

The Jonesi Consultancy | Houston, TX

EXECUTIVE AI ADOPTION · REFERENCE HANDOUT

DATA CLASSIFICATION



Know Your Data. Protect What Matters. Use AI Responsibly.

Before you paste anything into an AI tool, know what you are holding.

1 Data Classification Guide

This guide maps five sensitivity levels to what is permitted, who approves it, and how it must be handled.

	1. PUBLIC	2. INTERNAL	3. CONFIDENTIAL	4. RESTRICTED	5. HIGHLY SENSITIVE
WHAT IT IS	Publicly available and approved for unrestricted use.	For internal use only. Not intended for public distribution.	Sensitive business information that could cause harm if disclosed.	Highly sensitive information carrying significant legal, financial, or operational risk.	Extremely sensitive information with severe legal, regulatory, or personal impact.
EXAMPLES	Marketing materials, press releases, published research, public social posts.	Internal policies, employee directories, meeting minutes, training materials.	Financial forecasts, client lists, project plans, performance reviews, contract terms.	Merger and acquisition material, legal case files, security assessments, system architecture.	Personal identifiable information, health information, payment card data, trade secrets, source code.
AI USAGE	Yes. Appropriate for all AI systems, including public tools.	Generally yes. Use approved tools with care. Do not share externally.	Limited. Approved enterprise AI tools only. Avoid public AI systems.	No. Never in public tools. Only in approved, secure enterprise environments.	Never in any AI system unless explicitly authorized in a secure, isolated environment.
WHO APPROVES	No approval required.	Business unit lead or department manager.	Data owner plus information security.	Security leadership plus legal counsel.	Executive leadership plus security, legal, and privacy.
HOW TO PROTECT	No restrictions. Follow standard good practice.	Protect from accidental disclosure. Limit sharing to an internal audience.	Protect confidentiality. Control access and share on a need to know basis.	Strong protection. Encrypt, restrict access, and monitor closely.	Maximum protection. Encrypt, minimize access, and monitor continuously.
HOW TO HANDLE	Share openly. No special storage. No retention restrictions.	Store in approved locations. Use role based access. Follow retention schedule.	Store in secure systems. Encrypt in transit and at rest. Log activity.	Store in highly secure systems. Encrypt and segment access. Audit access.	Store in isolated secure systems. Encryption mandatory. Continuous monitoring.

Classification levels and approval authorities should be mapped to your organization's own policy before use.

2 Quick Classification Check 4 Questions Before You Paste

1 IS IT ALREADY PUBLIC?

If it is genuinely published and unrestricted, level 1 applies.

2 DOES IT CONTAIN PERSONAL OR REGULATED DATA?

If yes, you are at level 5 until someone tells you otherwise.

3 COULD IT HARM THE ORGANIZATION IF SHARED?

If yes, treat it as level 3 or higher and get approval.

4 WOULD I BE COMFORTABLE SEEING THIS IN THE NEWS?

If the answer is no, stop and ask for guidance.

WHEN IN DOUBT, CLASSIFY HIGHER AND ASK

AI is powerful, and responsible use protects people, data, and the reputation you spent years building. Contact your data owner, information security team, or privacy officer for guidance.

© 2026 The Jonesi Consultancy. All rights reserved.

Know Your Data. Protect What Matters. Use AI Responsibly.

We help organizations set the lines, train to them, and put governance behind them.

