Nigeria Network of NGOs

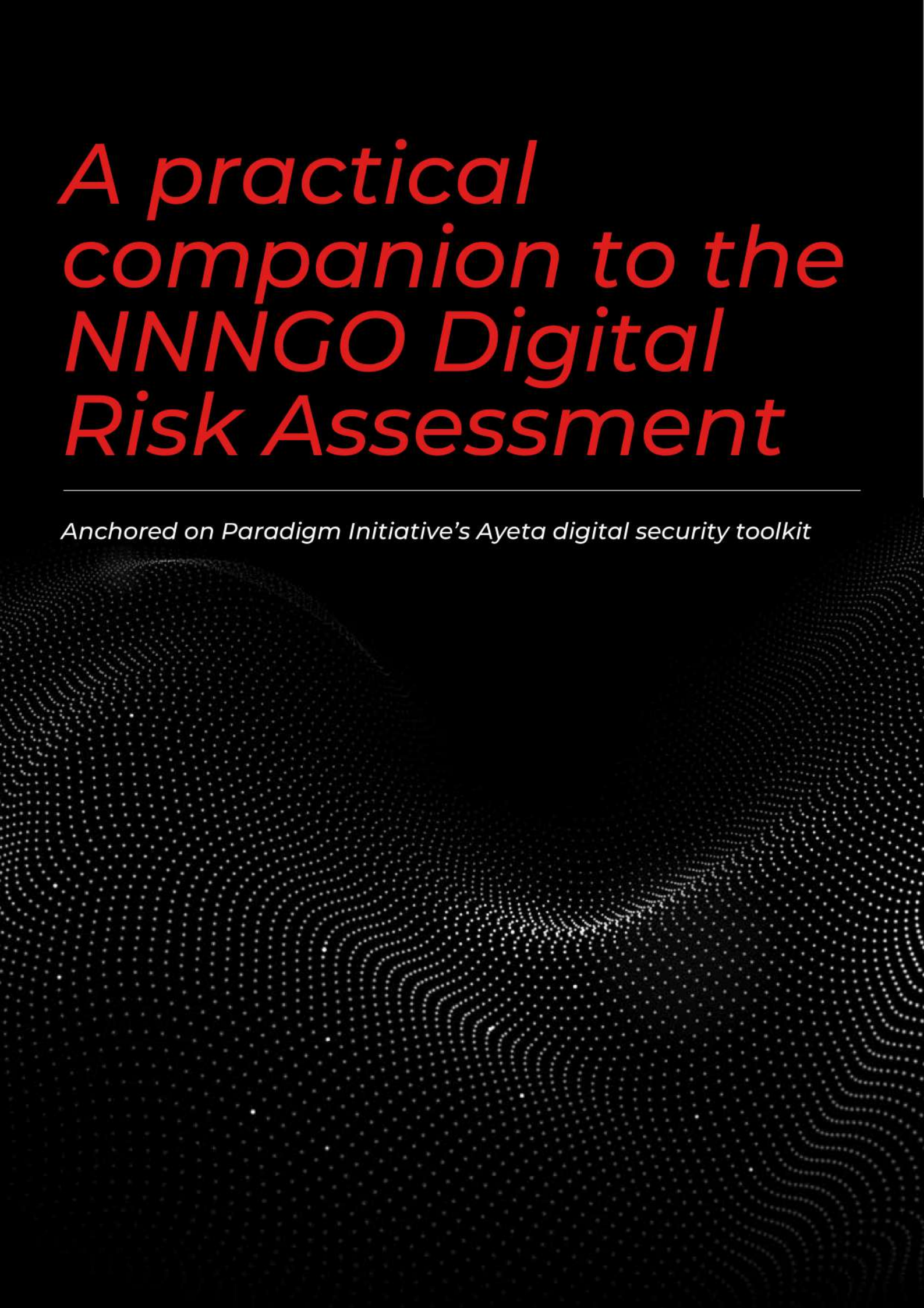
Digital Resilience Toolkit

for Civil Society Organisations

Version 1.0 · May 2026

A practical companion to the NNNGO Digital Risk Assessment

Anchored on Paradigm Initiative's Ayeta digital security toolkit



1. About this toolkit

This toolkit turns the findings of the **NNNGO Digital Risk Assessment** into action. The assessment surveyed 286 civil society organisations across all 36 States and the FCT and found that, while the median organisation implements about three-quarters of expected controls, roughly two-in-five are "Basic" or "Critical" — lacking the protections needed to safely hold beneficiary data, meet donor obligations, or recover from a serious incident. This toolkit gives every CSO, whatever its size or budget, a clear path to digital resilience.

