Annex IV of Regulamento n.º 756/2026

the measures for relevant public entities, group by group

1 October 2026

Portugal's NIS2 transposition, the Regime Jurídico da Cibersegurança (RJC), treats public administration separately. A public body that is not qualified as an essential or important entity is a relevant public entity (entidade pública relevante): it gets no conformity level and does not apply Annex III. It applies the measures in Annex IV of the CNCS's Regulamento n.º 756/2026, according to whether it falls in Group A or Group B. Annex IV runs to five pages of the Diário da República, and this note reads it measure by measure.

Who is in each group

The groups are defined in Decreto-Lei n.º 125/2025, not in the Regulamento (RJC, art. 7). **Group A** covers direct-administration services with 250 or more workers, indirect and autonomous administration with more than 250, public business entities above the SME thresholds, independent administrative bodies, and also the Economic and Social Council, the Ombudsman, the services of the Presidency, Parliament and the courts, and the judicial councils (CSM, CSTAF and CSMP). **Group B** covers direct, indirect and autonomous administration with 75 to 249 workers, and public business entities that are medium-sized.

Banco de Portugal, the CMVM and the ASF are outside the regime as independent administrative bodies (RJC, art. 3(3)). A body that fits more than one category goes into the most demanding one (art. 9), and a public body whose remit is ICT infrastructure, or with particularly high digital integration, can be qualified as an essential entity (art. 6(1)), in which case it moves from Annex IV to Annex III.

The two-year window

The duty to apply the Annex IV measures (RJC, art. 33) and the fine for not doing so (art. 61(1)(f)) take effect 24 months after the regime's implementing regulation is published (DL, art. 10(2)). With Regulamento n.º 756/2026 published on 22 June 2026, that date is **22 June 2028**. The calculation assumes the Regulamento is all the regulation the article refers to, and the Regulamento itself adds that provisions depending on CNCS technical instructions take effect only when those are published (Reg., art. 35(2)).

The window does not cover everything. The duty to register (RJC, art. 35) and the duty to notify any significant incident (art. 40) also apply to relevant public entities and are not on the list of deferred effects, so they do not wait for 2028. Once the window closes, failing to apply the measures is a very serious offence: €16,000 to €4,000,000 in Group A and €8,000 to €350,000 in Group B, for the legal person (art. 61(2)).

Address
Rua Major João Luís de Moura
Piso 1, Esc. AE · 1685-253 Famões

Contact
hello@deltacoders.com

Web
deltacoders.com

Group B: eighteen measures

Annex IV sets out each group as a table with three columns: the area, the measure and the verification criterion. The criterion is the column that matters, because it says what a supervisor will ask to see. Of the eighteen Group B measures, eight ask for technical evidence, and the other ten for a document, a record or an inventory.

Measure	What it asks	Verification criterion
O.CRI Incident-response point of contact	A named person able to answer outside requests and, where needed, reachable outside office hours.	Documentary evidence of the point of contact.
O.IAC Inventory of critical assets	The assets critical to the main activity and the dependencies between them, in an inventory updated regularly.	An up-to-date inventory of critical assets.
O.GAP Access and permission management	Every access granted, changed or revoked goes through a request and an approval.	Evidence of the requests and their approvals.
O.GEC Computer equipment management	Issuing and collecting equipment documented and kept up to date.	A documented record of issue and collection.
O.PSF Supplier security policy	An inventory of the suppliers with access to information systems, with their contacts for incident notification.	Documentary evidence of the supplier list.
T.GPT Systems, applications and workstation management	Security controls applied to systems, applications and workstations.	Technical evidence that those controls are in place.
T.PPT Workstation protection	Antivirus installed on workstations and servers.	Technical evidence of the installation.
T.AR Remote access to the entity	Remote access through a secure mechanism (VPN or VDI, for example) and with a second authentication factor.	Technical evidence of the mechanism and the second factor.
T.PAS Segregated administration profile	Separate users for application use and for administration.	Documented evidence that the accounts are segregated.

