01

AI USE

AI SAFETY QUICK-START

Seven rules that reduce avoidable AI risk before it reaches a customer, employee or decision.

CORMIER CONSULTING SVCS LLC

1 KEEP SENSITIVE DATA OUT

Do not paste customer, employee, financial, claim, legal, credential or trade-secret data into an unapproved AI tool.

2 USE APPROVED TOOLS ONLY

A familiar brand name is not a security review. Define which tools, accounts and features your team may use.

3 REQUIRE HUMAN REVIEW

AI can sound certain and still be wrong. A person approves customer-facing, financial, technical and public work.

4 VERIFY MONEY & ACCESS

Treat urgent invoices, payment changes, password resets and executive requests as unverified until confirmed another way.

5 KEEP PEOPLE IN HIGH-IMPACT DECISIONS

Do not let AI alone decide hiring, discipline, eligibility, pricing, coverage, lending or legal outcomes.

6 TRAIN, REPORT & LEARN

Employees need a safe way to report accidental data entry, suspicious content and AI mistakes quickly.

7 RECORD IMPORTANT USES

For higher-risk work, record the tool, purpose, reviewer and final decision. Accountability should be visible.

8 THE SIMPLE RULE

Use AI to assist judgment - not replace ownership. Protect the inputs, verify the outputs and assign responsibility.

AI & CYBER RISK REVIEW

A generic checklist finds the gaps. A tailored policy closes them.

Cormier Consulting Svc LLC | (254) 661-2231 | CormierConsultingSvc.com

Sources: NIST AI Risk Management Framework and Generative AI Profile - nist.gov/itl/ai-risk-management-framework