ABiAN

Security Whitepaper

How we protect client data, infrastructure, and identity.

Document version	v1.0 — Public release
Effective date	April 2026
Next review	April 2027 (or upon material change)
Owner	ABiAN — Information Security function
Classification	Public
Distribution	Prospects, clients, vendors, regulators

SIA ABiAN · Reg. 40103712521 · Tallinas 77, Rīga, LV-1009, Latvia
hello@abian.lv · +371 25443536 · abian.lv

© 2026 SIA ABiAN · Reg. 40103712521

Table of contents

© 2026 SIA ABiAN · Reg. 40103712521

1. About ABiAN

ABiAN is a security-first managed service provider headquartered in Rīga, Latvia, operating across the Baltics, the European Union, and Poland. We provide end-to-end IT management — identity, endpoint, cloud, network, and cybersecurity — to clients in regulated and security-sensitive sectors, including financial services, retail and industrial groups, and media.

Our operating model is deliberately narrow: we embed named engineers into client environments under a single contract, with shared risk registers and quarterly security reviews. We do not operate as a generalist reseller or a tier-1 ticket aggregator. This document describes the controls, processes, and evidence that underpin that model.

1.1 Legal entity

Registered name	SIA ABiAN
Registration number	40103712521 (Latvian Register of Enterprises)
Registered office	Tallinas 77, Rīga, LV-1009, Latvia
Primary jurisdiction	Republic of Latvia (EU member state)
VAT	LV40103712521
General contact	hello@abian.lv · +371 25443536
Security contact	security@abian.lv (recommended channel for vulnerability reports)

1.2 Scope of this document

This whitepaper describes ABiAN's information security posture as a service provider — the controls applied to ABiAN's own systems, personnel, and the infrastructure used to deliver services to clients. It does not describe controls inside any specific client tenant, which are governed by individual master service agreements (MSAs), data processing addenda (DPAs), and where relevant, sector-specific addenda such as DORA.

Where a client engagement is in scope of regulated frameworks (e.g., DORA for financial entities, NIS2 for essential and important entities), additional contractual commitments, evidence packs, and audit rights apply. This document is the public-facing baseline; client-specific evidence is provided under NDA on request.

2. Frameworks and Governance

2.1 Reference frameworks

ABiAN's information security management is structured around the following frameworks. We do not claim certifications we do not hold; the table below states our current alignment posture honestly.

Framework	Posture	Notes
ISO/IEC 27001:2022	Aligned (Annex A controls)	Internal ISMS structured around Annex A. Certification roadmap on file; engaged with certification body planned for FY2026–2027.
NIS2 (Directive (EU) 2022/2555)	Operationally aligned	ABiAN supports clients classified as essential or important entities; internal controls cover the technical and organisational measures listed in Article 21.
DORA (Regulation (EU) 2022/2554)	ICT third-party provider commitments	For financial-entity clients, ABiAN executes DORA addenda covering ICT risk management, incident reporting, exit strategies, and concentration risk disclosures.
GDPR (Regulation (EU) 2016/679)	Compliant	ABiAN acts as data processor for client data and as data controller for ABiAN's own personnel and prospect data. DPA template available.
CIS Controls v8	Reference	Used as the operational checklist when designing controls for client endpoints, identity, and network configurations.
Microsoft Cloud Security Benchmark	Reference	Default baseline for Azure landing zones we design and operate.

2.2 Information Security Management System (ISMS)

ABiAN maintains an ISMS aligned to ISO/IEC 27001:2022. The ISMS comprises:

- A documented Information Security Policy approved by management and reviewed annually.
- Topical policies covering acceptable use, access control, cryptography, supplier security, secure development, incident response, business continuity, and data protection.
- A risk register reviewed quarterly, with risks scored on likelihood and impact and tied to identified treatment plans.
- A Statement of Applicability (SoA) that maps ISO 27001:2022 Annex A controls (93 controls across organisational, people, physical, and technological themes) to ABiAN's implementation.
- Internal review cycles, with management review held at least annually.

© 2026 SIA ABiAN · Reg. 40103712521

The ISMS scope covers all ABiAN personnel, all internal systems used to deliver client services, and all ABiAN-managed infrastructure used to operate client environments. Client-owned systems remain in scope of the client's ISMS.

2.3 Roles and responsibilities

Role	Responsibility
Management Board	Ultimate accountability for information security; approves policies and budget; reviews material risks at least quarterly.
Information Security function	Owns the ISMS, risk register, vendor reviews, incident response coordination, and security training programme.
Engineering leads	Implement controls in client environments; participate in design reviews; sign off on changes affecting security posture.
Data Protection contact	Handles GDPR data subject requests, supervisory-authority correspondence, and DPIA support for client engagements.
All personnel	Bound by acceptable-use policy, NDAs, and the duty to report incidents and suspected events without delay.

