DELTA TECH AFRICA LIMITED

ISO/IEC 27701

PRIVACY INFORMATION MANAGEMENT

The Key Requirements Of
ISO/IEC 27701

Clause 1: Scope

Normative references are documents referred to throughout a standard.
For ISO/IEC 27701 these include:

- ISO/IEC 27000 Information security management systems – Overview and vocabulary
- ISO/IEC 27001 Information security management systems – requirements
- ISO/IEC 27002 Code of practice for information security controls
- ISO/IEC 29100 Privacy framework

Clause 2: References To Norms

Documents referred to throughout a standard are referred to as normative references.
For ISO/IEC 27701, these are as follows:

- ISO/IEC 27000:2005 Overview and lexicon of information security management systems
- Requirements for ISO/IEC 27001 information security management systems
- Code of practice for information security measures (ISO/IEC 27002)
- Privacy framework ISO/IEC 29100

Clause 3: Terms And Conditions

This section contains definitions for significant terminology used throughout the standard that are not covered by ISO/IEC 27000 and ISO/IEC 29100.

Clause 4: General

This clause lays the groundwork for ISO/IEC 27701. It gives a high-level summary of the document's layout and shows the position of PIMS-specific requirements in reference to ISO/IEC 27001 and ISO/IEC 27002

Clause 5: Specific ISO/IEC 27001 Criteria For PIMS

This clause is all about expanding ISO/IEC 27001 information security criteria to include privacy protection. You must establish your function as a processor and/or controller within the context of the company, taking into account the influence of internal and external variables such as privacy-specific rules and contractual requirements. Depending on your function, you must implement and apply necessary controls from Annexes A and/or B to your current statement of applicability.

You must also evaluate the parties involved in the processing of PII, the extent of your PIMS, and how you will effectively install, maintain, and upgrade the system. ISO/IEC 27001 objectives for leadership, planning, support, operation, performance assessment, and growth must be examined and expanded as necessary to provide privacy protection. Risks to information and the processing of PII, in particular, must now be examined and addressed accordingly.

Clause 6: Specific ISO/IEC 27002 Advice For PIMS

This clause is all about expanding ISO/IEC 27002 information security recommendations to include privacy protection. Organizations, for example, must consider extra implementation guidelines for information security policies in order to integrate suitable privacy statements based on compliance, contractual, and stakeholder needs. With respect to PII processing, clearer information on duties and responsibilities is provided. This involves being aware of incident reporting requirements as well as the implications of a data breach. Guidance is offered to ensure that PII is considered within your information classification.

You must understand the PII that your business handles, where it is stored, and the systems through which it moves. People must also understand what PII is and how to spot it. Incident management, removable media, user access on systems and services that process PII, cryptographic protection, re-assigning storage space that previously stored PII, back-up, and recovery of PII, event log reviews, information transfer policies, and confidentiality agreements are all covered in greater detail. Furthermore, instruction in this clause urges you to consider PII before transmitting data over public networks, as well as part of system development and design. It is critical to handle supplier relationships, expectations, and obligations.

Clause 7: Additional Information For PII Controllers

This section provides PIMS-specific implementation guidelines for PII controllers. It is about the controls stated in Annex A. To comply with relevant legislation, for example, you must identify the exact reasons for the PII you handle and have a legal basis for processing data. If the reason for processing PII develops or expands, updates should be made. Considerations for special category data and permission requirements, privacy impact assessment standards to reduce risk to PII principals, contracts with PII processors, and clear roles and responsibilities with any joint controllers are also outlined in the guidance. Individuals whose PII you process should understand why and how you process information, and there should be a point of contact for any requests. There is detailed information on permission, withdrawals, and PII access, correction, or erasure.

Third-party duties, request processing, and automated decision-making advice are also offered. Finally, privacy by design for processes and systems should take into account the minimal needs for collection and processing, the accuracy and quality of PII, constraints on the quantity gathered depending on the purpose of processing, and end-of-processing requirements. Importantly, PII sharing, transfer, and disclosure guidelines are provided to assist you in transferring between jurisdictions with accompanying documentation.

Clause 8: Additional Recommendations For PII Processors

This clause addresses PIMS-specific implementation guidelines for PII processors. It is about the controls stated in Annex B. Customer contracts, for example, should include your organization's function as a PII Processor in order to help with customer duties, including those of PII principals. To utilize PII data for marketing and advertising reasons, prior consent is required. Guidance is provided to assist you identify and keep the documents you need to establish compliance with the agreed-upon PII processing you do.

Annexes

ISO/IEC 27701 includes a number of Annexes. Annexes A and B are for controllers and processors, respectively, while annexes C–F give extra information to assist with the setup and operation of an effective PIMS.

Annex A

A List Of PII Controller Controls.

