DOC-SEC-0004 - Privileged Access Standard

Document ID: DOC-SEC-0004
Owner: CISO
Approver: CIO
Version: 1.7
Status: Published
Effective date: 2025-09-01
Review date: 2026-09
Applicability: All staff holding or requesting elevated access to Compass One or customer systems
Source system: Policy repository; privileged access management platform

Fictional document created for the GS Reference Enterprise. Not real policy.

PURPOSE

Elevated access concentrates risk. This standard sets how privileged access is defined, granted, bounded in time, monitored, and removed, so that elevation is always traceable to a named person acting on a stated business need.

DEFINITION OF PRIVILEGED ACCESS

Privilege is determined by what a credential can do, not by the job title of the person holding it.

- Privileged access is any credential that can alter security controls.
- Administrative access to customer production systems is always privileged.
- Access that can read an entire customer dataset is treated as privileged.
- Compass One grants privileged access only through a named individual account.
- Shared administrator credentials are prohibited across all Compass One systems.

GRANTING ELEVATED ACCESS

Standing privilege is avoided wherever a just-in-time elevation path exists. Requests are reviewed against the role profile maintained under DOC-IT-0002.

- A privileged access request requires manager approval with Security review.
- The requester must state a specific business justification for every elevation.
- Privileged sessions are limited to four hours by default.
- Elevation beyond eight hours requires CISO approval.

SESSION CONTROLS

- All privileged sessions must originate from a managed Compass One endpoint.
- Privileged access from personal devices is prohibited.
- Every privileged session is recorded in the privileged access management platform.
- Session recordings are retained for eighteen months.

MONITORING AND REVOCATION

Review is continuous rather than annual. Inactivity is treated as evidence that the access is no

longer needed.

- Security must review privileged access grants each quarter.
- Unused privileged access is revoked after thirty days of inactivity.
- Privileged access is revoked within one hour of an employment termination notice.
- A transferring employee loses privileged access on the effective transfer date.

EMERGENCY ACCESS

- Break-glass credentials are sealed in the emergency vault.
- Any break-glass use must be reported to the CISO within one hour.
- Security must rotate a break-glass credential immediately after use.

OWNERSHIP AND REVIEW

- The CISO owns this standard.
- Compass One reviews this standard each September.