3. How We Access Client Environments

Privileged access into client tenants is the most sensitive surface in any MSP relationship. ABiAN treats it as such. The model below applies by default; client-specific deviations are documented in the engagement runbook.

3.1 Identity and access principles

- Named engineers, not shared accounts. Each engineer has an individual identity in the client tenant; shared admin accounts are not used.
- Just-in-time elevation. Standing privileged roles are minimised. Where the platform supports it (Microsoft Entra PIM, Azure RBAC eligible assignments), elevation is time-bound, reason-tagged, and approver-gated.
- Phishing-resistant MFA. All ABiAN engineers authenticate with FIDO2 / Windows Hello for Business or, where unavailable, Microsoft Authenticator with number matching. SMS and voice-call factors are not used.
- Conditional Access enforcement. Access from ABiAN to client tenants requires a compliant, ABiAN-managed device on a trusted location, with risk-based sign-in evaluation.
- Least privilege by role. Engineers are assigned the narrowest role that lets them complete the work. Global Administrator-equivalent roles are reserved for break-glass and emergency change scenarios.
- Break-glass accounts. Emergency accounts in client tenants are stored in a sealed, monitored vault, excluded from Conditional Access policies that could lock out, and logged on every use.

3.2 Privileged Access Management

ABiAN distinguishes between Privileged Identity Management (PIM) — governing who can elevate to a privileged role and under what conditions — and Privileged Access Management (PAM) — governing the session itself once elevated.

- PIM. Microsoft Entra PIM is the default for Microsoft 365 and Azure environments. Eligibility, activation duration, approval requirement, and MFA-on-activation are all enforced.
- PAM. Where supported, sessions are launched from hardened administrative workstations or via session brokering; session activity is logged.
- Audit trail. Activations, approvals, and privileged actions are logged in the client tenant and retained according to the client's retention policy.

3.3 Joiner / Mover / Leaver

Engineer access lifecycle into client tenants is governed by a documented Joiner / Mover / Leaver (JML) process:

- Joiner. Access is provisioned only after onboarding training, NDA execution, and explicit assignment to the client engagement. Default state is no access.

© 2026 SIA ABiAN · Reg. 40103712521

- Mover. When an engineer rotates off an engagement, client-tenant access is removed within one business day.
- Leaver. On termination, all client-tenant access is revoked the same day; ABiAN-internal access is revoked immediately on termination of the employment or contractor relationship.
- Quarterly access reviews. Engineering leads attest to the appropriateness of standing access for each engagement at least once per quarter.

4. ABiAN's Own Security Posture

Engineer endpoints are an attack path into every client environment. ABiAN's own posture is therefore treated as part of the client attack surface, not as a separate concern.

4.1 Endpoint security

Control	Implementation
Device management	All ABiAN endpoints are enrolled in Microsoft Intune (or Jamf for macOS where applicable) and marked as compliant before access to corporate or client resources is granted.
Disk encryption	BitLocker (Windows) and FileVault (macOS) are enforced on all endpoints, with recovery keys escrowed in the management plane.
EDR / XDR	Endpoint Detection and Response is deployed on every endpoint (Microsoft Defender for Endpoint and/or Sophos Intercept X, depending on platform).
Patching	Operating system and third-party application patches are deployed on a defined cadence: critical within 7 days, high within 14 days, others within 30 days.
Local admin	Engineers do not hold permanent local administrator rights on their primary endpoint. Elevation is on-demand and audited.
Browser hardening	Managed browser profiles, controlled extension lists, and DNS filtering applied via the management plane.
Removable media	USB mass-storage write access is disabled by default; exceptions are policy-driven and logged.

4.2 Identity

ABiAN's corporate identity is provided by Microsoft Entra ID (tenant: abian.lv). The following controls apply:

- MFA enforced for all users on all sign-ins, with phishing-resistant factors as the primary method.
- Conditional Access policies require compliant device, restrict legacy authentication protocols, and apply session controls for privileged roles.
- Self-service password reset is enabled with strong proof-of-identity steps; passwords meet entropy requirements aligned to NIST SP 800-63B.
- Privileged roles are activated through Entra PIM, time-bound, and require justification.
- Sign-in and audit logs are retained and forwarded to a central log store for monitoring and incident response.

