

1-PAGE AI SAFETY POLICY

SAFETY

Protect people from the model

≠

SECURITY

Protect the model from attackers

CLASSROOM TEMPLATE · SAMPLE · NOT A CERTIFICATE

Module 0 · Why AI Safety Is Not Security

Fill this page for your shop. Completing it does not issue GASC-2026-XXXX.

ORGANIZATION

DATE

OWNER (NAMED ROLE)

1. SCOPE

Which tools, which staff, and which work. Not the whole internet.

4. DATA RULES

Never in a prompt: PII, PHI, secrets, source code, client files.

2. ALLOWED USE

What people may draft. What still needs a human before it leaves.

5. INCIDENT REPORTING

Who they tell, how fast, and what they write down.

3. HUMAN REVIEW REQUIRED

Name the moments a person with domain expertise must look first.

6. OWNER & DATE

A named role owns this page. Add a review date. Refuse "the team."