BIZ-F3

BIZ-F3 — AI Safety, Ethics, and Policy for Organisations

Business — Foundation / Foundation

Audience	All staff, with particular value for compliance, legal, HR, and leadership
Prerequisites	BIZ-F1 — AI Literacy for Teams (recommended)
Duration	1 day
Delivery format	Workshop — policy and governance focused
Group size	8–25
Materials provided	AI use policy template, data risk checklist, regulatory reference guide, incident response template

Description

This one-day workshop is essential for any organisation deploying AI tools at scale. Covers data protection, regulatory landscape, how to write an AI use policy that actually works, and contractual obligations. Participants will leave with a draft policy ready for legal review, a data risk assessment for current tool use, and a clear understanding of regulatory exposure specific to their sector. Designed for mixed audiences including compliance, legal, HR, and operations teams.

Key Modules

Module 1 — Where data leakage risk comes from

What happens when data enters an AI tool. Understanding cloud storage, data retention policies, training data usage, and cross-border data flows. Practical audit of what your organisation is currently putting into AI systems.

Module 2 — What must never go into a public AI tool

Classification of sensitive information: PII, confidential business data, customer data, IP, financial data, health information. Business and regulatory consequences of breaches. Building a data classification framework for your organisation.

Module 3 — The regulatory landscape

EU AI Act, UK Government AI principles, GDPR implications, sector-specific regulations (finance, healthcare, etc.). What your obligations are and what changes are coming. Risk register for your organisation.

Module 4 — Writing a practical AI use policy

Policy structure, scope, permitted and prohibited uses, data handling, escalation procedures, and review cycles. Participants draft a section of their organisation's policy during the session. Tone: enforcement-aware but practical.

Module 5 — AI in contracts and procurement

What to require from vendors, what to negotiate, IP ownership, liability, audit rights, and sub-processor transparency. Procurement checklist for AI tools and services.

Module 6 — Incident response

Detecting data breaches, containment steps, notification procedures, regulatory reporting, and communication planning. Walk through a mock incident scenario.

What You Will Be Able To Do

1.	Draft an AI use policy that balances risk management with practical adoption
2.	Identify and classify data at risk of leakage in current AI tool use
3.	Assess regulatory exposure specific to their sector and jurisdiction
4.	Build a data classification and handling framework for AI systems
5.	Define incident response procedures for AI-related security events
6.	Evaluate AI vendors and tools for compliance and contractual risk

Delivery Notes

Meeting room with internet, projector, and breakout spaces for group work. Participants need laptops for policy drafting and risk assessment exercises. Bring sector-specific regulatory guides and organisation's current vendor agreements. Trainer should have legal and compliance expertise or access to specialist input. Optimal group size 12–20; mixed disciplines (legal, compliance, operations) recommended.

Pathway Position

Comes after: BIZ-F1 — AI Literacy for Teams (recommended)

Feeds into: BIZ-I4 — AI in Operations and Process Improvement / BIZ-A8 — AI Strategy and Transformation

Ready to book this course?

Contact Io Technologies to discuss delivery at your organisation.

All courses and engagements are delivered on request — on-site, remote, or blended.