THE NEW ISO 27701:2025; PRACTICAL STEPS FOR DEVELOPING YOUR BREACH RESPONSE PLAN

By Boluwatife Deborah Ekundayo & Oluwatobi Ogo-oluwa Akinola

In October 2025, the International Organisation for Standardisation *("ISO"),* in collaboration with the International Electrotechnical Commission *("IEC"),* released ISO/IEC 27701:2025 *("the Standard"),* a revised international standard for Privacy Information Management Systems.[1] Unlike ISO/IEC 27701:2019, which operated as an extension to ISO/IEC 27001, the 2025 revision transforms privacy management into a standalone, certifiable standard. This shift reflects a growing global emphasis on privacy governance as a distinct operational and risk management discipline.

At its core, the Standard provides a structured and internationally recognised framework for identifying, assessing, and managing privacy risks. One of its most practical applications is in the development of a robust and defensible personal data breach response plan. Unlike ad hoc or stand-alone incident response playbooks that operate in isolation and are typically consulted only after a breach has occurred, a breach response plan developed in accordance with ISO/IEC 27701:2025 is embedded within an organisation's broader Privacy Information Management System.[2] When aligned with the Nigeria Data Protection Act (NDPA), 2023 and its General Application and Implementation Directive (GAID), a breach response plan built on ISO/IEC 27701:2025 enables organisations to move away from ad hoc and reactive incident handling, and embrace a pre-planned, accountable, and auditable approach to breach management that regulators increasingly expect.

This article outlines practical steps organisations can take to operationalise ISO/IEC 27701:2025 for data breach response planning, while meeting Nigerian regulatory requirements.

STEP 1: ESTABLISH CLEAR GOVERNANCE AND ACCOUNTABILITY

ISO/IEC 27701:2025 requires organisations to define and document responsibility for privacy management, including incident response, with active support from top management. Governance is not optional and must be embedded within the organisation's operational structure. Organisations must therefore appoint a person or team responsible for coordinating privacy management, especially breach response planning. This aligns with the accountability principle under the NDPA and GAID, which requires data controllers and processors to demonstrate responsibility for compliance, including breach management.

In practice, organisations should formally identify:

A designated data protection or privacy lead with authority to coordinate breach response.
- Technical teams responsible for detection, containment, and forensic investigation.
- Legal and compliance teams responsible for regulatory analysis and notification decisions.
- Communications leads responsible for internal and external messaging.
-

These roles should be documented, communicated internally, and reflected in job descriptions, escalation matrices, and internal policies.

1 PECB, 'The Future of Privacy with ISO/IEC 27701' https://pecb.com/en/whitepaper/the-future-of-privacy-with-isoiec-27701 accessed 19 December 2025.
2 DPO Centre, 'ISO 27701:2025 update: What's changed and why it matters' (8 December 2025) https://www.dpocentre.com/iso-27701-2025-whats-changed/ accessed 19 December 2025.

STEP 2: GROUND THE BREACH RESPONSE PLAN IN PRIVACY RISK ASSESSMENT

Breach response plans are most effective when they are built on an understanding of what could go wrong. The Standard adopts a risk-based approach to privacy management. A breach response plan should therefore be informed by prior privacy risk assessments and, where applicable, Data Protection Impact Assessments.

Organisations should map:

- Categories of personal data processed, including sensitive personal data.
- Critical systems, platforms, and third-party vendors involved in processing.
- High-risk processing activities, including profiling and automated decision-making.
- Jurisdictions whose laws may impose breach notification obligations, including Nigeria.

This risk mapping allows organisations to prioritise response actions and decision-making during an incident.

STEP 3: DEFINE DETECTION, IDENTIFICATION, AND INTERNAL REPORTING PROCEDURES

Early detection is critical. Dela breach detection often results in delayed regulatory reporting and increasing enforcement risks. ISO/IEC 27701:2025 therefore requires procedures for early detection and escalation of privacy incidents.

