PRIVION

Trust Center

Security Documentation

Comprehensive public summaries: trust boundaries, security controls, compliance posture, security policies, subprocessors, and incident response.

Privion · Effective May 22, 2026 · 1.0 (public summary)

security@priviontech.com · priviontech.com/trust

Overview

Privion helps organizations modernize Microsoft 365 environments and operates hosted services (Privion Intranet and PAnalytics). This document mirrors the public Trust Center at https://priviontech.com/trust as of May 22, 2026.

Trust boundaries

Client tenant — Where most of your data lives

Microsoft 365 / SharePoint / Power Platform consulting. Data remains in your Microsoft 365 tenant. Privion does not store, copy, or relocate client content for this work.

Privion infrastructure — Hosted services Privion operates

Privion Intranet. Privion-managed Azure (Azure West US 2). Privion Intranet processes documents into structured outputs via cloud AI services. Privion's processing methodology is proprietary and is not disclosed publicly to protect competitive advantage. Privion acts as data processor where processing occurs in the service. Data handling: encrypted transit, post-delivery deletion of documents and intermediate artifacts, no training re-use.

PAnalytics (Privion-hosted Matomo). PAnalytics is Privion-hosted Matomo on a shared Privion-managed Azure stack (Azure West US 2). Clients may instead deploy Matomo in their own environment. Privion acts as data processor for visitor analytics collected on clients' websites when the hosted service is in use.

- For consulting work, client Microsoft 365 data stays in the client's tenant. Privion's risk surface is privileged access, not data custodianship.
- For Privion Intranet and PAnalytics, Privion is the data processor. Controls for those environments are described on this Trust Center.
- Privion's SOC 2 scope (when in scope) is intended to cover hosted services and the privileged-access program for client tenants — not the client tenants themselves.

Security controls

Privileged Access Management

- MFA required for all personnel and admin accounts
- FIDO2 for tenant-admin operations
- Entra PIM for just-in-time elevation
- GDAP partner access (no standing Global Admin)
- Conditional Access on admin accounts
- Quarterly client tenant access reviews
- GDAP/PIM recovery playbooks; annual review

Data Protection

- TLS 1.2+ in transit
- Encryption at rest (Azure defaults)

- Privion Intranet: proprietary methodology; encrypted transit; no persistent store after delivery; no training re-use; DPA/NDA for specifics.
- Nightly MySQL dumps to Azure Blob Storage in Azure West Central US (30-day retention).
- Secure disposal at engagement end
- No client data on Privion endpoints for tenant-based consulting

Infrastructure Security

- Azure West US 2 for Privion Intranet and PAnalytics
- Privion Intranet: no persistent client content after delivery

Endpoint & Personnel

- MFA required for all Privion personnel and administrative accounts
- Company-managed devices used for client tenant and infrastructure administration: full-disk encryption, current OS security updates, and host firewall enabled
- Infrastructure and privileged access via SSH keys and MFA; password-only remote administrative access is not permitted
- Conditional Access policies require managed devices for Microsoft 365 and client tenant administrative work
- Microsoft Intune and Microsoft Defender for Endpoint — phased deployment through 2026 for centralized endpoint management and monitoring
- Background checks (FCRA-compliant vendor) for all Privion personnel with client or infrastructure access, including criminal history, employment verification, and adverse media screening where permitted by law.
- Annual security awareness training covering phishing, data classification, incident reporting, and GDPR/CCPA fundamentals. Completion is tracked; evidence available upon request.

Compliance and certifications

Privion's SOC 2 scope is intended to cover (1) the Privion Intranet hosted service, (2) the PAnalytics hosted service, and (3) the privileged-access program by which Privion personnel access client Microsoft 365 tenants. It does not cover client tenants themselves, which remain the client's responsibility.

SOC 2 Type 1 — Roadmap. Target Q4 2026. Readiness program and control mapping in progress.

SOC 2 Type 2 — Roadmap. Target Q3 2027. Readiness program and control mapping in progress.