It is deliberately practical. Each module explains why a control matters (citing the sector-wide gap the assessment uncovered), shows what "good" looks like as a printable checklist, and recommends free or low-cost tools — led by Paradigm Initiative's Ayeta toolkit and its companion platforms — that a non-technical team can adopt without specialist help.

1.1 Why "resilience", not just "security"

Security asks whether a control is present. Resilience asks whether the organisation can keep operating, protect the people it serves, and recover quickly when something goes wrong — a power cut, a lost phone, a phishing email, an internet shutdown, or a data breach. For Nigerian CSOs working on civic space, human rights, and sensitive beneficiary data, resilience is mission continuity. A single ransomware event or device loss should never be able to erase years of programme records.

1.2 The one finding that shapes everything

The assessment's most important result was statistical: across the seventeen control areas measured, organisational scores were highly correlated (mean r = 0.60). In plain terms, **weakness clusters**. An organisation that is weak in one area is almost always weak across the board, because the real gap is not a missing tool — it is the underlying organisational foundation: a written policy, a named person responsible, and leadership attention. **This is why the toolkit starts with governance (Module 1) and treats tools as the second step, not the first.**

> **How to read each module**
>
> Why it matters — the risk, with the sector-wide gap from the assessment.
> What good looks like — a printable checklist your team can tick off.
> Tools that help — free or low-cost options, led by Ayeta and the PIN suite.
> Do this first — the single highest-value action if you do nothing else.

2. How to use this toolkit

You do not need to do everything at once. Start by locating your organisation on the maturity ladder below — the same four tiers used in the assessment — then follow the recommended pathway. Re-assess every six months and move up a tier at a time.

Table 1. Find your starting point

Tier	You are here if...	Your pathway through this toolkit
Critical	You have few written policies and several of the eleven baseline controls (Section 3) are missing.	Complete the Minimum Digital Security Baseline (Section 3) first. Do Modules 1, 2, 4 and 7 before anything else. Seek hands-on support — do not attempt this alone.
Basic	You have some controls but they are patchy and undocumented.	Close every gap in the Baseline (Section 3), then work through Modules 1–6 in order. Adopt the Ayeta toolkit org-wide.
Developing	Most controls exist but governance and monitoring are weak.	Focus on Modules 1 (governance), 6 (detection) and 8 (incident response). Formalise policies and run your first incident drill.
Mature	Controls are implemented and documented across the board.	Maintain, test and mentor. Run annual drills, mentor peer CSOs, and contribute to the sector via NNNGO and the PIN community.

To self-assess, work through the eleven-point Minimum Digital Security Baseline in Section 3. If you answer “no” or “not sure” to four or more, treat yourself as Critical; one to three, Basic; all yes but undocumented, Developing; all yes and documented, Mature.

3. The Minimum Digital Security Baseline

These eleven controls are the irreducible minimum for any CSO that holds personal data, donor funds, or beneficiary records. The assessment found every one of them missing in a fifth to nearly two-fifths of organisations. Treat this page as a self-assessment worksheet: print it, tick what is true today, and turn every blank into an action.

Worksheet: the eleven baseline controls (sector failure rate in brackets)

- ☐ A written information security policy, approved by leadership *[Governance (R8 in assessment)]*
- ☐ A named person responsible for digital security (and a Data Protection Officer) *[Governance]*
- ☐ NDPR/NDPA compliance assessed at least annually (failing in 37.9%) *[Compliance]*
- ☐ Strong, unique passwords stored in a password manager *[Identity]*
- ☐ Multi-factor authentication on all important accounts (missing in 24.7%) *[Identity]*
- ☐ Account lockout after repeated failed logins (missing in 35.8%) *[Identity]*
- ☐ Access removed promptly when staff leave (missing in 23.2%) *[Access]*
- ☐ A firewall protecting your network or website (missing in 34.5%) *[Network]*
- ☐ Sensitive data encrypted, and backups tested for recovery (backups untested in 22.5%) *[Data]*
- ☐ Up-to-date anti-malware on every device (out of date in 27.2%) *[Endpoint]*
- ☐ An incident response plan and basic staff awareness training (no plan in 32.1%; no training in 30.4%) *[Respond]*

Anchor resource

Download the Ayeta toolkit (free) and use its security goal-setting feature to record your baseline targets. Ayeta is available in English, French, Hausa, Igbo, Swahili and Yoruba at ayeta.africa, or via paradigmhq.org/ayetadownload.

