



June 17 2026

## PPDA Uganda Makes History as the First Public Institution to Achieve ISO/IEC 27001:2022 Certification Under Uganda's Digital Acceleration Project

Here is how they achieved it.



On 12 June 2026, Uganda's Minister of ICT and National Guidance, Hon. Justine Kasule Lumumba, handed a certificate to the management of the Public Procurement and Disposal of Public Assets Authority.

It was not just a piece of paper.

It was the first ISO/IEC 27001:2022 certification achieved by any of the ten government institutions currently working under the **Uganda Digital Acceleration Project**, a national programme led by the **National Information Technology Authority Uganda** to strengthen digital governance and accelerate secure digital transformation across Uganda's public sector.

PPDA was first.



And what made them first is a story worth telling, not because of the certificate, but because of what had to change inside an institution before that certificate was possible.

## **The Context: Why Data Protection in Uganda's Public Sector Has Never Mattered More**

Uganda's public institutions are managing more sensitive information than at any point in the country's history.

Procurement bids. Supplier records. Contract documentation. Evaluation data. Financial records. The systems that govern how public money is spent and how public assets are managed sit at the intersection of institutional accountability, data protection compliance Uganda, and national digital security.

As Uganda's digital economy accelerates, driven by the Uganda Digital Acceleration Project, Bank of Uganda's cybersecurity mandates for supervised financial institutions, and the enforcement of the Data Protection and Privacy Act - the expectations on public institutions have fundamentally shifted.

Information security is no longer an IT function. It is a governance responsibility.

And in 2026, with Uganda's first criminal conviction under the Data Protection and Privacy Act already on record, and with the PDPO's ruling against Google establishing that no organisation, regardless of size or global standing, is exempt from Uganda's data protection obligations, the cost of getting this wrong has never been higher.

PPDA understood that.

## **The Challenge: From Controls to Culture**

PPDA was not starting from zero.

Policies existed. Processes existed. Technology controls existed.

But information security was not yet operating as an integrated system, a framework that connected individual controls, measured effectiveness, managed risk systematically, and embedded security into the institution's daily behaviour.

This is the gap that most organisations in Uganda's public sector are sitting in right now. Individual security measures without the governance architecture that makes them sustainable, auditable, and genuinely resilient.

The challenge PPDA faced was not primarily technical. It was cultural.

How do you move an institution from treating information security as an IT department responsibility to treating it as an organisational value, owned by every team, reflected in every process, and championed by leadership?

That is the harder problem. And it is the one that matters most.

## The Approach: Security as an Institutional Initiative

What distinguished PPDA's journey was the breadth of organisational participation.

Information security did not stay in the IT department.

Teams from procurement, compliance, administration, and operations collaborated to review policies, assess risks, strengthen procedures, and align daily practices with the requirements of ISO/IEC 27001:2022.



Staff across departments participated in awareness sessions, policy discussions, and process reviews, not as passive recipients of training, but as active participants in building a security culture from the inside out.

Over six months, something shifted.

Security became less about compliance and more about behaviour. Less about technology and more about accountability.

This shift, from security as a technical exercise to security as an organisational value, is precisely what separates institutions that achieve certification from institutions that achieve transformation.

PPDA achieved both.

## The Role of Leadership

Every successful Information Security Management System implementation has one non-negotiable ingredient.

Leadership commitment.

Not because executives write policies or conduct risk assessments. But because in any institution, culture follows leadership. When management treats information security as a strategic priority, through active participation in management reviews, policy approvals, governance oversight, and visible engagement, the rest of the organisation follows.

Throughout PPDA's implementation journey, this commitment was consistent and genuine.

Dr. Hatwib Mugasa, Executive Director of NITA-U, acknowledged it directly at the certification ceremony:



***"While NITA-U provided the technical guidance, helped build internal capacity, and sponsored the certification, the true heavy lifting was done by PPDA's own dedicated team. Their commitment to securing public procurement data is exemplary."***

Leadership commitment is not a soft requirement. It is the foundation on which everything else is built.

## How Sentinel Africa Supported the Journey



Institutional transformation of this scale requires expertise, structure, and a partner who understands that the goal is not certification, it is long-term resilience.

Sentinel Africa worked alongside PPDA throughout the implementation journey, providing the advisory, technical, and capacity-building support required to design, build, and operationalise an Information Security Management System aligned with ISO/IEC 27001:2022.

The engagement covered:

- **Information Security Governance Advisory** - establishing the governance architecture that gave PPDA's leadership visibility, accountability, and control over the institution's security posture.
- **ISMS Implementation Guidance** - translating the requirements of ISO/IEC 27001:2022 into practical, context-specific policies, procedures, and controls suited to PPDA's operational environment.
- **Risk Management Support** - building a systematic approach to identifying, assessing, and treating information security risks across the institution's people, processes, and technology.
- **Policy and Procedure Development** - creating documentation frameworks that were not only ISO-compliant but usable, understandable, and embedded into daily workflows.
- **Awareness and Capacity Building** - equipping staff across departments with the knowledge and skills to carry information security forward as active participants, not passive recipients.
- **Certification Readiness Preparation** - guiding PPDA through the audit readiness process to ensure the institution was fully prepared for external certification assessment.
- **Automation-Driven Compliance Support** - integrating automation tools into the ISMS to reduce manual effort, ensure consistency, and build a compliance infrastructure that sustains itself beyond certification.

