Privacy Policy

Platinum DB Consulting, Inc. — Information Security Management System

Policy PDB-SEC-98 | Platinum DB Consulting, Inc. | SOC 2 Trust Services Criteria

Field	Value	Field	Value
Policy ID	PDB-SEC-98	Version	3.0
Owner	Information Security Officer	Effective	2026-09-01
Approver	President, Platinum DB Consulting	Last reviewed	2026-08-18
Approval status	**Approved 2026-08-18**	Next review	2027-09-01
Classification	Internal — Confidential	Supersedes	2010 issue

1. Purpose

PDB processes personal data belonging to its customers' employees and customers. This policy defines how PDB handles personal information and meets its privacy obligations — the basis for the SOC 2 Privacy criteria where they are in scope.

2. Scope

This policy applies to all Platinum DB Consulting, Inc. (“Platinum DB”, “PDB”) information systems, to every workforce member, contractor and third party acting on PDB’s behalf, and to all customer systems and data hosted or managed by PDB. Unless stated otherwise, the following environments are in scope:

- **Chicago production colocation** — the PDB equipment cage in a third-party data center in the Chicago metropolitan area, hosting customer SAP, database and application systems.
- **Corporate environment** — the PDB office at 728 W. Jackson Blvd., Suite 807, Chicago, IL, together with all corporate endpoints, identity services and SaaS applications.
- **Remote and consultant access** — VPN, bastion/jump hosts and consultant laptops used at customer sites or from home.
- **Customer-hosted environments** — the segregated per-customer VLANs, servers, storage and backups that PDB operates under a hosting or managed-services agreement.

3. Policy

3.1 Roles and scope

3.1.1 PDB **must** distinguish clearly between personal data for which it is the **controller** (its own workforce and business contacts) and personal data it processes as a **processor** on behalf of customers.

3.1.2 As a processor, PDB **must** process customer personal data only on the documented instructions of the

customer, and **must not** use it for its own purposes — including for product improvement, analytics or model training.

3.1.3 Processing arrangements **must** be governed by a data processing agreement executed before processing begins, per PDB-SEC-57 and PDB-SEC-95.

3.1.4 PDB **must** maintain a record of processing activities describing the categories of personal data it handles, the purposes, the parties, retention and safeguards.

3.2 Principles applied

3.2.1 **Minimization** — PDB collects and retains only the personal data necessary for the stated purpose; production extracts and support copies are minimized and deleted when finished.

3.2.2 **Purpose limitation** — personal data is used only for the purpose for which it was collected or provided.

3.2.3 **Accuracy** — reasonable steps are taken to keep personal data accurate; workforce members may review and correct their own records.

3.2.4 **Retention** — personal data is retained only as long as necessary, per the schedule in PDB-SEC-97, and securely disposed of afterwards.

3.2.5 **Security** — personal data is classified Restricted and protected accordingly under PDB-SEC-30 through PDB-SEC-33.

3.2.6 **Transparency** — individuals whose data PDB controls are informed of what is collected and why.

3.3 Individual rights and requests

3.3.1 Requests from individuals to access, correct, delete or restrict processing of their personal data **must** be logged, acknowledged and handled within the period required by applicable law.

3.3.2 Requests concerning customer personal data **must** be forwarded promptly to the relevant customer, since the customer is the controller and PDB **must not** respond directly except on the customer's instruction.

3.3.3 PDB **must** assist customers in meeting their own obligations to individuals, as required by the processing agreement.

3.3.4 Requests **must** be verified as genuine before disclosure, since a request itself can be a social engineering vector.

3.4 Subprocessors, transfers and breach

3.4.1 Subprocessors handling customer personal data **must** be assessed under PDB-SEC-24, bound by equivalent obligations, and disclosed to customers where the agreement requires — including notice of changes.

3.4.2 Cross-border transfers **must** comply with applicable restrictions and customer requirements, with data location constraints enforced technically per PDB-SEC-95.