Module 1

Governance & foundations

Why it matters

Because weakness clusters (the r = 0.60 finding), the single highest-leverage investment is not a tool but a foundation: a short written policy, a named owner, and leadership attention. The assessment's strongest organisations were strong everywhere precisely because they had this base. Without it, individual controls are fragile and do not last.

What good looks like

- ☐ A 2–4 page Information Security & Data Protection Policy, approved by your board or leadership.
- ☐ One named person accountable for digital security (can be part-time), and a designated Data Protection Officer.
- ☐ A simple risk register listing your top digital risks and who owns each.
- ☐ Registration with the Nigeria Data Protection Commission (NDPC) and an annual NDPA/NDPR compliance review.
- ☐ Digital security is a standing item at leadership meetings, at least quarterly.

Tools that help

- **Ayeta security goal-setting** — use it to set and track your organisation's security goals and turn this toolkit into a dated action plan.
- **NDPC registration portal** — register as a data controller and document your lawful basis for holding beneficiary data.
- **Londa (PIN)** — PIN's annual digital rights report; use it as context and evidence when briefing your board or donors on the threat environment.

> **Do this first**
>
> Write (or adopt) a one-page information security policy this month and have leadership sign it. Everything else in this toolkit hangs off that page.

Module 2

Identity & access

Why it matters

Stolen or guessed passwords are the most common way attackers get in. The assessment found **35.8% of CSOs have no account lockout, 24.7% no multi-factor authentication, and 23.2% do not remove access when staff leave** — three low-cost gaps that together make account takeover easy. Identity is where the cheapest, highest-impact wins are.

What good looks like

- ☐ Every staff member uses a password manager to create long, unique passwords for each account.
- ☐ Multi-factor authentication (MFA/2FA) is switched on for email, banking, social media, donor portals and cloud storage.
- ☐ Accounts lock after a set number of failed login attempts.
- ☐ Access follows the job role (role-based access) — people can reach only what they need.
- ☐ A written joiners/leavers checklist revokes all access on the day someone leaves.

Tools that help

- **Bitwarden or KeePassXC** — free, open-source password managers. Ayeta explains password safety and points to trusted options.
- **Authenticator apps (e.g. Aegis, or Google/Microsoft Authenticator)** — free app-based MFA. Prefer an app over SMS where possible. Ayeta covers two-factor authentication step by step.
- **Built-in lockout settings** — enable failed-login lockout in Google Workspace, Microsoft 365 and your website admin panel; it is free and already there.

> **Do this first**
>
> Turn on multi-factor authentication for your organisation's main email account today — it is the account that can reset all the others.

Module 3

Devices & endpoints

Why it matters

Most CSO work now flows through laptops and staff-owned phones. The assessment found **22.0% have no anti-malware on all devices, 27.2% do not keep it updated, and only 51.9% manage mobile devices (MDM)**. A lost or stolen unmanaged phone can hand over years of beneficiary data in one moment.

What good looks like

- ☐ Anti-malware is installed on every computer and kept automatically up to date.
- ☐ Devices lock automatically and require a PIN, password or biometric.
- ☐ Laptops and phones are encrypted (BitLocker on Windows, FileVault on Mac, built-in encryption on phones).
- ☐ Mobile device management lets you remotely lock or wipe a lost or stolen device.
- ☐ Removable media (USB drives) are scanned, and staff cannot disable protection without approval.

Tools that help

- **Windows Defender / built-in antivirus, or ClamAV** — free anti-malware adequate for most CSOs; ensure automatic updates are on.
- **Device encryption (BitLocker, FileVault, Android/iOS encryption)** — free and built in; just switch it on.
- **Google Endpoint Management / Microsoft Intune** — basic MDM is included with Google Workspace and Microsoft 365 nonprofit plans at no extra cost.

> **Do this first**
>
> Switch on device encryption and automatic screen-lock on every laptop and phone this week — it costs nothing and defeats most theft.

Module 4

Data protection & backup

Why it matters

Your data is your mission — and, increasingly, your civic-space exposure. The assessment found **22.5% of CSOs have no tested backups and a further share store backups where the same attack could destroy them**; combined with the 25.3% that do not encrypt sensitive data, this is the sector's clearest path to catastrophic, unrecoverable loss — and to compelled disclosure of beneficiary records. The single highest-value control is **data minimisation**: collecting less beneficiary data at source reduces breach impact, surveillance exposure and the harm of any seizure at once (assessment recommendation FA1).