NIST CSF — Aligned. Self-assessment mapping of security program controls to NIST Cybersecurity Framework functions (Identify, Protect, Detect, Respond, Recover), maintained as part of Privion's SOC 2 readiness program. Detailed mapping available under NDA — not a third-party NIST certification.

GDPR — Available. PAnalytics can be configured for GDPR-aligned processing; Data Processing Agreement available on request

CCPA — Available. Data Processing Agreement available on request for applicable engagements

ISO 27001 — Roadmap. Planned after SOC 2 program maturity

Microsoft AI Cloud Partner Program — Active. Microsoft AI Cloud Partner Program designation

Penetration testing — Roadmap. Organization-wide penetration testing planned for 2027. PAnalytics is built on Matomo; see Matomo published security assessments at matomo.org/security and Privion operational controls on the Trust Center.

Hosted service infrastructure (PAnalytics)

PAnalytics is deployed in Azure West US 2 on Azure Linux App Service with private MySQL Flexible Server connectivity, Key Vault for secrets, and platform monitoring.

- Linux App Service (containerized Matomo), HTTPS-only public endpoint
- Azure Database for MySQL — Flexible Server (private VNet integration)
- Azure Files (Standard LRS) for configuration and custom plugins
- Azure Key Vault for database credentials (user-assigned managed identity)
- Azure Monitor — Application Insights and Log Analytics (platform telemetry)

Nightly MySQL dumps to Azure Blob Storage in Azure West Central US (30-day retention).

PAnalytics is Privion-hosted Matomo on a shared Privion-managed Azure stack (Azure West US 2). Clients may instead deploy Matomo in their own environment.

Privion acts as data processor for visitor analytics collected on clients' websites when the hosted service is in use.

Backup and disaster recovery (implemented):

• Automated nightly MySQL logical backups (mysqldump) from Azure Database for MySQL Flexible Server

• Cross-region copy to Azure Blob Storage in Azure West Central US (30-day retention; lifecycle-managed)

• Documented restore procedure (provision recovery-region MySQL Flexible Server in Azure West Central US and replay latest dump)

• Quarterly recovery test per documented procedure

• RTO/RPO targets available on request

Privion Intranet

Privion Intranet processes documents into structured outputs via cloud AI services. Privion's processing methodology is proprietary and is not disclosed publicly to protect competitive advantage.

- Documents are transmitted to processing infrastructure via encrypted channels.
- Results are returned to the client and made available for download.
- Documents and intermediate processing artifacts are not retained persistently on Privion infrastructure after delivery.
- No training data re-use: client data is not used to improve Privion products or third-party model services.
- For detailed data residency and processing specifics, see the Data Processing Agreement (available under NDA).

PAnalytics security posture

PAnalytics is a Privion-managed offering built on Matomo. Platform risk and operational risk are addressed separately below.

- Deployed on Privion-managed Azure infrastructure (Azure West US 2).
- Built on Matomo, an open-source platform with published security assessments at matomo.org/security.
- Privion manages network isolation, access controls, patch management, and compliance-oriented configuration for hosted deployments. Nightly MySQL dumps are replicated to Azure Blob Storage in a secondary region (30-day retention) with a documented restore path.
- Clients may deploy Matomo in their own environment to eliminate Privion's processor role for visitor data.

Privileged-access recovery

Privion maintains documented records of GDAP relationships, PIM role assignments, and partner access procedures to re-establish client tenant administration after disruption.

Recovery playbooks cover partner center unavailability, compromised administrative accounts, and client offboarding.

Procedures are reviewed at least annually; exercise and test evidence available under NDA.

Verifying controls

Privion SOC 2 Type 1 (target Q4 2026) and Type 2 (target Q3 2027) reports will be available under NDA upon request when issued. Until then, customers may download the SOC 2 readiness report and management attestation letter (management self-assessment against AICPA Trust Services Criteria — not an audited SOC 2 report), request NIST Cybersecurity Framework mapping, or contact security@priviontech.com for additional evidence.

DPA summary

Privion provides Data Processing Agreements for hosted services and applicable consulting engagements. Executed terms govern; this summary helps procurement teams understand typical commitments.

Roles — Defines controller/processor roles; client Microsoft 365 tenants remain under client control for consulting workloads.