4.3 Network

- Engineers connect to client environments either through the client's sanctioned remote access (Entra Private Access, ZTNA, or VPN) or via management workstations on hardened network segments.
- ABiAN's office and remote-work network access is gated through identity- and device-aware controls; flat-network access to production tooling is not used.
- DNS filtering is applied at the endpoint to block known-malicious and high-risk categories.

4.4 Email and collaboration

- Microsoft Defender for Office 365 provides anti-phishing, anti-malware, and Safe Links / Safe Attachments protection across email.
- Domain authentication is enforced: SPF, DKIM, and DMARC at p=reject for ABiAN-owned sending domains.
- External-sender warnings are applied; impersonation protection covers the leadership team and high-risk roles.

4.5 Vulnerability management

- Continuous vulnerability assessment runs against ABiAN endpoints and internet-exposed systems.
- Findings are tracked in the security backlog, prioritised by CVSS and exploitability, and remediated against the patching SLAs above.
- External attack-surface reviews are conducted at least annually for ABiAN-operated public-facing assets.

© 2026 SIA ABiAN · Reg. 40103712521

5. Data Handling and Residency

5.1 Roles under GDPR

In the typical client engagement, ABiAN acts as a data processor for personal data contained in the client's tenant or systems we operate, and as a data controller for personnel data, prospect data, and operational data we collect for our own purposes. Each client engagement is governed by a Data Processing Addendum (DPA) executed alongside the master agreement.

5.2 Data residency

- Default storage location for client tenant data is the European Union, typically EU North (Ireland), EU West (Netherlands), or Sweden Central, selected based on latency and regulatory preference.
- Where a client requires Latvian or Baltic residency, services are configured accordingly; this is documented in the engagement design.
- ABiAN does not transfer client personal data outside the EU/EEA unless the client explicitly approves a transfer mechanism (Standard Contractual Clauses, adequacy decision) and the transfer is documented in the records of processing.

5.3 Encryption

Data state	Standard
In transit	TLS 1.2 minimum, TLS 1.3 preferred. Legacy protocols (TLS 1.0/1.1, SSL) are disabled on systems we operate. Modern cipher suites only.
At rest (cloud)	AES-256 by default via platform-managed keys (Azure Storage Service Encryption, M365 service encryption). Customer-managed keys (CMK) supported via Azure Key Vault on request.
At rest (endpoint)	BitLocker (Windows) / FileVault (macOS) — full-disk encryption with TPM-backed keys.
Secrets	Stored in Azure Key Vault or equivalent enterprise secrets manager. Plaintext secrets are not stored in source repositories, configuration files, or ticket systems.

5.4 Retention and deletion

- Operational logs (sign-in, audit, security telemetry) are retained for the period required by the client's policy or by regulation, whichever is longer; default is 12 months for security-relevant logs.
- Ticket and engagement records are retained for the duration of the engagement plus the period required by Latvian commercial and accounting law.
- On termination of an engagement, client data in ABiAN-controlled systems is returned and/or deleted per the DPA, with a written confirmation of deletion provided on request.

© 2026 SIA ABiAN · Reg. 40103712521

- Deletion from cloud services follows the underlying platform's deletion timelines (e.g., Microsoft 365 service-specific recycle and purge windows).

5.5 Data minimisation

ABiAN collects only the data required to deliver the contracted service. Client end-user personal data is processed only where necessary for support (e.g., verifying the identity of a caller) and is not retained beyond the support transaction unless the client requires it.

© 2026 SIA ABiAN · Reg. 40103712521

6. Monitoring and Incident Response

6.1 Monitoring

- Identity and sign-in telemetry from ABiAN's tenant and from client tenants we operate is centrally monitored, with alerting on impossible-travel, anomalous sign-in, and privileged-role activation events.
- Endpoint telemetry (EDR) is monitored on a 24/7 basis; high-severity detections are triaged on-call.
- Cloud platform alerts (Azure Defender, Microsoft Defender for Cloud, equivalent) are routed into the incident pipeline.
- Public-facing assets are monitored for availability and security headers; certificate expiry is tracked.

6.2 Incident response process

ABiAN follows a documented incident response process aligned to NIST SP 800-61r2:

- Preparation. Runbooks per engagement; on-call rotation; contact tree and escalation paths defined and tested.
- Detection and analysis. Triage by severity using a documented matrix; severity drives notification timelines.
- Containment, eradication, recovery. Containment actions are taken in line with client-approved playbooks; eradication and recovery follow.
- Post-incident. Root cause analysis, lessons learned, and corrective actions are documented and shared with the client.

