

Data Classification & Handling Policy

How we classify data by sensitivity and the handling rules for each level.

Version: 1.0 · Last updated: December 2025 · Owner: Security Lead

1. Purpose

To ensure data is classified by sensitivity and handled with appropriate controls.

2. Classification levels

- **Public.** Information intended for public release (e.g. marketing content).
- **Internal.** Day-to-day business information not intended for public release.
- **Confidential.** Customer account data, the analytics and content managed in Backpack OS, client source code and designs, and business-sensitive information.
- **Restricted.** Secrets, credentials, personal data subject to legal protection, and website-visitor data collected through the customer snippet.

3. Handling rules

Level	Storage	Sharing	Encryption
Public	Any approved system	Unrestricted	Optional
Internal	Approved systems	Internal only	In transit
Confidential	Approved systems, access-controlled, isolated per organization	Need-to-know	In transit & at rest
Restricted	Secrets manager / encrypted store	Strictly need-to-know	In transit & at rest

4. Responsibilities

All personnel must classify data they create or handle and apply the corresponding controls. Customer and website-visitor data is processed only as needed to provide the service.

5. Review

This policy is reviewed at least annually.