Data residency — Hosted services (Privion Intranet and PAnalytics) run in United States regions unless otherwise agreed; subprocessors listed on the Trust Center.

Subprocessors — 30 days' notice before adding or changing subprocessors that process client personal data; list published at priviontech.com/trust/subprocessors.

Security — Technical and organizational measures aligned with the Trust Center and SOC 2 readiness program.

Breach notification — Processor notification commitments aligned with applicable law and contract (including GDPR-aligned timelines where required).

Audit rights — Customers may request SOC 2 reports, readiness summaries, and security documentation under NDA as the audit program matures.

Security policies

The following are public summaries. Policy owner: Privion security program. Review frequency: Annual.

Information Security Policy

Purpose, authorized use, system-owner duties, governance, and links to subsidiary policies for Privion Intranet and PAnalytics, and consulting access.

This policy describes how Privion protects and manages information assets for Privion, its clients, partners, and the public. It guides Privion personnel, contractors, and other authorized users in the responsible handling, use, and disposal of information within a secure environment.

This public summary supports procurement and security reviews. The complete policy document, including operational procedures and evidence references, is available under NDA.

1. Purpose

Privion is committed to the following security objectives:

- Protect information against unauthorized access, disclosure, and misuse.
- Maintain confidentiality of sensitive information for those with proper authorization.
- Preserve integrity and accuracy of information used in service delivery.
- Maintain availability of information and systems needed for operations.
- Support business continuity for Privion Intranet and PAnalytics, and consulting delivery.
- Meet applicable regulatory, contractual, and legal obligations.
- Maintain physical, logical, and communications security across platforms Privion operates.
- Require reporting and investigation of information security incidents through defined channels.
- Dispose of information that is no longer required in a secure and appropriate manner.

Applicability

This policy applies to all forms of information Privion processes, including electronic systems (software, cloud services, and endpoints), Privion networks and data stores, paper records where used, and information handled when Privion personnel access client Microsoft 365 tenants under engagement terms.

The program covers Privion Intranet and PAnalytics (hosted in Azure West US 2), Privion corporate systems, and partner-delegated administrative access to client tenants. Client Microsoft 365 tenants remain under client control; Privion's obligations in those environments focus on how Privion personnel access and operate within them.

2. Information security requirements

All authorized users must exercise a duty of care when operating Privion information systems so that confidentiality, integrity, and availability are preserved.

2.1 Authorized users

Only individuals formally authorized by Privion — employees, contractors, or partners with a documented need — may access Privion information systems. Authorization is granted by management with security program oversight.

Each authorized user receives a unique identity. Passwords, keys, and other credentials must remain confidential and must not be shared. Privion requires multi-factor authentication for personnel and administrative accounts; FIDO2 hardware keys are required for tenant-admin operations.

- Confidential, personal, or sensitive information must not be copied, transferred, or stored outside approved systems without authorization from the information owner or engagement lead.
- Before transporting information, users must assess risks such as loss or unauthorized access in transit and at the destination.
- Encryption and other approved protections must be used when moving or storing sensitive data outside primary systems.
- Consulting work is performed in client Microsoft 365 tenants where practicable; client content is not stored on Privion endpoints for that work.

2.2 Acceptable use

Authorized users must use Privion systems lawfully, ethically, and for legitimate business purposes. Use must respect the rights of others and align with Privion values and subsidiary policies.

- Activities must support authorized engagements and must not infringe on client or Privion rights.
- Users must not abuse resources through excessive consumption, unauthorized software, or illegal activity.
- Users must not share credentials, circumvent security controls, or use client environments for non-engagement purposes.

Acceptable Use Policy — Detailed rules for Privion systems and client tenant access. (https://priviontech.com/trust/policies/acceptable-use/)

Access Control Policy — MFA, GDAP, PIM, and access lifecycle requirements. (https://priviontech.com/trust/policies/access-control/)

2.3 Information system owners

Information system owners, under security program guidance, are responsible for the security and effective management of systems in their scope. For hosted services, this includes Privion Intranet and PAnalytics on Privion-managed Azure infrastructure.