Not all controls will be necessary, but any control that is not required must be justified in the declaration of application.

Annex B

Controls For PII Processors Are Listed Here.

Not all controls will be necessary, but any control that is not required must be justified in the declaration of application.

Annex C

Controls For PII Controllers Are Mapped To The ISO/IEC 2900 Privacy Concepts.

This diagram depicts how ISO/IEC 27701 compliance requirements and controls connect to ISO/IEC 29100 privacy principles.

Annex D

Articles 5 Through 49 Of The GDPR Are Mapped To ISO/IEC 27701 Clauses (Except 43).

This demonstrates how compliance with ISO/IEC 27701 principles and controls might be important to meeting GDPR responsibilities.

Annex E

- ISO/IEC 27018 standards for PII processors in public clouds are mapped to ISO/IEC 27701 clauses.
- ISO/IEC 29151, which specifies additional controls and guidelines for PII controllers.

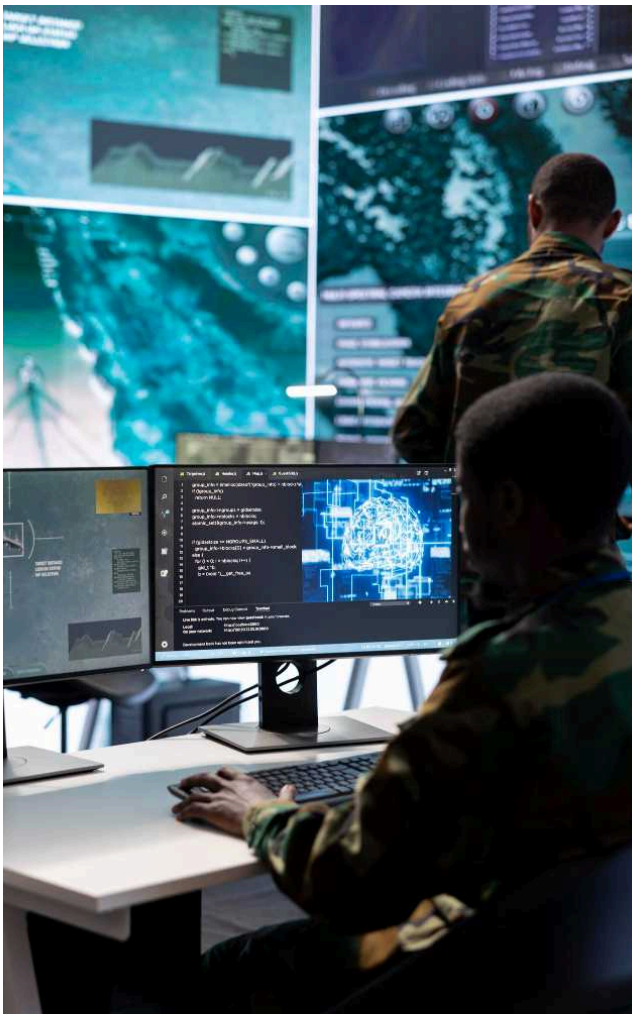
Annex F

Specifications For Applying ISO/IEC 27701 To ISO/IEC 27001 And ISO/IEC 27002.

It clearly maps the expansion of information security concepts to encompass privacy and gives several application examples.

About DTA

Delta Tech Africa Limited Is An ICT And Quality Consulting Organization Focused On Performance Management Across Business Verticals. Delta Means“ A Finite Increment”. We Help Organizations To Achieve This Increment Across Departments And Functions And To Improve The Overall Organizational Performance While Adding Value To The Stakeholders. Evolution Is A Constant Change. When The Pace Of Evolution Renders Societies Impatient, It Is A Technology That Accelerates Evolution Leading To The Transformation Of Societies. When That Evolution Happens, It Doesn’t Limit The Human Endeavors, To Get The Technology Evolution, It Has To Be Supported By Processes And Management Of The Best Quality. Hence, We At Delta Tech Africa Thought Of Bringing Both Technology And Quality Management Processes Together To Get The Best Organizational Performance And Value Across The Fast Growing Continent Of Africa.



Our Offices

Nigeria | PLOT 55B, Baderinwa Alabi Street, Central Lekki Residents' Association , Rahman Adeboyejo Street Lekki Phase 1, Lagos, Nigeria
Kenya | P.O.Box 39562-00623, Parklands, Nairobi, Kenya.
Ghana | Plot 3, Dade Link, Off Dade Street, Labone, Accra, Ghana.
South Africa | 1 Waterhouse Place Century City Cape Town 7441

Our Phone Numbers

+27 63 933 1982, +27 10 594 5356

Our Email

info@dtafrica.com

Our Website

https://www.dtafrica.com

DELTA TECH AFRICA LIMITED

info@dtafrica.com | www.dtafrica.com