Access Control Policy

Document code	POL-014
Document name	Access Control Policy
Type	Policy
Version	1.0
Approved on	[DD/MM/YYYY]
Approved by	[Name, role — CISO]
Review cycle	Annually
Mandatory under	ISO/IEC 27001:2022 Annex A controls A.5.15 (access control), A.5.16 (identity management), A.5.18 (access rights). Related: A.8.2 (privileged access rights), A.8.3 (information access restriction).
Distribution	All personnel; managers; IT/Engineering; system owners; CISO; Internal Audit
Compliance scope	Strategic policy on identity, authorisation, and access — what access exists, how it is granted and reviewed. Authentication mechanics live in the Authentication Policy; password specifics in the Password Policy. Implements Annex A.5.15/5.16/5.18.

Revision history

Version	Date	Description
1.0	[DD/MM/YYYY]	Initial version — ISO 27001 edition (content aligned with NIS-2 source document of the Docply library).

1. Purpose

This Policy defines the approach of [Organisation] to identity and access. Annex A control A.5.15 of ISO/IEC 27001:2022 requires rules to control physical and logical access to information and other associated assets, established and implemented based on business and information security requirements. Access control determines what each person and system can do — done well it limits the blast radius of compromised accounts and enforces accountability; done badly it grants standing privileges that compound over years.

2. Scope

This Policy covers access to all IT systems, applications, data, and physical zones of [Organisation]. It applies to personnel, contractors, suppliers with system access, and to non-human identities (service accounts, API clients, machine identities). Physical access controls are aligned with this Policy in principle.

3. Principles

Principle	Application
Least privilege	Each identity has the minimum access required to perform its function. Privileges are explicit, scoped, and time-bounded where appropriate.
Need-to-know	Access to Confidential and Restricted data is granted only when required for the role's function; mere employment is not sufficient.
Separation of duties	Sensitive end-to-end actions are split such that no single identity can complete them unsupervised (e.g. developer cannot deploy to production unattended; payment authoriser cannot also be the requestor).
Identity-based, not network-location-based	Access is decided on identity and posture, increasingly independent of network location. Network controls remain a layer; they are not the sole gate.
Regular review	Access is not granted once and forgotten. Reviews are scheduled and risk-based.

4. Identity types

Type	Treatment
Human — employee	Tied to HR record. Lifecycle aligned with employment (joiner-mover-leaver per HR security policy).
Human — contractor / temporary	Tied to contract. Default expiry at contract end; renewal is explicit. Sponsor (employee) is accountable.
Human — supplier (vendor staff)	Per supplier contract. Time-limited; reviewed per supplier review.
Service account / non-human	Distinct from human accounts. Owner is a named role/team. Authentication via certificates or short-lived tokens preferred over long-lived secrets.
Shared account (where unavoidable)	Discouraged. Where unavoidable, wrapped in privileged access management with audited individual access; not used directly by humans.

5. Access provisioning

- Request. Access requests are submitted via the access request system, with identity, requested access, business justification, requested duration where appropriate.
- Approval. Approved by the data/system owner or delegate. Privileged access requires CISO endorsement. Sensitive data access requires data owner approval.
- Provisioning. Automated where possible (joiner workflows, group membership). Manual steps are tracked.
- Notification. The user is informed of the access granted and acknowledges acceptable use.

6. Role-based access

Default access is role-based — defined sets of access aligned with job roles. Role definitions are owned by the relevant function and reviewed annually. Exceptions to role defaults are tracked individually with justification.

7. Privileged access (A.8.2)

- Privileged access (administrators, root, database owners, cloud admins) is granted only when justified by role.
- Privileged access uses multi-factor authentication per the Authentication Policy.
- Privileged access is reviewed at least quarterly. Privileges not used in the period are presumed unnecessary unless justified.
- Privileged actions are logged. Just-in-time / just-enough access models are preferred where supported.
- Break-glass accounts are stored under dual control and use is logged and reviewed.

8. Access review (A.5.18)

Scope	Cadence
Privileged access (admin, root, sensitive systems)	Quarterly
Access to Confidential or Restricted data	Quarterly for Restricted; semi-annually for Confidential
General access (Internal data, standard systems)	Annually
Service / non-human identities	Annually with credential rotation review
Stale accounts (no login for [N] days)	Monthly automated flagging

Reviews are conducted by the system owner with attestation; outcomes are recorded; access not re-attested is removed.

9. Joiner-mover-leaver

- Joiner. Access provisioned to start with the role on day one — not earlier, not later.
- Mover. On role change, access is reassessed: additions for the new role, removals of access not relevant to it.
- Leaver. Same-day deprovisioning: accounts disabled on last working day; disabled (not deleted) for [90] days for evidential purposes; deleted thereafter.
- Suspended employment. On suspension or under-investigation, access is suspended pending review.

10. Compliance and exceptions

Compliance is verified by the CISO via measurement and Internal Audit. Exceptions require CISO approval.

References

Reference	Subject
ISO/IEC 27001:2022 A.5.15	Access control
ISO/IEC 27001:2022 A.5.16	Identity management
ISO/IEC 27001:2022 A.5.18	Access rights
ISO/IEC 27001:2022 A.8.2 / A.8.3	Privileged access; access restriction
POL-015 Authentication Policy	Authentication mechanics
Password Policy	Password specifics
Information Classification Policy	Drives access granularity
ISMS-DOC-04 Statement of Applicability	Control selection
POL-001 Policy on Information System Security	Top-level policy framework

Approval

Approved by: [Name, role — CISO] **Date:** [DD/MM/YYYY] **Signature:** _____