Data Classification Guide for AI Systems

SOLUTIONS24X7 · TCS FRAMEWORK   STARTER EDITION

Four-tier classification system. Apply to every data input before it reaches an AI model.

The Four Tiers

Tier	Label	Definition
🟢	**PUBLIC**	Information designed to be shared externally with no restrictions
🔵	**INTERNAL**	For internal use only. Not sensitive, but not intended for public disclosure
🟡	**CONFIDENTIAL**	Sensitive business or personal information. Restricted to authorised staff
🔴	**RESTRICTED**	Highest sensitivity. Regulatory, legal, or national security implications

Classification by Data Type

Data Type	Tier	Examples
Marketing content, press releases	🟢	Website copy, public case studies, blog posts
Published product documentation	🟢	User manuals, public API docs, help centre articles
Internal process documentation	🔵	SOPs, team wikis, non-sensitive meeting notes
Business performance data	🔵	Non-sensitive KPIs, project status, team metrics
Customer records, contracts	🟡	Account data, vendor agreements, NDAs
PII, health, financial, credentials	🔴	Names + contacts, patient data, bank accounts, API keys

AI Model Handling Rules — Starter Edition

Rules shown for 🟢 PUBLIC and 🔵 INTERNAL tiers. Full handling rules for 🟡 CONFIDENTIAL and 🔴 RESTRICTED tiers are available in the Framework Engagement.

Rule	🟢 Public	🔵 Internal
Send to public LLM APIs	✅	⚠️ Review required
Use in RAG / vector search	✅	✅
Use for fine-tuning	✅	⚠️ Review required
Log in observability systems	✅	✅
Include in agent memory / context	✅	✅
Return in AI-generated outputs	✅	⚠️ Authorised users only

> 🔗 ***Rosetta connection:*** *Data classification feeds directly into Knowledge Substrate access controls in the Rosetta Business OS — scoping what each agent layer can see and act on.*

Classification Decision Tree

```
Is this data intended for public release?
├── YES → 🟢 PUBLIC — no restrictions on AI use
└── NO ↓
    Does it identify or relate to a specific individual?
    ├── YES → 🔴 RESTRICTED — apply full PII controls
    └── NO ↓
        Could disclosure cause financial or competitive harm?
        ├── YES → 🟡 CONFIDENTIAL — restricted AI use, access controls required
        └── NO → 🔵 INTERNAL — internal AI use permitted, review public cloud use
```

What's in the Full Version?

- Full handling rules for 🟠 CONFIDENTIAL and 🔴 RESTRICTED tiers — AI model restrictions, masking and tokenisation protocols, and session-scoping rules.
- Complete PII handling guidelines: input-layer detection, de-identification rules, retention policies, and data subject rights propagation to AI stores.
- Knowledge Substrate integration guide and Rosetta Periscopes configuration for role-scoped data access.

Full version included in our AI Framework Engagement — solutions24x7.com