What good looks like

- ☐ Data minimisation is practised: only data that is needed for a clear purpose is collected, and it is deleted when no longer needed.
- ☐ You follow the 3-2-1 rule: three copies of important data, on two types of media, with one copy off-site or in the cloud.
- ☐ Backups are tested by actually restoring a file at least quarterly — an untested backup is not a backup.
- ☐ The backup is isolated, so ransomware on the main system cannot reach it.
- ☐ Sensitive and beneficiary data is encrypted, both on devices and in the cloud.
- ☐ Data is classified (e.g. public / internal / sensitive) and access follows least privilege; cross-border storage respects NDPA transfer rules.

Tools that help

- **Cryptomator or VeraCrypt** — free, open-source encryption for cloud folders and local drives.
- **Encrypted cloud + an offline external drive** — the simplest 3-2-1 setup; nonprofit Google Workspace / Microsoft 365 plans include generous storage.
- **Ayeta data-protection guidance** — practical steps on protecting sensitive information, aligned to the needs of human rights defenders.

Do this first

Switch on device encryption and automatic screen-lock on every laptop and phone this week — it costs nothing and defeats most theft.

Module 5

Network & connectivity resilience

Why it matters

Nigerian CSOs face two network threats at once: ordinary cyber-attack and deliberate disruption — throttling, blocking, or full internet shutdowns during elections and protests. The assessment found **34.5% have no firewall and many lack secure remote access.** Resilience here means both keeping attackers out and staying connected when the network is under

What good looks like

- ☐ A firewall protects your office network and your website/hosting.
- ☐ Remote access uses a VPN and strong authentication, never an open connection.
- ☐ Wi-Fi uses strong WPA2/WPA3 encryption and a separate guest network.
- ☐ Staff know how to keep working and communicating during a shutdown or blackout.
- ☐ You can detect and document network interference if it happens.

Tools that help

- **Ayeta shutdown-circumvention guidance** — Ayeta's core strength: how to prepare for, circumvent and keep records during internet disruptions, plus VPN guidance.
- **OONI Probe** — free, open-source app (PIN is an OONI partner) that measures and evidences website blocking and censorship in real time.
- **Reputable VPN / Tor Browser / Psiphon** — for secure remote access and for circumventing blocking; Ayeta points to trusted options for the African context.

> **Do this first**
>
> Install OONI Probe on a staff phone now, so that if a shutdown or blocking event happens you can measure and document it from the first minute.

Module 6

Threat detection & monitoring

Why it matters

You cannot respond to what you cannot see. Monitoring was one of the weakest areas in the assessment, with **only 53.8% using any intrusion detection and large gaps in logging, alerting and email security**. Most CSO compromises begin with a phishing email, so email defence is the priority here.

What good looks like

- ☐ Email anti-phishing protection is on, with SPF, DKIM and DMARC configured for your domain.
- ☐ Logging is enabled on key systems, and logs are reviewed at least monthly.
- ☐ Alerts are set for suspicious sign-ins (e.g. logins from new countries).
- ☐ Attachments and links are scanned before opening.
- ☐ Staff have a simple, known way to report a suspicious email.

Tools that help

- **SPF / DKIM / DMARC** — free email-authentication settings configured at your domain provider; they stop attackers spoofing your address.
- **Built-in security alerts** — Google Workspace and Microsoft 365 nonprofit plans include sign-in alerts and basic monitoring at no cost; switch them on.
- **Have I Been Pwned** — free service to check whether staff emails have appeared in known data breaches, and to monitor your domain.

Do this first

Configure SPF, DKIM and DMARC on your email domain this month — it is free and is the strongest single defence against phishing that impersonates your organisation.

Module 7

The human firewall — awareness & training

Why it matters

Technology fails at the keyboard. **30.4% of CSOs provide no security awareness training**, which turns every untrained staff member into a way in. Because the dominant attack on the non-profit sector is social engineering, training is not optional — it is a frontline control, and one of the cheapest.

What good looks like

- ☐ Every staff member and volunteer completes basic security awareness training on joining.
- ☐ Staff can recognise phishing, fake login pages, and social-engineering phone calls.
- ☐ Everyone understands the password, MFA and device rules and why they exist.
- ☐ Refresher training runs at least once a year, with simulated phishing where possible.
- ☐ Lessons from any incident are shared so the whole team learns.

Tools that help

- **Ayeta games and quiz** — Ayeta includes engaging games and a knowledge quiz that make digital-security learning accessible and memorable for non-technical staff.
- **Ayeta guides in local languages** — available in Hausa, Igbo, Yoruba, Swahili, French and English, so training reaches every team member in their own language.
- **Short internal phishing drills** — send a harmless test email occasionally and coach, do not blame, anyone who clicks.