- Access control: Protect systems against unauthorized access through least privilege, MFA, and periodic access reviews.
- Physical and logical security: Protect systems against theft, damage, and misuse using cost-effective controls appropriate to the environment.
- Business continuity: Maintain and test continuity and recovery plans for critical hosted services.
- Backup and recovery: Nightly MySQL dumps to Azure Blob Storage in Azure West Central US (30-day retention). Documented restore procedure; quarterly recovery test per documented procedure.
- Data accuracy: Maintain reliable configuration and operational data for hosted services.
- Proper usage: Ensure systems are used only for intended purposes; address misuse promptly.

- Retention: Retain logs and records only as long as required for operations, law, or contract, then dispose securely.
- Third parties: Ensure subprocessors that process client personal data meet contractual security and privacy obligations.
- Threat protection: Apply approved measures against malware and abuse, including platform monitoring on hosted workloads.

Business Continuity & Disaster Recovery — Backup, recovery, and continuity for hosted services. (https://privion-tech.com/trust/policies/business-continuity/)

Vendor Management Policy — Subprocessor evaluation and contractual requirements. (https://priviontech.com-/trust/policies/vendor-management/)

2.4 Personal information and privacy

Privion processes personal information in hosted services (for example, website analytics via PAnalytics) and in corporate operations. Where Privion acts as a processor, processing follows customer instructions and applicable data protection agreements.

Privion may monitor use of company systems to the extent permitted by law and policy to protect assets, investigate incidents, and verify compliance. Monitoring is limited to what is necessary for those purposes.

Breaches of this policy may result in disciplinary action, termination of access, contract remedies, and referral to law enforcement where appropriate.

Data Classification Policy — Handling tiers for public, internal, client-confidential, and regulated data. (https://privion-tech.com/trust/policies/data-classification/)

Privacy policy (website) — How Privion handles personal data on priviontech.com. (https://priviontech.com/privacy/)

3. Ownership and governance

The Privion security program owner is responsible for maintaining this policy, aligning it with emerging threats and regulatory expectations, and ensuring it is communicated to authorized users.

3.1 Security program owner

- Maintain and review this policy at least annually, or sooner when business, technology, or regulatory conditions change materially.
- Provide guidance and resources so users and system owners can comply with security requirements.
- Oversee reporting and investigation of information security incidents, including coordination with affected customers for hosted-service and processor scenarios.
- Manage the SOC 2 readiness program and track remediation of identified gaps.

3.2 Information system owners

- Implement policy requirements within assigned systems and ensure users understand their obligations.
- Monitor systems for compliance and address non-compliance promptly.
- Support security awareness training and role-appropriate guidance for users in their domain.
- Identify and treat risks for their systems, including controls and mitigation plans.

- Participate in audits and report significant risks or incidents to the security program owner without delay.

3.3 Policy review

This policy is reviewed at least annually, or more frequently when warranted by changes in services, technology, regulation, or threat landscape. System owners and leadership provide input during review.

4. Related policies

The following subsidiary policies provide detailed requirements. Together they form Privion's documented security program for the Trust Center:

Access Control Policy — Authentication, authorization, GDAP, and access reviews. (https://priviontech.com/trust/policies/access-control/)

Data Classification Policy — Classification and handling requirements. (https://priviontech.com/trust/policies/data-classification/)

Incident Response Policy — Detection, response, notification, and post-incident review. (https://priviontech.com-/trust/policies/incident-response/)

Acceptable Use Policy — Permitted and prohibited use of systems and client access. (https://priviontech.com/trust/policies/acceptable-use/)

Vendor Management Policy — Third-party and subprocessor security expectations. (https://priviontech.com/trust/policies/vendor-management/)

Business Continuity & Disaster Recovery — Continuity, backups, and restoration for hosted services. (https://priviontech.com/trust/policies/business-continuity/)

Reporting incidents

Report information security concerns to security@priviontech.com. For urgent matters affecting hosted services, clients with active engagements may also use the emergency contact channels established during onboarding. Phone: +1 (888) 600-2236.

