INTELLISYNC SOLUTIONS

STRUCTURE - CLARITY - BETTER DECISIONS

DATA ACCESS

AI Data Classification and Access Matrix

A worksheet for defining what information AI may access, restrict, retain, or escalate.

WHAT THIS TEMPLATE HELPS YOU DECIDE

Map data classes, permitted use, restricted sources, role-based access, retention, expiry, and review rules before AI systems connect to operational context.

BEST FOR

- CRM and inbox-connected assistants
- HR, finance, and document systems
- Teams designing context boundaries

OUTPUTS

- Data classification table
- Permitted access rules
- Retention and expiry rules

STEP 1

Frame the operating need

Start with the workflow, decision, owner, and business pressure. The template is useful only when it is grounded in a real operating moment.

Operating frame

System or workflow
Name where AI will retrieve, read, write, or remember data.

Sensitive data class
Customer, employee, financial, confidential, regulated, or internal-only.

Access owner
Name who approves use and handles exceptions.

Readiness check

- [ ] Data classes are named before connection
- [ ] Access rules are role-aware
- [ ] Restricted sources are explicit
- [ ] Retention and expiry are visible
- [ ] Review or legal escalation is defined

STEP 2

Map the architecture questions

Use this page to separate the parts of the system that need design before anyone jumps to tools, prompts, or implementation details.

Design map

Public	Which sources can AI use freely?
Internal	Which sources are safe only inside the organization?
Confidential	Which sources require role, purpose, or approval constraints?
Sensitive	Which personal, financial, or regulated data needs strict handling?
Forbidden	Which data should never enter this AI workflow?

Context boundaries only work when data classes are visible. AI access should be governed before retrieval feels convenient.

STEP 3

Turn the answers into a brief

A strong brief makes the next decision easier: proceed, defer, redesign, govern, or assess more deeply before implementation.

Decision brief

Access rule	Who can use each data class and for what purpose?
Retention rule	What can be stored, logged, cached, or forgotten?
Escalation	When should legal, privacy, security, or leadership review be triggered?
Control gap	Which missing permission or boundary must be resolved first?