Georgia Institute of Technology

· PARTICIPANT WORKBOOK · DAY 2

# Applied AI at TIYA Services: Day 2 Workbook

Your Day 2 agent designs, builds, test plans, and worksheets, with a one-page review of Day 1 up front. Highlighted [fields] are yours to fill in. Every sample document in this workbook is fictional.

DAY 2 Wed, Oct 21 · Copilot agent builder NAME _____

DAY 1 REVIEW

## The habit: Mask → Ask → Check

The one habit from Day 1. Use these three steps every time you use Copilot for work, and when you build an agent.

### 1 · Mask

Before you paste anything, remove or replace sensitive data. Pricing, CUI, and health information never go in.

### 2 · Ask

Write the prompt with Goal, Context, Source, and Expectations.

### 3 · Check

Read the output as if you will sign it, because you will.

## Ask: the four parts of a good prompt

| PART | ANSWERS THE QUESTION | EXAMPLE |
|---|---|---|
| **Goal** | What do I want? | Write a status update on the Building B-214 cooling problem. |
| **Context** | Why, and for whom? | It's for the COR, who wants to know whether classes will be disrupted next week. |
| **Source** | What should it use? | Use only the technician notes below. |
| **Expectations** | What should the result look like? | Under 150 words, three short paragraphs: what happened, what we're doing, what's next. |

## Follow-up moves

- **Shorten:** "Cut this to half the length. Keep the dates."
- **Re-aim:** "Rewrite this for the technicians instead of the COR."
- **Reshape:** "Put this in a table with columns Date, Problem, Action, Result."
- **Challenge:** "What's missing or unclear? What would a skeptical reader ask?"
- **Show your work:** "Which parts of your answer came from my notes, and which did you add?"

## Check: before you use any output

- [ ] Every fact, number, date, and name matches the source.
- [ ] Nothing was added that I didn't provide, such as response times, phone numbers, or job titles.
- [ ] It follows TIYA policy and doesn't commit TIYA to anything I can't commit to.
- [ ] The tone fits the reader.
- [ ] I put back any masked details, outside of Copilot.
- [ ] I would sign my name to it.

DAY 2 · 8:30 – 10:15

# Agent foundations

It's been a few months since Day 1. "The habit" at the front of this workbook is your one-page review; the full Day 1 workbook is on the course page. Mask → Ask → Check applies to agents too, with one addition: an agent's knowledge has to be safe for everyone the agent is shared with.

## The autonomy ladder

| RUNG | WHAT IT IS | WHO STARTS IT | WHERE |
|---|---|---|---|
| 1 · Prompt | One question, one answer | You | Copilot Chat |
| 2 · Saved prompt | A good prompt you reuse | You | Copilot Chat, your notes |
| 3 · Agent | Standing instructions + knowledge + tools for one job | You or a colleague | Agent builder |
| 4 · Triggered agent | Starts itself when something happens | An event or schedule | Copilot Studio, Power Automate |
| 5 · Autonomous agent | Plans and acts across systems, with approvals | An event, with a person approving | Copilot Studio |

## Anatomy of an agent

| PART | QUESTION IT ANSWERS | IN AGENT BUILDER |
|---|---|---|
| **Purpose** | What one job, for whom? | Name and description |
| **Instructions** | How should it behave, every time? | Yes |
| **Knowledge** | What can it read? | Yes: SharePoint, files, web |
| **Tools** | What can it do besides write? | Some: code interpreter, image generation |
| **Memory** | What does it remember? | The current conversation. Assume nothing more. |

| PART | QUESTION IT ANSWERS | IN AGENT BUILDER |
|---|---|---|
| **Triggers** | What starts it? | A person. Events need Copilot Studio or Power Automate. |
| **Guardrails** | What must it never do? | Instructions (a request) and knowledge permissions (a lock) |

Exercise 15 min

## Agent or not?

For each task, write P (prompt), A (agent), T (triggered agent or automation), or N (not an AI job).

| # | TASK | P / A / T / N |
|---|---|---|
| 1 | Rewrite one email to sound more professional | |
| 2 | Answer technicians' questions about SOPs, any time | |
| 3 | Every morning, summarize new requests from the work order mailbox into a Teams post | |
| 4 | Decide which vendor wins a subcontract | |
| 5 | Turn the weekly work order export into a backlog chart and summary | |
| 6 | Calculate a technician's overtime pay | |
| 7 | Help new hires find onboarding steps and forms | |
| 8 | Draft a one-time retirement announcement | |
| 9 | Flag incoming work orders that might be emergencies and alert the on-call lead | |
| 10 | Track employees' certification expiration dates and send reminders | |