Access Control Policy

MFA, role-based access, GDAP and PIM for client tenants, and joiner/mover/leaver procedures for Privion personnel.

Access to Privion systems and client environments is granted on a least-privilege basis and reviewed periodically.

Administrative access

Multi-factor authentication is required for Privion accounts. Client tenant administration uses Microsoft's partner delegation models (including GDAP) rather than standing global administrator roles in customer directories where practicable.

Lifecycle

Joiner, mover, and leaver processes are intended to provision and revoke access promptly. Access reviews for client tenants are conducted on a recurring basis.

Partner access recovery

Privion maintains documented records of GDAP relationships, PIM role assignments, and partner access procedures to re-establish client tenant administration after disruption.

Recovery playbooks cover partner center unavailability, compromised administrative accounts, and client offboarding.

Procedures are reviewed at least annually; exercise and test evidence available under NDA.

Data Classification Policy

Handling of public, internal, client-confidential, and regulated data categories where engagements require it.

Privion classifies information to apply appropriate handling requirements across consulting and hosted-service contexts.

Categories

Public information may be published on priviontech.com or in client-approved materials. Internal information supports Privion operations. Client-confidential information includes engagement data, credentials, and tenant configuration details. Regulated categories (for example PHI, PCI, or FERPA) receive additional controls when an engagement requires them.

Incident Response Policy

Detection, triage, containment, eradication, recovery, post-incident review, and customer notification commitments.

Privion maintains procedures to detect, respond to, and learn from security incidents affecting hosted services or Privion's access to client environments.

Process

Incidents are triaged by severity, contained to limit impact, eradicated, and recovered with documented timelines. Post-incident review captures root cause and corrective actions.

Notification

Where personal data processed by Privion as a processor is affected, notification commitments align with applicable law and contractual terms, including GDPR-aligned timelines where required.

Acceptable Use Policy

Expected use of Privion systems and acceptable behavior when accessing client Microsoft 365 environments.

Privion personnel must use company systems and client access responsibly and in line with engagement scope and client policies.

Prohibited activities include unauthorized data exfiltration, sharing credentials, circumventing client security controls, and using client environments for non-engagement purposes.

Vendor Management Policy

Subprocessor onboarding, contractual security requirements, DPA expectations, and periodic vendor review.

Third parties that process client personal data on Privion's behalf are evaluated before onboarding and listed on the public subprocessor page.

Contracts address confidentiality, security, subprocessors, and breach notification where applicable. Vendors are reviewed periodically for continued suitability.

Business Continuity & Disaster Recovery

Continuity and recovery objectives for Privion Intranet and PAnalytics, backup strategy, and restoration planning.

Privion plans for continuity of Privion Intranet and PAnalytics so that hosted analytics and related services can be restored after disruption.

Backups and recovery

PAnalytics is Privion-hosted Matomo on a shared Privion-managed Azure stack (Azure West US 2). Clients may instead deploy Matomo in their own environment.

Privion acts as data processor for visitor analytics collected on clients' websites when the hosted service is in use.

Backup and disaster recovery (implemented):

- Automated nightly MySQL logical backups (mysqldump) from Azure Database for MySQL Flexible Server
- Cross-region copy to Azure Blob Storage in Azure West Central US (30-day retention; lifecycle-managed)
- Documented restore procedure (provision recovery-region MySQL Flexible Server in Azure West Central US and replay latest dump)
- Quarterly recovery test per documented procedure
- RTO/RPO targets available on request

Privion Intranet

Privion Intranet processes documents into structured outputs via cloud AI services. Privion's processing methodology is proprietary and is not disclosed publicly to protect competitive advantage.

Continuity planning focuses on service availability and restoration of configuration rather than customer content recovery.

For third-party processing dependencies (for example, Azure OpenAI), see the Subprocessors page on the Trust Center.

- Documents are transmitted to processing infrastructure via encrypted channels.
- Results are returned to the client and made available for download.
- Documents and intermediate processing artifacts are not retained persistently on Privion infrastructure after delivery.

- No training data re-use: client data is not used to improve Privion products or third-party model services.
- For detailed data residency and processing specifics, see the Data Processing Agreement (available under NDA).

