PERSONAL DATA PROTECTION POLICY

AUZA IT Services and Consultancy Inc.
Personal Data Protection Policy – Internal Data Governance and IT Service
Document Version: 1.1
Last Updated: 01 January 2026

1. Purpose

This Personal Data Protection Policy ("Policy") outlines the principles, governance structure, and organizational controls adopted by AUZA IT Services and Consulting Inc. ("AUZA") to ensure the lawful, fair, and secure processing of personal data across its operations and services.

This Policy establishes AUZA's internal framework for personal data protection and accountability and aligns data protection governance with AUZA's IT Service Management (ITSM) practices.

2. Scope and Applicability

This Policy applies to all AUZA personnel, including employees, contractors, consultants, and third parties acting on behalf of AUZA, as well as all systems, platforms, and processes that involve the handling of personal data.

This includes personal data processed within ITSM-related activities such as service delivery, incident management, change management, problem management, asset and configuration management, and service reporting.

The Policy applies regardless of geographic location or service model.

3. Relationship to Other Policies and Agreements

This Policy is an internal governance document and complements AUZA's external-facing Privacy Policy.

It supports contractual obligations under the Master Service Agreement, Service Level Agreement, Service Schedules, and other engagement documents, while remaining distinct from client-facing contractual terms.

Where inconsistencies arise, applicable laws and external contractual commitments prevail for client obligations, while this Policy governs internal data protection and ITSMaligned controls.

4. Data Protection Principles

AUZA processes personal data in accordance with recognized data protection principles, including:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy and data quality
- Storage limitation
- Integrity and confidentiality
- Accountability

These principles are embedded into ITSM processes and applied across the personal data lifecycle.

5. Governance and ITSM Alignment

Personal data protection governance is integrated into AUZA's IT Service Management framework.

Data protection considerations are incorporated into ITSM processes, including:

- Incident and request management
- Change and release management
- Problem management
- Asset and configuration management
- Service continuity and availability management

Governance ensures that personal data protection risks are identified, assessed, and managed as part of routine service operations.

6. Roles and Responsibilities

AUZA assigns clear responsibility for personal data protection across relevant business and ITSM functions.

Responsibilities include oversight of data protection compliance, implementation of controls, incident handling, and coordination with service management processes.

Personnel involved in ITSM activities are required to handle personal data in accordance with this Policy and related procedures.

7. Data Security Controls

AUZA implements appropriate organizational, technical, and physical safeguards to protect personal data against unauthorized access, loss, misuse, alteration, or disclosure.

Security controls are risk-based and integrated with ITSM controls such as access management, logging, monitoring, and incident response.

Controls are reviewed as part of service management and continuous improvement activities.

8. Data Lifecycle Management

Personal data is managed throughout its lifecycle in alignment with ITSM practices, including controlled creation, access, use, retention, and disposal.

Retention and disposal of personal data are coordinated with service asset management, configuration records, and service reporting requirements.

9. Third-Party and Vendor Management

Where personal data is processed by third parties in support of services, AUZA applies vendor management and supplier assurance controls aligned with ITSM and data protection requirements.

Third-party access to personal data is limited, monitored, and governed by contractual and operational controls.

10. Incident and Breach Management

Personal data incidents and breaches are managed through AUZA's incident management process, aligned with ITSM practices.

Incidents involving personal data are identified, recorded, assessed, escalated, and resolved using defined incident response and service management workflows.

Notification obligations are handled in accordance with applicable legal, regulatory, and contractual requirements.

11. Training and Awareness

AUZA promotes data protection awareness through role-based training integrated with ITSM onboarding and operational readiness programs.

Personnel involved in service delivery are required to understand data protection risks relevant to their ITSM responsibilities.

12. Monitoring, Audit, and Continuous Improvement

Compliance with this Policy is monitored through periodic reviews, internal audits, and service management metrics.

Findings are addressed through corrective actions and continuous improvement activities within the ITSM framework.

13. Policy Exceptions

Any exceptions to this Policy must be formally documented, risk-assessed, and approved through AUZA's governance and change management processes.

14. Availability of the Policy

The official and current version of this Personal Data Protection Policy is made available in PDF format through a secure download mechanism, ensuring controlled access to the authoritative internal data protection standards.