> **Do this first**
>
> Run a 45-minute team session using Ayeta's materials and quiz this quarter — awareness is the control with the highest return for the lowest cost.

Module 8

Incident response & reporting

Why it matters

When — not if — something goes wrong, a written plan turns panic into procedure. **32.1% of CSOs have no incident response plan**, and many would not know they had been breached, nor how to report it. The Nigeria Data Protection Act 2023 requires breaches to be notified, so the ability to detect, contain and report is a legal duty, not just good practice.

What good looks like

- ☐ A one-page incident response plan names who to call, what to do, and in what order.
- ☐ Staff know how to report a suspected incident immediately, without fear of blame.
- ☐ You know your NDPA breach-notification obligations and have a template ready.
- ☐ The plan is tested at least once a year with a simple tabletop exercise.
- ☐ You know where to report digital rights violations and document online abuse.

Tools that help

- **Ripoti (PIN)** — a confidential platform to report and document digital rights violations in Africa; identities are not made public.
- **FeedShield (PIN)** — a toolkit to document online abuse and harassment and unmask coordinated trolling against your staff or organisation.
- **NDPC breach reporting** — know the Commission's notification route and timelines; keep a pre-drafted notice so you can act fast.

> **Do this first**
>
> Write your one-page incident response plan and pin it where staff can see it — then run a 30-minute "what if our email is hacked?" tabletop this quarter.

Module 9

Physical & environmental resilience

Why it matters

Digital protection fails if someone can walk off with the hardware, or if power and connectivity are unreliable. **Physical access was the lowest-scoring area in the assessment (42.7%)**, partly because many CSOs share or lack dedicated offices. Scale these controls to your situation — a co-working desk needs different measures from an owned building.

What good looks like

- ☐ Doors and windows lock; sensitive equipment is not left unattended in shared spaces.
- ☐ Servers, routers and backup drives are kept in a restricted, lockable location.
- ☐ There is a visitor and lock-up routine for the workspace.
- ☐ Reliable power backup (inverter/UPS) protects against outages and data loss.
- ☐ A plan exists for working through extended power or network failure.

Tools that help

- **Power backup (UPS/inverter + surge protection)** — prevents the sudden shutdowns that corrupt files and damage equipment.
- **Cloud-first working** — keeping work in encrypted cloud storage means a stolen or damaged device does not equal lost data.
- **Scaled physical checklist** — match controls to your office type: owned building, shared office, or fully remote/co-working.

> **Do this first**
>
> Move your single most important data off any one physical device and into encrypted cloud storage this week, so no theft or fire can erase it.

Module 10

Operating in a hostile civic space

Why it matters

Beyond ordinary cyber-risk, Nigerian CSOs face threats aimed squarely at their freedom to associate, speak and organise: broadly-drawn cyber laws, surveillance, internet shutdowns, SIM-linked de-anonymisation, online harassment and gendered abuse, platform takedowns, and disinformation. These are **rights threats, not just security threats** — and the companion assessment validated them against the Constitution's Section 40, ICCPR Article 22 and the African Charter. The encouraging news is that the same baseline controls that protect your systems also protect your rights; only a few additional, people-centred practices are needed.

What good looks like

- ☐ Staff understand their exposure under the Cybercrimes Act and know to seek legal support early, not after charges.
- ☐ High-risk roles have a simple threat model and stronger protection — app-based authentication (not SMS), and encrypted messaging.
- ☐ The organisation keeps off-platform channels it owns (a website and an email list), so a takedown cannot silence it.
- ☐ Staff facing online harassment or gendered abuse have a clear, trauma-informed reporting and support route.
- ☐ A legal contact or rapid-response relationship is agreed before it is needed.
- ☐ Shutdown contingency (Module 5) and lawful data handling under the NDPA (Module 4) are both in place.

Tools that help

- **Ayeta (PIN)** — guidance on surveillance, shutdowns and protecting digital rights defenders, plus a directory of digital-security actors and an events calendar that connect you to the wider support ecosystem.
- **Ripoti (PIN)** — confidentially report and document digital rights violations, including legal harassment of staff.
- **FeedShield (PIN)** — document coordinated online abuse and unmask trolling directed at your staff or organisation.

- **Kuram (PIN/Hivos)** — research-based resources and justice pathways for online gender-based violence, with TechHer-led digital literacy; use it where staff are targeted because of gender or identity.
- **Signal + app-based authentication** — encrypted messaging for sensitive work, and app-based (not SMS) MFA to break the SIM-to-identity link created by NIN–SIM registration.