Practical measures include:

- Technical monitoring, logging, and alerting mechanisms.
- Clear thresholds for what constitutes a potential personal data breach.
- Simple and accessible internal reporting channels for all staff.
- Regular training to ensure employees can recognise and escalate incidents promptly.

STEP 4: DOCUMENT RESPONSE AND CORRECTIVE AND PREVENTIVE ACTIONS (CAPA)

Once a breach is confirmed, the response plan must set out specific corrective and preventative actions, to mitigate the inherent risk of a breach and to prevent future recurrence. The Standard require CAPA to be documented, repeatable, and auditable.

A practical breach response plan should set out:

- Immediate containment actions to limit further data exposure.
- Technical and operational steps to secure affected systems.
- Processes for preserving evidence and maintaining audit trails.
- Short-term and long-term remediation measures.

This aligns with the provision of the NDPA which mandates organisations to maintain records of breaches including the remedial actions taken after the breach[3].

3 Section 40(8) NDPA 2023

STEP 5: INTEGRATE LEGAL AND REGULATORY NOTIFICATION REQUIREMENTS

Privacy standards do not replace the law. ISO/IEC 27701:2025 encourages organisations to integrate legal and regulatory obligations into their breach response planning.

In Nigeria, this means being aware of all data protection obligations under NDPA and GAID, including requirements for breach notification to the Nigeria Data Protection Commission (NDPC) and, where applicable, affected data subjects [4].

A compliant breach response plan should:

- Identify applicable notification obligations under NDPA and GAID.
- Define internal timelines for assessing breach severity and risk.
- Assign responsibility for regulatory engagement and correspondence,including notifying the NDPC.
- Establish clear criteria for determining when notification is mandatory, both to the NDPC and the data subjects

STEP 6: PREPARE COMMUNICATION AND STAKEHOLDER MANAGEMENT PROTOCOLS

Beyond regulatory notification, data breaches often require communication with customers, employees, business partners, and, in some cases, the public.

The Standard encourages advance planning for breach communications. This aligns with the NDPA requirement for transparency and breach notifications to affected data subjects where the breach is likely to result in a high risk to the rights of the data subjects.[5]

Organisations should prepare:

- Pre-approved communication templates adaptable to different breach scenarios.
- Clear internal communication protocols to prevent misinformation.
- Guidelines for engaging third-party vendors, insurers, and advisors.

Effective communication can significantly mitigate reputational and operational harm.

STEP 7: TEST, REVIEW, AND CONTINUALLY IMPROVE THE PLAN

A breach response plan is a living document. ISO/IEC 27701:2025 establishes principle of continual improvement. A breach response plan must therefore be tested and reviewed on an ongoing basis.
Practical steps for continuous improvement of a breach response plan include:

- Periodic tabletop exercises and breach simulations.
- Post-incident reviews and lessons learned.
- Regular updates to reflect regulatory, technological, and organisationalchanges.

---

3 Section 40(8) NDPA 2023
4 Section 40(2) NDPA 2023, Article 33 GAID
5 Article 42 (2) GAID, Article 24 NDPA 2023,

Regular reviews foster a culture of readiness. They also demonstrate to stakeholders, including regulators, that you are serious about privacy management and committed to continuous improvement.

CONCLUSION

A solid breach response plan helps limit harm to individuals, minimises regulatory risks and sustains trust. A breach response plan that aligns ISO/IEC 27701:2025 with the NDPA and GAID integrates governance, risk assessment, incident detection, legal decision-making, and continuous improvement into a coherent and auditable process. Organisations that adopt this approach position themselves to respond to incidents with greater speed, consistency, and defensibility. More importantly, they move beyond minimum compliance toward a mature privacy posture that can withstand regulatory scrutiny and support sustained stakeholder confidence in today's highly regulated digital economy.

Babalakin & Co. is a firm with broad experience on the subject of Tech, Information Technology and all matters encompassing it. If you have any questions or would like information on the issues discussed, please contact:

Boluwatife Deborah Ekundayo

Associate

Oluwatobi Ogo-oluwa Akinola

Trainee Associate