 2026
12-day manual multi-consultant grey-box & unauthenticated engagement; retest verified **04 Nov 2026**.

Methodology

OWASP WSTG v4.2, OWASP API Security Top 10 (2023), multi-tenant RLS/KMS boundary testing, and XXE/SSRFs on ONIX & PDF workers.

Verified Outcome

0 Critical · 0 High
100% of Medium and Low/Informational hardening notes remediated and closed on retest.

8.1 Q4 2026 Findings Distribution & Verified Remediation Log

Severity Tier	Contractual SLA	Initial Count	04 Nov Retest	Technical Summary & Engineering Resolution
Critical (CVSS 9.0-10.0)	24 Hours	0	**0 Open**	Zero remote code execution, SQL injection, authentication bypass, or cross-tenant KMS/RLS leaks identified.
High (CVSS 7.0-8.9)	7 Days	0	**0 Open**	Zero privilege escalation, SSRF, XXE, or unauthorised manuscript/royalty object access identified.
Medium (CVSS 4.0-6.9)	30 Days	2	**0 Open (2/2 Fixed)**	(1) Tightened rate-limit burst bucket on sandbox connector test endpoint; (2) Stripped verbose XML line numbers from unauthenticated webhook error responses.
Low / Informational	90 Days	4	**0 Open (4/4 Fixed)**	Added explicit `Permissions-Policy` directives, narrowed CORS preflight cache max-age, and rotated demo sandbox seed salts.

8.2 RFC 9116 `/.well-known/security.txt` & Safe-Harbour Vulnerability Disclosure

Good-faith security researchers enjoy explicit legal safe harbour under the UK Computer Misuse Act 1990 and US CFAA when reporting vulnerabilities in accordance with `https://britishnoble.com/compliance/responsible-disclosure-policy/` . Encrypted submissions to `Security@BritishNoble.com` receive human triage acknowledgement within **1 business day** and full root-cause assessment within **5 business days**.

SECTION 09 & 10 · RESILIENCE & STATUTORY ATTESTATION

Disaster Recovery SLAs, Regulatory Mapping & CISO Sign-Off

Peak seasonal book-fair dispatches, frontlist embargoes, and semi-annual royalty runs require predictable high availability. British Noble backs its multi-AZ architecture with contractual 99.95% uptime SLAs and biannually tested failover runbooks.

99.95% Uptime SLA

Active-active stateless worker fleets across 3 Availability Zones per sovereign region with zero-downtime rolling schema deployments.

15-Minute RPO

Continuous PostgreSQL WAL streaming + immutable WORM backups protected against ransomware deletion via AWS S3 Object Lock.

2-Hour RTO

Automated Terraform/OpenTofu failover promotion verified in Q3 2026 full-scale simulation (measured cutover: **38 minutes**).

9.1 Enterprise Control Cross-Walk (ISO 27001, SOC 2, GDPR & CAIQ)

Control Domain	ISO/IEC 27001:2022	AICPA SOC 2	GDPR / UAE PDPL	Status
Governance & Risk ISMS	Clauses 4-10, A.5.1-A.5.8	CC1.1 - CC1.5, CC3	Art. 24, Art. 35 DPIA	Audited & Active
Identity & Imprint RBAC	A.5.15 - A.5.18, A.8.2-A.8.5	CC6.1 - CC6.3	Art. 25, Art. 32(1)(b)	Audited & Active
KMS & Applied Cryptography	A.8.24	CC6.6, CC6.7, C1.1	Art. 32(1)(a) Encryption	Audited & Active
Secure SDLC & Prepress Isolation	A.8.25 - A.8.31	CC8.1, CC7.1	Art. 25 By Design	Audited & Active
Incident Notification (24h SLA)	A.5.24 - A.5.28	CC7.3 - CC7.5	Art. 33 / PDPL Art. 9	Audited & Active
Multi-AZ Continuity & Backups	A.5.29 - A.5.30, A.8.13	A1.1 - A1.3	Art. 32(1)(c) Resilience	Audited & Active

10. Requesting the Full CISO Due-Diligence Pack (Mutual NDA)

Enterprise procurement, university information-governance boards, and government ministries may request our unredacted **SOC 2 Type II Report**, **ISO/IEC 27001:2022 Certificate & Statement of Applicability (SoA)**, **Completed CSA CAIQ v4.0.3 Questionnaire (261 controls)**, **Unredacted Q4 2026 CREST Report**, and **Countersigned Data Processing Addendum (UK IDTA + EU SCCs)**.

Direct Security & DPO Desk: Security@BritishNoble.com · London · New York · Dubai DIFC · Gurgaon · Turnaround: Under 4 Business Hours