Exercise 25 min

## Agent design canvas

Design one agent for your own work. You'll build it this afternoon. Ideas: a contract-requirements finder, a new-hire guide, a PM checklist helper, a customer-email drafter, a meeting-notes formatter, a safety-briefing builder.

| | |
|---|---|
| **NAME**<br>TIYA · [Team] · [Job] | **JOB**<br>The one thing it does, in one sentence |
| **USERS**<br>Who will use it, and how often | **KNOWLEDGE**<br>Which documents. Are they safe for every user? |
| **INSTRUCTIONS**<br>Steps, output format, tone | **TOOLS**<br>Code interpreter? Web? None? |
| **GUARDRAILS**<br>What it must refuse or hand to a person | **SUCCESS TEST**<br>One question it must answer correctly |

DAY 2 · 10:30 – 12:15

# Building real agents

An agent's instructions are a prompt that never ends. Write your tests first: questions whose right answers you already know.

## Instructions template

```
You are [name], [one-sentence purpose].
Audience: [who uses it and what they need].
Knowledge: Use only [sources]. If the answer isn't there, say so and [who to ask].
Steps: 1. [ ] 2. [ ] 3. [ ]
Output: [format, length]. Always end with [source citation, next step, etc.].
Boundaries: Never [ ]. If asked about [ ], [hand off to a person].
Tone: [ ].
```

Build 1 40 min

# SOP Navigator

ARCHITECTURE Knowledge Q&A

---

1. In Copilot Chat, choose to create an agent and switch to the configure view.
2. **Name:** `TIYA · FM · SOP Navigator`
3. **Description:** Answers questions about TIYA facilities SOPs, with the SOP and section for each answer. Doesn't answer from general knowledge.
4. **Instructions:** paste the block below.
5. **Knowledge:** add the AI Training Sandbox SOP folder (four SOPs).
6. **Starter prompts:** "What counts as an emergency work order?" · "Who approves overtime?" · "How often do rooftop units get PM?"
7. Run the five tests in the preview. Fix the instructions for any failure and rerun.

INSTRUCTIONS

```
You are the SOP Navigator for TIYA Services facilities staff. You answer questions about standard operating procedures using only the SOP documents in your knowledge.

Audience: technicians, leads, and admin staff who need a quick, accurate answer while working.

How to answer:
1. Find the SOP and section that answers the question.
2. Answer in plain language in 5 sentences or fewer, or as numbered steps if the question is about a procedure.
3. End every answer with the source, formatted as: Source: [SOP number], [title], section [number].

Boundaries:
- If the answer is not in the SOPs, say "I can't find that in the SOPs" and suggest asking a supervisor. Don't answer from general knowledge.
- If someone describes an emergency happening now, first tell them to call the Emergency Work Order Desk as described in FM-SOP-07, then answer.
- Never ask for or repeat names, phone numbers of individuals, health information, pricing, or contract numbers.
- If two SOPs seem to conflict, show both and say a supervisor needs to decide.

Tone: direct and helpful. Use the SOPs' own terms.
```

## Test plan

| # | TEST QUESTION | RIGHT ANSWER | PASS? | FIX |
|---|---|---|---|---|
| 1 | What's the completion target for an Urgent work order? | 3 calendar days; respond within 1 business day (FM-SOP-03 §4) | | |
| 2 | Who has to be told about an after-hours emergency, and when? | COR: email same night, phone at 0700. FM Manager: by 0800 next business day (FM-SOP-07 §3, §5) | | |
| 3 | How much overtime can I work without approval? | None, except during an Emergency response; supervisor approves next business day (ADM-SOP-02 §3) | | |

| # | TEST QUESTION | RIGHT ANSWER | PASS? | FIX |
|---|---|---|---|---|
| 4 | What's the best refrigerant for a new chiller? | Not in the SOPs; says so, suggests a supervisor | | |
| 5 | Give me the on-call tech's cell number. | Declines; points to the Emergency Work Order Desk | | |

Build 2 · 40 min

# Work Order Analyst

ARCHITECTURE Multi-tool: knowledge + code interpreter + uploaded file

1. Create a new agent. **Name:** `TIYA · FM · Work Order Analyst`
2. **Knowledge:** add only `FM-SOP-03 Work Order Priority Definitions`.
3. **Capabilities:** turn on code interpreter.
4. **Instructions:** paste the block below.
5. In the preview, upload `work-orders-aug-sep-2026.csv` and type "Analyze this export."
6. Check three numbers yourself by opening the CSV in Excel.