3.4.3 A breach involving personal data **must** be handled under PDB-SEC-16, with the affected customer notified without undue delay so they can meet their own statutory notification deadlines — PDB's notification to the customer must be fast enough to leave the customer time to act.

3.4.4 Privacy impact assessment **must** be conducted before new processing that presents elevated risk to individuals.

Processor discipline

The most consequential privacy rule for PDB is the simplest: customer personal data is processed only on the customer's instructions and never for PDB's own purposes. Using customer data to test, to demonstrate, or to prompt a third-party AI service breaches that rule even where no data is exposed.

4. Roles and Responsibilities

Role	Responsibility
President, Platinum DB Consulting	Approves the policy annually, allocates budget and resources, and accepts residual risk.
Information Security Officer (ISO)	Owns this policy, approves exceptions, performs the scheduled reviews named below, and reports control status to the President quarterly.
Service Delivery Manager	Confirms customer contractual and SLA obligations are reflected in day-to-day operation of this control.
HR / Office Manager	Executes the workforce-lifecycle steps (onboarding, training, offboarding) that this policy depends on.
All workforce members	Comply with this policy, complete required training, and report suspected violations or security events per PDB-SEC-16.

5. Evidence and Monitoring

The artifacts below are produced, retained and made available to the SOC 2 auditor as evidence that this policy operates. Retention is a minimum of twelve months unless a longer period is stated.

Evidence artifact	Frequency	Owner
Record of processing activities	Annually	Information Security Officer
Executed data processing agreements with customers	Per customer	President
Subprocessor register and customer disclosures	Annually and on change	Service Delivery Manager
Individual rights request log with response times	Per request	Information Security Officer
Privacy impact assessments for elevated-risk processing	Per assessment	Information Security Officer
Personal data retention and disposal records	Annually	Information Security Officer
Privacy content within annual awareness training	Annually	Information Security Officer
Breach notification records to customers	Per event	Service Delivery Manager

6. Definitions

Term	Meaning
Controller	The party determining the purposes and means of processing personal data.
Processor	A party processing personal data on behalf of, and on the instructions of, a controller.
Personal data	Information relating to an identified or identifiable individual.
Subprocessor	A third party engaged by PDB to process customer personal data on PDB's behalf.

7. Exceptions and Enforcement

Any deviation from this policy requires a written exception request stating the business need, the compensating control applied, the residual risk accepted and an expiry date not exceeding twelve months. Exceptions are approved by the Information Security Officer, recorded in the PDB exception register, and re-evaluated at expiry. Unapproved deviations are handled under the Sanction Policy (PDB-SEC-37).

8. Framework Mapping

SOC 2 TSC	ISO/IEC 27001:2022	Legacy ISO 17799	Control description
P1.1–P8.1	A.5.34	15.1.4	Privacy criteria: notice, choice, collection, use, retention, disclosure, quality, monitoring
CC9.1	A.5.34	15.1.4	Protection of personally identifiable information
CC9.2	A.5.19, A.5.20	6.2.3	Subprocessor management and disclosure
P6.3	A.5.26	13.2.1	Breach notification concerning personal information
P4.2	A.5.33	15.1.3	Retention and disposal of personal information

9. Related Policies

- Regulatory Compliance of Sensitive Data (PDB-SEC-95)
- Protection of Organizational Records (PDB-SEC-97)
- Classification of Data (PDB-SEC-30)
- Information Security in Outsourced Environments (PDB-SEC-24)
- Information Security Response and Reporting (PDB-SEC-16)

10. Revision History

Version	Date	Author	Summary of change
1.0	2010	PDB InfoSec	Original issue mapped to ISO 17799

3.0	2026-08-18	PDB InfoSec	Rewritten for SOC 2 Privacy criteria. Added controller/processor distinction, processing only on customer instruction with explicit prohibition on own-purpose use including AI training, record of processing activities, rights request handling, subprocessor disclosure and breach notification timing.