Do this first

For any staff member whose work or identity carries heightened risk, switch their key accounts to app-based authentication and Signal this week, and agree a legal contact to call if they are threatened — advice here must be legally aware and trauma-informed, so consult specialists rather than applying generic guidance.

Module 10 add-on

How the toolkit operationalises FA1–FA6

The companion assessment (Section 10.4) makes six freedom-of-association recommendations. The crosswalk below shows where in this toolkit each one is operationalised, so the assessment's rights findings translate directly into action.

Table 2: How the toolkit operationalises FA1–FA6

Rec.	Freedom-of-association recommendation	Where in this toolkit
FA1	Frame the Minimum Digital Security Baseline as a civic-space safeguard, led by data minimisation.	Section 3 (the eleven-point Baseline as a worksheet) and Module 4, which now opens with data minimisation as the highest-value control.
FA2	Role-based threat modelling and stronger protection for high-risk staff.	Module 2 (app-based MFA over SMS) and the new Appendix B — a role-based threat-model tier worksheet for assigning staff to Standard, Elevated or High protection.
FA3	A legal rapid-response and digital-rights defence capability.	Module 10 above (legal contact agreed before it is needed) and Appendix A, where the incident response quick card now carries a dedicated legal rapid-response contact field.
FA4	Safeguarding for online harassment and gendered violence.	Module 8 (reporting and Ripoti/FeedShield) and the new Appendix C — a policy outline for adopting safeguarding provisions covering online harm, trauma-informed and legally aware.
FA5	Protect operational and communicative continuity against shutdowns and takedowns.	Module 5 (shutdown contingency and OONI Probe) and Module 4 (data ownership and the NDPA cross-border caveat).
FA6	Mainstream the civic-space lens into NNNGO's advocacy and monitoring.	Section 12.1 sets out NNNGO's convening and advocacy role, including the EU-SEE Snapshot link and the next-wave survey additions.

Use the worksheets together

Before delivering Module 10 advice to specific staff, complete Appendix B (role-based threat-model tier worksheet) so that protection is proportionate to actual exposure.

If your organisation does not yet have a staff-welfare or safeguarding policy that covers online harm, adopt the outline in Appendix C this quarter — it is the fastest way to operationalise FA4.

Module 11

Tool directory

Every tool below is free or available at no extra cost to non-profits, and is widely trusted in the human rights and civil society community. Paradigm Initiative's own tools (shaded) are the anchor of this toolkit. This is guidance, not endorsement: confirm that each tool still meets your needs and check its current status before relying on it.

Table 3: Recommended tools, mapped to the gaps they close

Tool	What it does	Closes which	Cost
Ayeta (PIN)	Core digital security toolkit: guides, games, quiz, security goal-setting; multilingual.	Whole programme; training; shutdowns	Free
Ripoti (PIN)	Confidential reporting and documentation of digital rights violations.	Incident response (M8)	Free
Londa (PIN)	Annual digital rights & inclusion report for Africa; advocacy evidence	Governance, board briefing (M1)	Free
FeedShield (PIN)	Document online abuse and unmask coordinated trolling.	Incident response; civic space (M8/M10)	Free
Kuram (PIN/Hivos)	Resources and justice pathways for online gender-based violence.	Civic space; staff protection (M10)	Free
OONI Probe	Measure and evidence internet censorship, blocking and shutdowns.	Network & civic space (M5/M10)	Free / open-source
Bitwarden / KeePassXC	Password managers for strong, unique passwords.	Identity (M2)	Free / open-source
Aegis / Authenticator apps	App-based multi-factor authentication.	Identity (M2)	Free

Tool	What it does	Closes which	Cost
Signal	End-to-end encrypted messaging and calls.	Data in transit (M4/M5)	Free / open-source
Tor Browser / Psiphon	Circumvent blocking; protect browsing	Network resilience (M5)	Free
Cryptomator / VeraCrypt	Encrypt files on devices and in the cloud.	Data protection (M4)	Free / open-source
Windows Defender / ClamAV	Anti-malware on computers	Endpoint (M3)	Free
Google / Microsoft MDM	Remotely lock or wipe lost devices; basic monitoring.	Endpoints, detection (M3/M6)	Free with nonprofit plan
SPF / DKIM / DMARC	Email authentication that stops spoofing/phishing.	Detection (M6)	Free
Have I Been Pwned	Check if staff emails appear in known breaches	Detection (M6)	Free

Getting the PIN suite

Ayeta toolkit and downloads: ayeta.africa · paradigmhq.org/ayetadownload (English, French, Hausa, Igbo, Swahili, Yoruba).

