no-platform-data-on-personal-devices-policy.md

No Platform Data on Personal Devices Policy

Purpose

- Ensure that platform data (user content, PII, or platform backups) are not stored on personal devices unless explicitly approved and encrypted.

Policy

- No platform production data shall be copied or stored on personal devices (laptops, phones, removable media) without pre-approved, documented justification and security controls (full-disk encryption + company-managed device).
- Access from personal devices must be via approved remote sessions or web consoles that do not cache data locally.

Enforcement and Evidence

- Access logs are retained and reviewed weekly. Automated alerts are raised for bulk export or unusual data access patterns and create tickets.
- Evidence provided: sample access log output, alert ticket example, and a short description of the protective controls (no local backups policy, DLP/console controls).

Exceptions

- Exceptions require written approval from security and are time-limited.

Contact

- security@autopromote.example