Measure	What it asks	Verification criterion
T.AS Security updates	Manufacturers' recommended security updates applied promptly to operating systems and software on workstations and servers.	A documented record of the updates.
T.PEW Email and web service protection	Good security practice for email and web pages.	Technical evidence of email authentication, and of secure protocols and digital certificates on the web pages.
T.CS Backups	Backups taken, and usable when needed.	Technical evidence that backups run.
T.RAR Log collection and storage	The default logs enabled on operating systems, applications and other devices.	Technical evidence that they are enabled.
T.PPL Logical perimeter protection	Perimeter protection of the infrastructure.	Technical evidence of logical security measures on the equipment.
T.PPF Physical perimeter protection	Physical protection of the spaces housing critical infrastructure, such as a data centre.	Technical evidence of physical security measures in those spaces.
T.MA Authentication mechanisms	A policy that keeps passwords as strong as the operation requires.	Evidence the policy is applied on the platforms.
H-PF Awareness and training	Cybersecurity awareness or training sessions.	A documented record of the sessions.
H.FIC Information sources and communication channels	Regular reading of trustworthy sources on threats, and access to channels that share them.	Evidence of the research and dissemination channels.

Address
Rua Major João Luís de Moura
Piso 1, Esc. AE · 1685-253 Famões

Contact
hello@deltacoders.com

Web
deltacoders.com

Group A: twenty-two more

Group A has no list of its own that replaces Group B's: it applies the eighteen Group B measures and adds the twenty-two in its own table (Reg., art. 30(3)), forty in all. Five of the twenty-two are policies with the same criterion, "approved and implemented", and nine ask for technical evidence.

Measure	What it asks	Verification criterion
O.PSI Cybersecurity policy	A policy that sets out the entity's commitment to cybersecurity.	Policy approved and implemented.
O.IAC Asset inventory	All assets, not only the critical ones, with the dependencies between them, in an inventory updated regularly.	A complete, up-to-date asset inventory.
O.PAP Access and permission policy	An access and permission management policy, defined and implemented.	Policy approved and implemented.
O.GEC Computer equipment management	Personal devices kept apart from corporate ones.	Technical evidence of network segregation.
O.PUA Acceptable use policy	An entity-wide policy made known to all staff, with requirements for the confidentiality and integrity of files exchanged with other entities.	Policy approved and implemented.
O.PP Password policy	A password management policy.	Policy approved and implemented.
O.PCF Information classification	A process with sensitivity criteria or levels for the entity's data.	A documented record of the classification.
O.GMO Organisational change management	ICT procedures for staff joining, changing role and leaving, kept in step with human resources.	A documented record of the procedures.
O.ID Critical functions or activities	The critical functions identified, with their dependencies on ICT.	A record of the functions, the assets behind them and the dependencies between them.

Measure	What it asks	Verification criterion
O.PSF Supplier security policy	A policy with a supply-chain risk assessment and acceptance criteria.	Policy approved and implemented.
T.PPT Workstation protection	Access control on workstations, and backups of the information on them.	Technical evidence of the access control and the backups.
T.PPT Work profile on mobile devices	Corporate information reached only through a work profile on the mobile device.	Technical evidence of the work-profile configuration.
T.GP Password management	Privileged-access passwords stored in a password management solution.	Technical evidence of the solution.
T.PAD Differentiated access privileges	Access granted on need to know and least privilege, in line with the access policy.	A record of access by job profile.
T.AS Security updates	Manufacturers' recommended updates, now on hardware as well.	A documented record of hardware updates.
T.AM Multi-factor authentication	MFA switched on for critical applications.	Technical evidence of MFA.
T.PEW Email and web service protection	The same good practice, with stricter criteria.	Technical evidence of email authentication and validation, secure protocols, digital certificates and security headers on the web pages.
T.CS Backups	Backups stored apart from the environment they protect.	Technical evidence that backup storage is segregated.

Measure	What it asks	Verification criterion
T.RAR Log collection and storage	Logs from operating systems, applications and other devices safeguarded.	Technical evidence of log collection.
T.SC Configuration hardening	Security practice applied to workstation, operating system and main application configurations.	Technical evidence of the practices.
H.EC Phishing exercises	Periodic exercises that test how prepared staff are.	A record of the results, conclusions and the actions taken on them.
H-PF Training plan	A cybersecurity training plan, with the processes to carry it out.	A documented record of the plans and sessions.