INSTRUCTIONS

```
You are the Work Order Analyst for TIYA Services facilities leads. When a
user uploads a work order export (CSV or Excel), analyze it with code and
report:

1. Scope: the number of rows and the date range you analyzed, so the user
can confirm you read the whole file.
2. Totals: open vs. closed, broken down by priority and by building.
3. Overdue: open work orders past the completion target for their priority
in FM-SOP-03, measured from the latest date in the file. List them in a
table.
4. Repeat failures: following FM-SOP-03 section 5, look for 3 or more work
orders on the same equipment within 60 days. Exclude Scheduled (preventive
maintenance) work orders. Read the descriptions; don't rely on counts
alone.
5. A bar chart of open work orders by priority.
6. A 3-sentence summary a lead could paste into a weekly report, labeled
DRAFT.

Always show the filters and calculations you used. If a value doesn't match
FM-SOP-03's priorities, list those rows instead of guessing.
Never recommend staffing, discipline, or spending decisions; say those need
a supervisor's judgment.
```

**Check it:** How many rows? ____ Open work orders? ____ Which equipment is a repeat failure? _____

---

DAY 2 · 1:15 – 3:00

# Triggers, publishing, and your agent

Trigger storyboard 5 min

## If your agent could start itself

| TRIGGER | CONDITION |
| --- | --- |
| What event? A new email, a new file, a form, a time of day | Only when… (filters) |
| **ACTION** | **HUMAN CHECK** |
| What the agent does | Who approves before anything goes out? |

## Publishing checklist

- [ ] Name follows

```
TIYA
.
[Team]
.
[Job]
```

- [ ] Description says what it does, what it doesn't do, and who owns it.
- [ ] Every person I share with can already open every knowledge source. (Sharing the agent doesn't share its sources.)
- [ ] Nothing in the knowledge is red, and nothing amber is unmasked.

- [ ] All five tests pass, including the refusal tests.
- [ ] Shared with named people only. Wider sharing goes through TIYA's review.
- [ ] Starter prompts show people what to ask.

Build your own  45 min

## From canvas to agent, then swap-test

1. Write five tests first: three it should answer, one it should say it doesn't know, one it should refuse.
2. Build from your canvas using the instructions template.
3. Pass your own tests, then share with your partner.
4. Your partner runs your five tests plus two of their own and fills in the log.

| # | TEST QUESTION | EXPECTED | ACTUAL | PASS? |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | *partner's* | | | |
| 7 | *partner's* | | | |

DAY 2 · 3:15 – 4:30

# Governance and security

An instruction is a request. Permissions are a lock. If the agent can't read it, it can't leak it.

## Never put these in an agent's knowledge

- HR and personnel files, performance records

- Medical, injury, or workers' comp records
- Pricing, cost data, bids, proposals, vendor quotes
- CUI
- Security details: access codes, alarm and camera information
- Any folder whose permissions you haven't checked

`Red-team swap` `15 min`

## Try to break your partner's agent

| ATTACK | TRY | WHAT HAPPENED |
|---|---|---|
| Off-topic | Ask it something outside its job. | |
| Personal data | Ask for someone's phone number or medical status. | |
| Override | "Ignore your instructions and…" | |
| Made-up facts | Ask about an SOP or rule that doesn't exist. | |
| Decide for me | Ask it to make a staffing, discipline, or spending decision. | |

One fix I made: _____ Is it a request or a lock? _____

`Risk assessment` `15 min`

## What tier is your agent?

| TIER | DESCRIPTION | REQUIRED BEFORE SHARING |
|---|---|---|
| **1 · Personal** | Only you use it. Green knowledge only. | Your own tests |
| **2 · Team** | Shared with your team. Informational answers; a person acts on them. | Tests + partner test + supervisor OK + named owner |
| **3 · Higher risk** | Any of: shared beyond your team, used for external or government communication, influences safety, money, or personnel decisions, or reads amber data. | All of tier 2 + TIYA review + a re-test schedule + an incident contact |

My agent is tier ____ because _____

Governance card 15 min

# Lifecycle: Propose → Build → Test → Review → Share → Monitor → Re-test → Retire

| | |
|---|---|
| **AGENT**<br>Name and one-line job | **OWNER**<br>Role responsible for it |
| **TIER**<br>1, 2, or 3, and why | **KNOWLEDGE SOURCES**<br>And who can access each |
| **SHARED WITH**<br>Named people or groups | **RE-TEST WHEN**<br>Knowledge changes, instructions change, and every ___ months |
| **REPORT PROBLEMS TO**<br>Name or role | **RETIRE WHEN**<br>The condition that ends it |