A core principle guiding Sentinel Africa's approach throughout was sustainability. Certification is a milestone. What matters is whether the institution can maintain, improve, and build on what was achieved once the external advisors leave the room.

For PPDA, the answer to that question was built into the implementation itself.

## The Outcome



After six months of focused effort, cross-functional collaboration, and continuous improvement, PPDA Uganda achieved ISO/IEC 27001:2022 certification, becoming the first institution under NITA-U's Uganda Digital Acceleration Project to reach this milestone.

The certificate was officially handed over to PPDA management by Hon. Justine Kasule Lumumba, Minister of ICT and National Guidance, at a ceremony attended by NITA-U leadership and PPDA management.



But the outcome is not the certificate.

The outcome is an institution where information security is embedded into governance structures, operational processes, and decision-making frameworks. An institution where the

question is no longer whether to protect information, but how to continuously improve the systems that do.

And an institution that has signalled to every supplier, partner, government body, and citizen that interacts with it: the information you share with us is protected to an internationally recognised standard.



In Uganda's current data protection landscape, where enforcement is accelerating, criminal liability is real, and the cost of a breach extends far beyond financial penalties into institutional reputation, that signal matters enormously.

## What This Means for Uganda's Public Sector

PPDA's achievement does not exist in isolation.

It is part of a broader national movement. The Uganda Digital Acceleration Project is working with ten government institutions. PPDA is the first to certify. The others are watching, and the path has now been walked.

For every public institution in Uganda managing sensitive procurement, financial, health, or citizen data, PPDA's journey answers the question that most leaders are quietly asking:

*Is this actually achievable for us?*

The answer is yes. With the right commitment, the right participation, and the right partner.

## Key Lessons for Organisations Pursuing ISO 27001 in Uganda

**Information security is a governance issue, not an IT issue.** Sustainable security requires leadership involvement, cross-functional accountability, and an ISMS that connects controls to strategy.

**Culture is the hardest and most important variable.** Technology can be procured. Culture has to be built, through leadership behaviour, staff participation, and consistent reinforcement over time.

**Certification is a milestone, not the destination.** ISO/IEC 27001 validates an organisation's current security posture. Continuous improvement is what makes that posture durable.

**National programmes amplify individual achievement.** PPDA's success is both an institutional milestone and a contribution to Uganda's national digital transformation agenda. That context matters, for stakeholders, for credibility, and for the institutions that follow.

**The right implementation partner makes the difference.** External expertise provides clarity, structure, and confidence. The goal of a good implementation partner is to make themselves unnecessary, by building capability inside the institution that lasts long after the engagement ends.

## A Final Thought

The future of information security in Uganda is not about stronger firewalls.

It is about stronger institutions.

Institutions where leadership treats information as a strategic asset. Where staff at every level understand their role in protecting it. Where governance frameworks and technical controls work together inside a system that is continuously improving.

PPDA Uganda has demonstrated that this is achievable, in six months, inside a government institution, as part of a national digital transformation programme.

That is not a small thing.

That is what data protection compliance Uganda looks like when it is done right.



*Sentinel Africa Consulting is an ISO 27001 and ISO 27701 certified risk advisory firm with offices in Nairobi, Kampala, and Kigali. We support organisations across East Africa on information security, data protection compliance, business continuity, and GRC advisory.*

*To explore how your organisation can begin its ISO 27001 journey — speak with our team in Kampala.*

 [info.ug@sentinelafricaconsulting.com](mailto:info.ug@sentinelafricaconsulting.com)  [www.sentinelafricaconsulting.com](http://www.sentinelafricaconsulting.com)

*Explore our Information Security services | Learn about ISO 27001 certification training*



[www.sentinelafrikaconsulting.com](http://www.sentinelafrikaconsulting.com)



**Uganda Office**

Kanjokya House  
P.O. BOX 119743 Kampala,  
GPO Uganda  
+256 757 818 444  
[info.ug@sentinelafrikaconsulting.com](mailto:info.ug@sentinelafrikaconsulting.com)



**Kenya Office**

Rainbow Tower, 6th Floor,  
Muthithi Road, Nairobi, Kenya  
+254 20 2484888, +254 715 484888  
[info@sentinelafrikaconsulting.com](mailto:info@sentinelafrikaconsulting.com)



**Rwanda Office**

Plot: KG 37 Avenue Kigali,  
Rwanda  
+250 782 746 073  
[info.rw@sentinelafrikaconsulting.com](mailto:info.rw@sentinelafrikaconsulting.com)



Sentinel Africa Consulting