Ripoti (reporting), Londa (report) and FeedShield: via paradigmhq.org.

OONI Probe: ooni.org — install on Android, iOS or desktop.

Module 12

Your 90-day resilience plan

Resilience is built in stages, not in a single push. Use this 90-day plan as a starting template and adjust it to your tier and capacity. Record each action in Ayeta's security goal-setting tool so progress is visible to your leadership.

Table 4: A 90-day starting plan (adapt to your tier)

Window	Foundation (do regardless of tier)	Build (as capacity allows)
Days 1–30	Download Ayeta. Turn on MFA for main email. Switch on device encryption and screen-lock. Make one tested encrypted backup.	Draft your one-page security policy. Name a security owner and DPO. Install OONI Probe. Agree a legal rapid-response contact (FA3) and record it on the Appendix A card.
Days 31–60	Roll out a password manager and MFA org-wide. Configure SPF/DKIM/DMARC. Enable anti-malware everywhere.	Run a 45-minute Ayeta awareness session. Register with the NDPC; begin NDPA review. Write joiners/leavers checklist. Complete the role-based threat-model tier worksheet (Appendix B; FA2) and switch high-risk staff to app-based MFA and Signal.
Days 61–90	Finalise the 3-2-1 backup routine and test a restore; cut data fields you do not need (FA1). Approve the security policy at leadership level.	Write and pin a one-page incident response plan; run a tabletop drill. Set sign-in alerts. Adopt the safeguarding outline in Appendix C (FA4). Re-assess against the Baseline.

At day 90, re-score yourself against the eleven-point Baseline in Section 3. You should have moved up at least one tier. Repeat the cycle every quarter until you reach — and can sustain — the Mature tier.

12.1 Where NNNGO and the sector come in

No small CSO should face this alone. Several controls — managed anti-malware, mobile device management, monitoring, and backup — are cheaper and stronger when CSOs act together. NNNGO's role is to convene that collective response: to publish the Baseline as a member standard, to broker shared services, and to connect members to Paradigm Initiative's Ayeta community and the wider digital rights ecosystem. If you are stuck, reach out through NNNGO rather than going without.

Appendix A: Incident response quick card

Print this page, fill in the blanks, and pin it where your team can see it. In an incident, work top to bottom and stay calm — a slow, correct response beats a fast, panicked one.

Step 1 — Recognise & report
Anyone who suspects an incident (lost device, suspicious email clicked, account acting strangely, data exposed) reports it immediately to:

Security owner: _____ *Phone:* _____

Data Protection Officer: _____ *Phone:* _____

Legal rapid-response contact (FA3): _____ *Phone:* _____

Step 2 — Contain

- Disconnect the affected device from the internet.
- Change the passwords of any accounts that may be affected, from a clean device.
- Do not delete anything — you may need it as evidence.

Step 3 — Assess

- What happened, when, and what data or accounts are involved?
- Is personal or beneficiary data exposed? If yes, NDPA breach-notification may apply.
- Is a staff member being threatened, harassed, or facing legal action? If yes, call the legal rapid-response contact immediately.

Step 4 — Notify & report

- Notify leadership and, if personal data is involved, prepare an NDPC notification.
- Report digital rights violations via Ripoti; document online abuse via FeedShield.
- If it is an internet shutdown or blocking, capture evidence with OONI Probe.

Step 5 — Recover & learn

- Restore from a clean, tested backup.
- Hold a short, blame-free review: what happened, what we will change, who owns it.
- Update your policy and share the lesson with the team — and, via NNNGO, with peers.

Appendix B: Role-based threat-model tier worksheet

Not all staff face the same digital risk. This worksheet operationalises FA2 of the assessment by sorting staff into three tiers and matching each tier to a set of controls. Complete it with leadership; review it annually and whenever a staff member's work changes meaningfully.

