Georgia Institute of Technology

APPLIED AI AT TIYA SERVICES · DAY 2 · AGENTIC AI WITH MICROSOFT COPILOT

Agentic AI with Microsoft Copilot

Wednesday, October 21, 2026

Alex Djalali · Alex Rhodeen

Today

- 8:30 Login check and a Day 1 review
- 8:50 Agentic AI foundations
- 10:30 Building real agents
- 1:15 Triggers, publishing, your own agent
- 3:15 Governance & security

EXERCISE

Login check

- Open Copilot Chat
- Find the option to create an agent

8:40

Day 1 in Review

Back from June · 10 min

What Day 1 was about

- Generative AI predicts likely words; it doesn't know TIYA's facts unless you give them
- It sounds just as confident when it's wrong
- Draft, not decide: it drafts and summarizes; people decide, approve, and sign
- If you send it, you own it

The habit: Mask → Ask → Check

1 · Mask

Names → roles, numbers → placeholders, prices and health details out

2 · Ask

Goal, Context, Source, Expectations (GCSE)

3 · Check

Facts match the source, nothing added. Would I sign this?

The data traffic light

Red

Never enter. CUI, PHI, pricing, IDs, security details, passwords

Amber

Mask first. Names, contacts, vendors, contract numbers

Green

Okay. How-to, public information, masked writing

8:50

Agentic AI Foundations

85 min

From chat to agent

- Standing instructions
- Its own knowledge
- Tools
- For one defined job

The autonomy ladder

1 · Prompt

You ask; it answers

2 · Saved prompt

You reuse what works

3 · Agent

Instructions, knowledge, tools

4 · Triggered

Starts itself on an event

5 · Autonomous

Plans and acts, with approvals

Anatomy of an agent

- Purpose · Instructions · Knowledge · Tools
- Memory · Triggers · Guardrails

What agent builder supports

Yes

Purpose, instructions, knowledge

Some

Tools: code interpreter, image generation

Limited

Memory: the current conversation

No

Triggers: a person starts it

The Microsoft ecosystem

Agent builder

In Copilot Chat. No-code, on-demand agents

Copilot Studio

Triggers, connectors, autonomous agents

Power Automate

Rules-based flows and triggers

Four architectures

Knowledge Q&A

Answers from defined documents

Task assistant

Walks a person through a task

Multi-tool

Knowledge plus tools and files

Orchestrated

Agents handing off to agents

EXERCISE · 15 MIN

Agent or not?

- Ten TIYA tasks
- Prompt, agent, triggered, or not AI?

Debrief: the hard ones

- #4 Choosing a vendor
- #9 Flagging emergencies

EXERCISE · 25 MIN

Agent design canvas

- Design one agent for your own work
- You'll build it this afternoon

10:30

Building Real Agents

Hands-on · 105 min

A prompt that never ends

- Instructions run in every conversation
- Every weakness shows up for everyone you share with

Instructions template

- Role and purpose · audience
- Knowledge rules · steps
- Output format · boundaries · tone

Tests first

- Five questions with known answers
- One it shouldn't know
- One it should refuse

LIVE DEMO

Build 1 · SOP Navigator

- Configure view
- Name, description, instructions, knowledge, starter prompts

EXERCISE · 20 MIN

Test, fix, rerun

- Run the five tests
- Fix the instructions for each failure

LIVE DEMO

Build 2 · Work Order Analyst

- Knowledge: FM-SOP-03
- Code interpreter on
- Upload the CSV in chat

EXERCISE · 10 MIN

Check the numbers yourself

- Rows, open count, repeat failure
- Open the CSV in Excel

Debrief

- Which test failed first?
- Would you put its chart in a report to the COR?

1 : 15

Building Real Agents, Continued

Hands-on · 105 min

Event triggers

Trigger

A new email, file, form, or time

Condition

Only when…

Action

What the agent does

Human check

Who approves

LIVE DEMO

A triggered flow

- New email → summary → Teams post for approval

EXERCISE · 5 MIN

Trigger storyboard

- Design a trigger for your canvas agent

Memory

Conversation

What's in this chat

Knowledge

What it can read

Long-term

Assume none

Publishing

- Users see only what they can already open
- Sharing an agent doesn't share its sources
- Named people first

Name and describe

- TIYA · [Team] · [Job]
- What it does, what it doesn't, who owns it

EXERCISE · 30 MIN

Build your own

- Tests first, then build
- Pass your own tests

EXERCISE · 15 MIN

Swap test

- Your partner runs your tests plus two of theirs
- Fix and reshare

Showcase

- Four or five volunteers, 2 minutes each

3 : 15

Governance & Security

75 min

A request vs. a lock

Request

Instructions. A clever question can get around them.

Lock

Permissions. What it can't read, it can't leak.

Never as knowledge

- Personnel, medical, pricing, CUI
- Security details
- Folders with unchecked permissions

EXERCISE · 15 MIN

Red-team swap

- Off-topic · personal data · override
- Made-up facts · decide for me

Risk tiers

1 · Personal

Only you; green knowledge

2 · Team

Shared with your team; a person acts on answers

3 · Higher risk

Beyond your team, external communication, decisions, or amber data

The agent lifecycle

- Propose → Build → Test → Review
- Share → Monitor → Re-test → Retire

EXERCISE · 15 MIN

Governance card

- Owner, tier, sources, sharing, re-test, retire

EXERCISE · 10 MIN

Wrap

- Knowledge check and exit checklist
- Evaluation and certificates

Georgia Institute of Technology

APPLIED AI AT TIYA SERVICES · DAY 2 · AGENTIC AI WITH MICROSOFT COPILOT

Thank you

Certificates at the door

Questions after today: [TIYA contact]