6.3 Severity definitions

Severity	Definition	Response time	Initial client notification
P1	Confirmed compromise, active data exfiltration, or critical service unavailability.	Immediate (24/7)	Within 1 hour of confirmation.
P2	High-severity detection requiring containment; partial service degradation.	Within 1 hour	Within 4 hours of confirmation.
P3	Suspicious activity warranting investigation; minor degradation.	Within 4 business hours	Within 1 business day or in the next service report.
P4	Informational; tuning, hygiene, or low-impact items.	Next business day	Reported in the standard service review.

© 2026 SIA ABiAN · Reg. 40103712521

6.4 Breach notification

- Where ABiAN, acting as processor, becomes aware of a personal data breach affecting client data, the client (as controller) is notified without undue delay and in any case within 24 hours of confirmation.
- For financial-entity clients, ABiAN supports DORA major incident reporting timelines (initial, intermediate, and final reports) per Article 19 of DORA and the related RTS.
- For NIS2 clients, ABiAN supports the 24-hour early warning, 72-hour incident notification, and one-month final report timelines under Article 23.
- Notification content includes the nature of the incident, categories and approximate volume of data subjects and records affected (where known), likely consequences, and measures taken or proposed.

6.5 Forensic readiness

- ABiAN preserves logs and artefacts relevant to security incidents in accordance with the engagement's retention policy.
- Where an incident may give rise to legal proceedings, ABiAN coordinates with the client's legal function and, if requested, an external forensic provider, to preserve chain of custody.

© 2026 SIA ABiAN · Reg. 40103712521

7. Business Continuity and Disaster Recovery

7.1 ABiAN operational continuity

ABiAN maintains a Business Continuity Plan (BCP) covering personnel availability, communication channels, and tooling redundancy. Engineers can deliver services from any location with conformant equipment and connectivity; ABiAN is not single-site-dependent.

- Critical internal systems (identity, ticketing, monitoring, RMM) are SaaS-based with vendor-side redundancy.
- Out-of-band communication channels are maintained for use during a primary-channel outage.
- The BCP is reviewed at least annually and tested through tabletop exercises.

7.2 Client-environment recovery

Disaster recovery for client environments is engineered per engagement against client-approved Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO). Defaults that we propose where the client has no prior position:

Workload class	Default RPO	Default RTO
Tier 1 — business-critical (e.g., core banking, payment, e-commerce)	≤ 15 minutes	≤ 4 hours
Tier 2 — important productivity (e.g., M365, ERP)	≤ 1 hour	≤ 8 hours
Tier 3 — supporting (e.g., archive, file shares)	≤ 24 hours	≤ 2 business days

7.3 Backup posture

- Backups are taken in line with workload tier, with at least one logically isolated copy.
- Restore tests are conducted on a defined cadence (Tier 1 quarterly, Tier 2 semi-annually, Tier 3 annually) with results recorded.
- Backup encryption keys are managed separately from production identity to limit blast radius from credential compromise.

© 2026 SIA ABiAN · Reg. 40103712521

8. Personnel Security

8.1 Hiring

- Background verification is performed on all personnel prior to access to client environments, in accordance with Latvian labour law and proportionate to the role's risk profile. Verification typically includes identity, employment history, and education.
- Roles with access to financial-entity client tenants are subject to enhanced verification, including criminal-record checks where lawful and appropriate.

8.2 Confidentiality and acceptable use

- All personnel sign confidentiality undertakings as part of their employment or contractor agreement. These survive termination.
- Acceptable Use Policy and Information Security Policy acknowledgement are required at hire and on material policy revision.

8.3 Training

- All personnel complete security awareness training at hire and at least annually thereafter.
- Phishing simulation is run on a regular cadence; results inform further training.
- Engineers receive role-specific training (Azure security, identity, EDR tooling) and maintain relevant vendor certifications where applicable.

8.4 Termination and offboarding

- On termination, all access is revoked the same day. Equipment is returned and wiped under a documented procedure.
- A formal offboarding checklist captures account closure, key recovery, and client-engagement handover.

8.5 Subcontractors and contractors

- Subcontractors used to deliver services are subject to written agreements requiring security and data-protection commitments at least equivalent to those ABiAN has accepted to the client.
- Subcontractor lists are disclosed to clients on request and updated when material changes occur. Where a DPA requires prior consent for sub-processor changes, the client's consent process is followed.

© 2026 SIA ABiAN · Reg. 40103712521

9. Sub-processors and Supply Chain

ABiAN relies on a defined set of vendors to deliver services. The list below identifies the principal categories. Engagement-specific sub-processor lists are provided in the DPA on request.