Tier definitions and required controls

Tier	Who is typically in this tier	Required protection (in addition to the Baseline)
Standard	General programme, administrative, finance and support staff who do not routinely handle sensitive beneficiary records, contentious advocacy material, or whistleblower information.	Strong unique passwords; multi-factor authentication on all important accounts (app-based preferred); device encryption and automatic lock; security awareness training; agreed reporting route.
Elevated	Staff handling sensitive beneficiary data; case workers; field staff in sensitive locations; staff with elevated system privileges; communications/social-media leads; staff with public profile.	All of Standard, plus: app-based MFA mandatory (no SMS); mobile device management enrolled; encrypted messaging (Signal) for work involving identifiable beneficiaries; quarterly security check-in.
High	Leadership; investigators and researchers on contentious issues; staff at heightened risk due to identity or the nature of their work; anyone receiving credible threats; staff handling whistleblowers or litigation material.	All of Elevated, plus: hardware security keys where feasible; named legal rapid-response contact; rehearsed shutdown contingency; review of public footprint; trauma-informed support pathway via leadership.

Staff assignment worksheet

Print this table; list each staff member and assign a tier. Review with the security owner and leadership; revisit at least annually.

Name	Role	Tier	Reviewed

Notes on use

Most organisations will have most staff in Standard; only a small share should be in High.

Tiering is about exposure, not seniority — a field researcher can be High while a director is Standard.

If you are uncertain, place the person in the higher tier; over-protection is cheaper than under-protection.

Reassess after any significant change — new programme, new threat, new role, or after any incident.

Appendix C:

Safeguarding for online harm — policy outline

This appendix operationalises FA4 of the assessment. Most CSOs already have a safeguarding policy for beneficiaries; few extend it to cover online harm against their own staff. Use the outline below to draft, adopt and pin a short policy. Keep it concise (two to three pages) and review it annually — a brief, used policy beats a long, ignored one.

Section 1 — Scope and principles

- ☐ The policy applies to all staff, volunteers and consultants of the organisation.
- ☐ It covers digital harassment, threats, doxing, impersonation, coordinated trolling, sexualised abuse, gender-based and identity-based violence, and non-consensual intimate imagery.
- ☐ It commits the organisation to a trauma-informed, blame-free response that prioritises the affected person's wellbeing and agency.
- ☐ It is legally aware: advice and response options take account of the Nigerian legal environment, in particular for staff at heightened risk because of identity or the nature of their work.

Section 2 — Reporting routes

- ☐ Any staff member experiencing online harm can report it confidentially to the named safeguarding lead, with an alternative route to a board member if the harm involves the safeguarding lead.
- ☐ Reporting is welcomed, never penalised; the staff member retains control over whether and how to escalate.
- ☐ The organisation logs incidents (anonymised) so that patterns can be identified and addressed.

Section 3 — Immediate response

- ☐ Document the harm using FeedShield or screenshots and metadata, preserving evidence before reporting it to the platform.
- ☐ Offer the affected person psychosocial support; do not require them to keep working on the matter that drew the abuse.
- ☐ Review and, where appropriate, harden the person's digital protection in line with their tier (Appendix B).
- ☐ If criminal threats are made, consult the legal rapid-response contact before approaching the police.

Section 4 — Specialist resources

- ☐ Use Paradigm Initiative's Kuram for online gender-based violence (research-based resources and justice pathways).
- ☐ Use FeedShield to document coordinated abuse and trolling and, where it informs the response, Ripoti to record the incident as a digital-rights violation.
- ☐ Where mental-health support is needed, refer to a vetted psychosocial-support provider (do not rely on informal contacts only).

Section 5 — Learning and prevention

- ☐ Hold a brief, blame-free review after any incident: what happened, what we changed, who owns the follow-up.
- ☐ Build digital harassment into onboarding and into refresher awareness training (Module 7), and brief leadership on patterns at least annually.
- ☐ Where staff are repeatedly targeted because of a specific campaign, consider sector coordination through NNNGO and connection to specialist civil society networks.

This toolkit is a companion to the NNNGO Digital Risk Assessment (May 2026) and draws on Paradigm Initiative's Ayeta digital security toolkit and companion platforms. Tool references are for guidance only and should be verified before use.

About Nigeria Network of NGOs

The Nigeria Network of NGOs (NNNGO) is the first generic membership body for civil society organisations in Nigeria that facilitates effective advocacy on issues of poverty and other developmental issues. Established in 1992, NNNGO represents over 4,049 organisations ranging from small groups working at the local level, to larger networks working at the national level.

The Network is charged with the objective of identifying, registering, coordinating, building capacity and mobilizing civil society organisations to promote interconnectivity and bring equity, justice, peace, and development to grassroots communities throughout Nigeria, including the implementation of the Sustainable Development Goals (SDGs).

This Digital Resilience Toolkit was developed by the Nigeria Network of NGOs for the Civil Society Organisations (CSOs). Its contents are the sole responsibility of the Nigeria Network of NGOs.

https://nnngo.org

@nnngo

nnngo@nnngo.org