Session 4 Handout: Policy and Incidents

FAST-10 AI Governance, Risk, Ethics, and Responsible Use · 7formations · Instructor: Wadood Chaudhary · All examples fictional · Training, not legal advice

> **Training, not legal advice.** Notification duties depend on facts. Involve counsel as soon as personal information or PHI may be involved.

Why this session matters

Sooner or later someone will paste the wrong thing into the wrong tool. Companies that handle it well have three things ready: a short policy people actually read, an incident checklist with names on it, and a culture where people report mistakes the same day.

Key concepts

1. A right-sized acceptable use policy (AUP)

Section	What it says
Purpose and scope	Who it covers; which tools and features
Approved tools	Named tools, work accounts; how to request a new one
Never allowed	Personal information (G.L. c. 93H), PHI, card numbers, employee records, customer confidential material
Required checks	Human review for customer-facing, money, and people decisions
Reporting	Same day, to a named role; honest reports are not punished
Training	Who, when, how understanding is checked
Owner and review date	Who updates it, and when

Short enough that people read it: one or two pages, plain language, examples from your own work.

2. Incident response: five steps

Step	Actions
Contain	Stop the use; remove or restrict access; use the vendor's deletion and support options; preserve facts
Assess	What data, how many people, which states, which tool, and what the vendor retains
Notify	With counsel: residents, the AG, and OCABR under c. 93H when it applies; HIPAA timelines for PHI; other states' laws; contracts (card brands, customers)
Fix	Approved alternative, technical controls, targeted training, vendor follow-up, register update

Step	Actions
Record	Dated log of facts, decisions, and who made them; after-action notes

3. Tabletop exercises

Walk through a realistic scenario in 30 to 60 minutes with the people who would actually respond. Add one or two surprises ("injects"). The goal is to find gaps (missing contacts, unclear authority, no approved alternative) before a real incident. End with after-action notes: what happened, what went well, gaps, actions with owners and dates.

4. Training your staff

- Short, role-based, with examples from the team's own tasks.
- Cover the three rules people must remember: **approved tools, never-allowed data, how to report**.
- Check understanding (a five-question quiz or a sort exercise).
- Refresh yearly and whenever tools or rules change. The DOL AI Literacy Framework (TEN 07-25) and the EU AI Act's AI literacy provision both point the same way: people need practical AI literacy for their role.

Worked example (fictional)

At Merrimack Freight, a billing clerk pasted 212 customer contacts into a free chatbot; 37 rows had names and full card numbers. The team thanked her, contained (stopped use, captured details, used the vendor's deletion options), assessed (about 180 Massachusetts residents and 25 New Hampshire residents; 37 rows meeting the 93H definition), and brought in counsel on notice to residents, the AG, OCABR, and the card processor. The fix was an approved spreadsheet tool, a browser warning on public chatbots, and a 20-minute refresher for billing.

Checklist

- ☐ AUP fits on one to two pages and names approved tools.
- ☐ Never-allowed data listed specifically.
- ☐ Incident checklist has roles and phone numbers for counsel, IT, vendors, and insurer.
- ☐ Tabletop scheduled at least yearly.
- ☐ Training plan with an understanding check and refresh trigger.

Do and don't

Do	Don't
Thank people who report	Punish the first honest report
Contain, then assess, then notify	Send rushed notices with guessed facts
Fix the cause	Ban all AI and push use underground
Write down every decision	Rely on memory after the fact