

The Jonesi Consultancy | Houston, TX

EXECUTIVE AI ADOPTION · TEAM HANDOUT

WHAT NOT TO PUT INTO AI



A One-Page Rule for Everyone Who Uses These Tools

Most AI incidents are not attacks. They are ordinary people pasting the wrong thing into a helpful box.

The tools do not know what is confidential. That judgment stays with you, it happens before you press enter, and there is no taking it back. Three categories cover nearly every decision.

1 Three Categories

NEVER ENTER

Client, customer, patient, or case records. Personal information about identifiable individuals. Health information. Financial account or payment details. Employee records and compensation. Passwords and credentials. Unpublished financial results. Anything under a confidentiality agreement.

APPROVED TOOLS ONLY

Internal drafts and working documents. Meeting notes with third parties removed. Non-public project material. Vendor correspondence. The rule: anything you would send in an internal email but would not post publicly. Use an organizational account, never a personal one.

GENERALLY FINE

Published and public material. General questions and background research. Your own writing that contains no confidential detail. Invented or anonymized examples built to stand in for the real thing.

2 Sanitize Before You Prompt

- › **Strip names and identifiers.** Use roles instead. A client, the vendor, Employee A.
- › **Round or mask identifying numbers.** An exact figure often identifies a single account or person on its own.
- › **Describe instead of paste.** The model usually needs the shape of the problem, not the document.
- › **Ask who is in this text.** If a real person could be identified from it, sanitize or stop.

3 The Two Questions That Settle Most Cases

- 1 Would this be a problem if it appeared in a screenshot outside the organization?
- 2 Am I allowed to share this with someone outside my team? If not, it does not go into a tool either.

4 If You Have Already Done It

Report it today rather than hoping it does not matter. Containment depends on how fast someone finds out, and organizations get into trouble through concealment far more often than through the original mistake.

THE WHOLE RULE, IN ONE LINE

The tool cannot make this judgment for you, and it will never tell you that you got it wrong. Deciding what goes in is the only control that operates before the exposure exists rather than after.

If a real person could be identified from it, sanitize or stop.

General educational resource. Not legal, privacy, cybersecurity, employment, or compliance advice.

© 2026 The Jonesi Consultancy. All rights reserved.

Not sure where your organization draws these lines?

We help teams write the rule, train to it, and make it stick.

