# Secure Development Delivery (for Copilot and Custom Apps)

## Introduction & Purpose

This delivery helps organisations who want to build their own **applications, automations, or Copilot agents** establish a secure foundation for development.

The goal is to take a customer from *“we want to start building”* to *“we have a secure development process and environment that reduces risk and meets compliance obligations.”*

The engagement focuses on **governance, identity, data protection, and secure-by-design practices** — not just the code itself.

## Rules of Engagement

* Keep conversations business-focused: connect secure development practices to protecting **customer data, IP, and reputation**.
* Avoid deep code-level training unless specifically scoped — focus on **frameworks, pipelines, and guardrails**.
* Emphasise repeatability: the customer should leave with a **process**, not just one-off configurations.
* Red flag: if a customer pushes to deploy production Copilot agents without data classification or DLP in place, raise as a **critical risk**.

## Step-by-Step Delivery

### Step 1 – Define Development Goals & Risks

* Clarify what is being built (Copilot agent, Power App, custom connector).
* Identify what data it will access (internal, customer, regulated, sensitive).
* Map applicable frameworks (Essential 8, ISO 27001, OWASP).
* Define the end state (internal tool, external app, regulated industry use case).

**Output:** Development security scope document.

### Step 2 – Establish Secure Environments

* Enforce separation of dev/test/prod environments.
* Apply secure identity and access controls (Entra ID, Conditional Access, MFA).
* Implement role-based access control for development platforms (GitHub, Power Platform, Azure).
* Deploy secrets management (Key Vault, environment variables).

**Output:** Hardened development environment checklist.

### Step 3 – Governance & Pipelines

* Introduce a lightweight **Secure SDLC framework** (requirements → design → build → test → deploy → review).
* Establish **CI/CD pipelines with security checks** (static analysis, dependency scanning).
* Define branching, peer review, and approval processes.
* Align practices with Microsoft SDL and OWASP standards.

**Output:** Secure pipeline reference model and governance roles.

### Step 4 – Data Protection & AI-Specific Risks

* Apply sensitivity labels and DLP to content accessed by apps/agents.
* Define guardrails for Copilot agents (data boundaries, prompt injection, jailbreak scenarios).
* Ensure encryption for all data (in transit and at rest).
* Use Microsoft Purview “Secure by Default” blueprints as reference.

**Output:** AI security guardrails document and DLP integration plan.

### Step 5 – Validation & Adoption

* Run a pilot build through the secure pipeline.
* Review vulnerabilities, adoption blockers, and lessons learned.
* Deliver training sessions for developers on secure-by-default practices.
* Establish governance model for ongoing reviews.

**Output:** Pilot validation report and secure development playbook.

## Engagement Outputs

* Secure Development Framework (lightweight SDLC guide tailored for Copilot/Apps).
* Hardened environment checklist (identity, access, secrets).
* Secure pipeline model (CI/CD with security gates).
* AI/Copilot security guardrails (prompt injection, data boundaries, DLP integration).
* Governance playbook (roles, responsibilities, adoption).

## Timeframe

* **3–4 weeks program**, depending on maturity:
  + Week 1 – Discovery & scope
  + Week 2 – Secure environment setup
  + Week 3 – Governance & pipelines
  + Week 4 – Validation & handover (optional, for larger builds)

## References & Learning

* [Microsoft Secure Development Lifecycle (SDL)](https://www.microsoft.com/en-us/securityengineering/sdl)
* [OWASP Top 10](https://owasp.org/www-project-top-ten/)
* [Microsoft Purview – Secure by Default](https://github.com/microsoft/purview/blob/main/purview-blueprints/Secure%20by%20default%20with%20Microsoft%20Purview.pdf)
* [NIST Secure Software Development Framework](https://csrc.nist.gov/publications/detail/sp/800-218/final)