SCREEN LMS

Screen LMS Cookie and Similar Technologies Notice

Explains strictly necessary session cookies and any separately enabled analytics or preference technologies.

LEGAL AND ASSURANCE STATUS: Operational draft for implementation and UAT. It has not been represented as approved by Singapore-qualified counsel, an accredited certification body or an external auditor.

Document code	COOKIE-001	**Version**	1.0
Effective date	2026-07-12	**Next review**	2027-07-12
Owner	Data Chord Pte. Ltd.	**Audience**	all
Status	Pending review by Singapore-qualified counsel and the appointed DPO	**Acknowledgement**	Notice / point-of-use control

Change history

Version / effective date	Change	Owner	Approval status
1.0 / 2026-07-12	New cookie and browser-storage transparency notice.	Data Chord Pte. Ltd.	Pending required approval and legal review

Controlled copy: the current LMS-published version. Printed or forwarded copies are uncontrolled. A material change creates a new version; earlier versions and acceptance evidence are preserved.

Purpose and scope

Explains strictly necessary session cookies and any separately enabled analytics or preference technologies.

This document applies to Screen LMS application operations, relevant Azure services, authorised users, administrators, service providers and records within its stated audience.

Governance principles

- Apply Singapore law, contractual commitments and approved organisational policy using documented, risk-based decisions.
- Use data minimisation, least privilege, separation of duties and secure defaults.
- Preserve evidence sufficient to demonstrate what was decided, implemented, tested and reviewed.
- Escalate uncertainty; do not treat this operational draft as legal advice or certification evidence by itself.

Roles and responsibilities

- The document owner maintains this controlled version, monitors changes and initiates review after a material legal, technical, supplier or business change.
- Managers assign accountable control owners, approve resources and review significant exceptions, risks, incidents and overdue actions.
- Users and authorised suppliers follow the policy, complete required training, protect credentials and report suspected incidents or nonconformities promptly.
- The Data Protection Officer reviews personal-data implications and the security owner reviews confidentiality, integrity and availability implications.

Essential technologies

Screen LMS uses essential session, security, continuity and interface storage needed to authenticate users, preserve authorised navigation, prevent abuse and remember non-sensitive preferences. Disabling essential storage may prevent the service from functioning.

Optional technologies

Analytics, advertising or third-party embedded technologies are not treated as essential. Before activation, the owner must document purpose, provider, data, duration, transfer, consent or preference mechanism and withdrawal route.

Browser controls

Users can remove browser storage through their browser. The policy centre and cookie inventory must be updated when technologies change, and material changes trigger a new controlled version.

Current essential storage inventory

- Session cookie: maintains authenticated session state; HttpOnly, SameSite and Secure attributes are applied according to deployment settings.

- Continuation and security tokens: short-lived state used for secure post-login destinations or one-click actions.
- Interface storage: limited browser-side state may remember non-sensitive display preferences.
- The production owner must document any new analytics, advertising or embedded-service cookie before enabling it.

Records and evidence

- Keep the approved version, superseded versions, approval record, publication record, acceptance evidence where required, training evidence, exceptions and review decisions.
- Apply role and tenant access restrictions, protect evidence from unauthorised change, and use the approved retention and secure-disposal schedule.
- Do not place secrets, passwords, access tokens or unnecessary personal data in governance evidence or issue trackers.

Monitoring, exceptions and review

The owner reviews the policy at least by the scheduled date and after a material incident, audit finding, law change, supplier change, architecture change or significant processing change.

- Record each exception with business justification, affected assets or data, risk, compensating controls, approver, owner, expiry and review date.
- Track findings and overdue actions through the corrective-action process and verify effectiveness before closure.
- A material change creates a new controlled version. Where the policy is an access condition, the LMS presents the new version for renewed acceptance while preserving earlier evidence.

Official sources and external references

Sources were checked during the 12 July 2026 policy refresh. The document owner must verify the current official version during every review. A source citation does not mean the issuing body has approved Screen LMS or this document.

- **Attorney-General's Chambers, Singapore: Personal Data Protection Act 2012 (Singapore Statutes Online)** — https://sso.agc.gov.sg/Act/PDPA2012
- **Personal Data Protection Commission: Advisory Guidelines on Key Concepts in the PDPA (revised 29 April 2026)** — https://www.pdpc.gov.sg/organisations/regulations-decisions/regulatory-guidance/advisory-guidelines-on-key-concepts-in-the-personal-data-protection-act

Approval and review record

Role	Name	Decision / date	Notes
Document owner	To be completed	Pending	Required before representing this document as fully approved
Information security	To be completed	Pending	Required before representing this document as fully approved
Data Protection Officer	To be completed	Pending	Required before representing this document as fully approved
Singapore-qualified legal reviewer	To be completed	Pending	Required before representing this document as fully approved