Category	Principal vendor(s)	Purpose
Cloud platform	Microsoft Azure, Microsoft 365	Identity, productivity, infrastructure, data services for ABiAN and client environments.
Endpoint security	Microsoft Defender, Sophos	EDR/XDR, anti-malware, encryption management.
RMM and PSA	Datto RMM, Autotask	Endpoint management, monitoring, ticketing, billing.
Distribution	Pax8	Microsoft and third-party software licensing distribution; commercial integration only — no client tenant data flows to Pax8.
ITSM / collaboration	ClickUp, Atlassian (Jira/Confluence)	Internal task and incident management; client-specific tenants where contracted.
Data protection	Microsoft Purview	DLP, information protection, audit, eDiscovery for client tenants.

9.1 Vendor due diligence

- New vendors are reviewed against a documented checklist covering security certifications, data residency, breach history, sub-processor disclosures, and contractual commitments.
- Reviews are repeated at material change and at least every 24 months for vendors that process client data.

9.2 Concentration risk

ABiAN acknowledges that its primary cloud platform (Microsoft) is concentrated. For financial-entity clients, this is reflected in DORA disclosures and exit-strategy documentation. Where mitigations are practical (parallel toolchains, exportable backups, alternative communication channels), they are documented.

© 2026 SIA ABiAN · Reg. 40103712521

10. Audit and Evidence

10.1 Available on request (under NDA)

- ISMS policy summary and Statement of Applicability.
- Penetration test executive summaries and remediation status (annual).
- Internal vulnerability scan summaries.
- Service-organisation reports for upstream vendors (e.g., Microsoft, Sophos, Datto), where the vendor licenses them for redistribution.
- DPIA support documentation for ABiAN-delivered services.
- Sub-processor list specific to the engagement.
- Insurance certificates (professional indemnity, cyber).

10.2 Audit rights

Clients with a written master agreement and DPA in force may exercise audit rights as agreed in the relevant contract. ABiAN supports proportionate audit approaches:

- Documentation review (default).
- Questionnaire-based assurance (CAIQ, SIG, or client-specific).
- On-site or remote interview-based review by client or agreed third party, on reasonable notice.
- For financial-entity clients, the DORA addendum provides for the audit, inspection, and access rights required by Article 30.

10.3 Regulator cooperation

- ABiAN cooperates with competent supervisory authorities where required by law, including Latvian Data State Inspectorate (DVI), the Bank of Latvia, and equivalent authorities in other Member States where ABiAN delivers services.
- Lawful access requests from authorities are reviewed by counsel before any data is disclosed; clients are notified to the extent permitted by law.

© 2026 SIA ABiAN · Reg. 40103712521

11. Responsible Disclosure

ABiAN welcomes good-faith security research on systems we operate. Researchers acting in accordance with this policy will not be subject to legal action by ABiAN for their research.

11.1 Scope

- ABiAN-operated public-facing systems on abian.lv, abian.it, and abian.ai domains.
- Out of scope: client systems unless specifically delegated; third-party SaaS used by ABiAN (report to the vendor); social engineering of personnel; physical attacks; denial-of-service tests.

11.2 How to report

- Email security@abian.lv with a clear description, reproduction steps, and any supporting artefacts. Encrypt sensitive details with our PGP key (published at abian.lv/.well-known/security.txt).
- ABiAN will acknowledge receipt within 3 business days and provide a status update within 10 business days.
- We ask researchers not to publicly disclose findings until we have had a reasonable opportunity to remediate; we will agree a coordinated disclosure timeline.

11.3 Safe harbour

- Researchers must avoid privacy violations, service disruption, and destruction of data.
- Testing is limited to accounts the researcher owns or has explicit written permission to test.
- Findings must be reported promptly and not exploited beyond what is necessary to demonstrate the vulnerability.

© 2026 SIA ABiAN · Reg. 40103712521

12. Contact

General enquiries	hello@abian.lv · +371 25443536
Security and vulnerability reports	security@abian.lv · abian.lv/.well-known/security.txt
Data protection enquiries	privacy@abian.lv · GDPR / DPA matters
Procurement and due diligence	hello@abian.lv · questionnaires accepted in CAIQ, SIG, or client format
Postal address	SIA ABiAN, Tallinas 77, Rīga, LV-1009, Latvia

Document control

Version	Date	Author	Summary of change
1.0	April 2026	Eduards Harčuks	Initial public release.

Disclaimer. *This whitepaper describes ABiAN's general security posture and is provided for informational purposes. It does not form part of any contract unless expressly incorporated. Specific commitments to clients are made in the master service agreement, data processing addendum, and any sector-specific addenda (e.g., DORA addendum). In the event of conflict, the contract prevails.*

© 2026 SIA ABiAN · Reg. 40103712521