Privileged-access program

Privion maintains documented records of GDAP relationships, PIM role assignments, and partner access procedures to re-establish client tenant administration after disruption.

Recovery playbooks cover partner center unavailability, compromised administrative accounts, and client offboarding.

Procedures are reviewed at least annually; exercise and test evidence available under NDA.

Subprocessors

Privion provides 30 days' notice via this page before adding or changing a subprocessor that processes client personal data.

Microsoft Azure

Purpose: Privion Intranet and PAnalytics hosting; corporate infrastructure

Region: West US 2 (Privion Intranet, PAnalytics)

Certifications: SOC 2 Type II, ISO 27001, FedRAMP (platform)

DPA: Yes (Microsoft DPA)

Microsoft Azure OpenAI Service

Purpose: Privion Intranet document processing (Azure OpenAI API)

Region: United States (Privion deployment in West US 2)

Certifications: Inherits Microsoft Azure / OpenAI enterprise commitments per Microsoft DPA

DPA: Yes (Microsoft DPA; see Azure OpenAI data handling documentation)

Microsoft 365

Purpose: Privion corporate productivity and collaboration

Region: United States / global

Certifications: SOC 2, ISO 27001

DPA: Yes

Supabase

Purpose: Client portal database and authentication; Privion Intranet licensing server data store

Region: United States (Privion-managed projects)

Certifications: SOC 2 Type II, ISO 27001 (platform)

DPA: Yes (Supabase DPA)

Netlify

Purpose: Static hosting for priviontech.com, client portal, Privion Intranet licensing application, and product documentation; contact form delivery on the marketing site

Region: Global edge

Certifications: SOC 2 Type II; GDPR and CCPA program

DPA: Yes (Netlify DPA; incorporated in terms)

Twilio SendGrid

Purpose: Transactional email for general client communications and Privion client portal notifications (API/SMTP)

Region: United States / global delivery

Certifications: SOC 2 Type II (SendGrid); ISO 27001, GDPR, CCPA (Twilio platform)

DPA: Yes (Twilio Data Protection Addendum)

Zoho

Purpose: Password management (Zoho Vault), billing, accounting, and client ticketing

Region: United States / global (Zoho data centers)

Certifications: ISO 27001, ISO 27017, ISO 27018, SOC 2 Type II, GDPR

DPA: Yes (Zoho DPA available)

Incident response

Detection

Monitoring of Privion infrastructure (Privion Intranet and PAnalytics) via Azure Monitor platform telemetry (Application Insights and Log Analytics). Client-tenant incidents may be detected through Microsoft 365 Defender alerts and partner notifications.

Response

15-minute acknowledgment target for critical incidents affecting hosted services. Emergency contact channels for clients with active engagements.

Communication

GDPR-aligned 72-hour breach notification commitment for personal data incidents where Privion acts as processor. Per-client communication channels established at engagement start.

Detection capabilities

Hosted workloads use Azure Monitor (Application Insights and Log Analytics) for operational and security-relevant telemetry on PAnalytics. Privion does not operate a separate SIEM beyond Azure platform monitoring for hosted services at this time.

Escalation

Critical incidents affecting hosted services are escalated to designated security and engineering contacts. Client-specific escalation paths are agreed during onboarding for active engagements.

Customer notification

Notification timelines follow contractual commitments and applicable privacy law. For processor personal-data incidents, Privion targets communication within 72 hours of becoming aware, where GDPR applies, in coordination with the customer controller.

Post-incident reporting

A summary of impact, root cause, and remedial actions is provided to affected customers for significant incidents, subject to engagement terms and regulatory constraints.

Emergency contact: security@priviontech.com · +1 (888) 600-2236

Trust indicators

Targets and program metrics — not historical averages unless noted.

100%	MFA adoption (Privion personnel)
99.999%	Privion Intranet uptime (historical; not a contractual SLA)
15 min	Critical incident acknowledgment
72 h	Breach notification SLA (GDPR-aligned)

For SOC 2 readiness materials, full policy text, or security questionnaires, contact security@priviontech.com. Online version: https://privion-tech.com/trust