The code T.PPT appears twice in the Group A table, for workstation protection and for the work profile on mobile devices. That is how the published text has it; when citing either measure, give the area as well as the code.

What changes from Group B to Group A

Nine codes appear in both tables, and in almost all of them Group A goes a step further rather than repeating the ask. The inventory covers all assets instead of only the critical ones (O.IAC). Equipment management moves from a record of who holds what to a technical separation of personal and corporate devices (O.GEC). Suppliers stop being a contact list and get a policy with a risk assessment and acceptance criteria (O.PSF). Backups, as well as existing, have to be stored apart from the environment they protect (T.CS). Logs, as well as being on, have to be safeguarded (T.RAR). Updates reach hardware (T.AS), email and web protection adds email validation and security headers (T.PEW), and training moves from one-off sessions to a plan (H-PF).

The rest of the Group A table is new: the cybersecurity, access, acceptable-use and password policies, information classification, critical functions, staff changes coordinated with human resources, multi-factor authentication on critical applications, a vault for privileged passwords, hardening, and phishing exercises.

Two examples

A public institute with 120 staff. Indirect administration with 75 to 249 workers, so Group B, with eighteen measures. Our reading is that three come first, because the others depend on them or because the duty they serve already applies: the incident-response point of contact (O.CRI), because notifying significant incidents is already mandatory; the inventory of critical assets (O.IAC), because the technical measures apply to systems that have to be known first; and the list of suppliers with access to the systems, with their incident contacts (O.PSF), because an incident at a supplier is often the first one an entity has to notify.

A directorate-general with 400 staff. Direct administration with 250 or more workers, so Group A, with forty measures. What takes longest is not technical: it is the five policies the criterion wants approved and implemented, and approving a policy involves the leadership. Starting with them leaves the technical work for when the policy already says what the technical work has to meet, and the access policy (O.PAP), for example, is named outright in the T.PAD criterion.

Certification as proof

The Regulamento presumes the measures are met when the entity holds a certification that covers them, and for relevant public entities it names DNP TS 4577-1, the Selo Digital (Reg., art. 27(3)). The CNCS can also require certification, by reasoned decision (RJC, art. 34(1)). Without certification, the proof is the verification criterion, measure by measure.

Address
Rua Major João Luís de Moura
Piso 1, Esc. AE · 1685-253 Famões

Contact
hello@deltacoders.com

Web
deltacoders.com

Where we come in

We do not qualify entities or run the regime for them. Three Annex IV criteria ask for technical evidence we produce. The T.PEW criterion, email authentication, secure protocols, certificates and security headers on the web pages, is what Buteo reads from outside on each domain. The O.IAC inventory, for the network part, is what Ibex keeps per device, including on networks with no connection to the internet. And the T.AS update record gains an independent check when Ibex reads the version each service is actually running.

The full RJC calendar, the incident-notification deadlines and a self-check are on NIS2 em Portugal: o RJC, in Portuguese.

Checked on 26 September 2026 against the text of Decreto-Lei n.º 125/2025 and Regulamento n.º 756/2026 as published in the Diário da República. The measures are summarised and translated; where in doubt, the Portuguese text of Annex IV prevails.

Sources

- Decreto-Lei n.º 125/2025, of 4 December, approving the Regime Jurídico da Cibersegurança, Diário da República, 1.ª série, n.º 234: arts. 3, 6, 7, 9, 33, 34, 35, 40 and 61 of the regime; art. 10 of the decree.
- Regulamento n.º 756/2026 of the CNCS, Diário da República, 2.ª série, n.º 118, 22 June 2026: arts. 1, 27, 30 and 35, and Annex IV, pp. 85 to 89.

Address
Rua Major João Luís de Moura
Piso 1, Esc. AE · 1685-253 Famões

Contact
hello@deltacoders.com

Web
deltacoders.com