INDEPENDENT PORTFOLIO PROJECT

Protecting Customer Data

Privacy and escalation training for customer support



Charles Lee | Senior Instructional Designer

Fictional scenario • 8–10 minute prototype

02

Project brief

Nexa Mobile support agents handle identity and account requests every day. Small judgment errors can expose customer data or create unnecessary escalations.

Business need

Improve consistent handling of privacy-sensitive requests without slowing customer service.

Audience

New and experienced customer support agents working across phone and chat channels.

Learning solution

A short branching scenario supported by a searchable decision guide and final transfer check.

Success signal

Agents verify identity, limit disclosure, document the interaction, and escalate only when policy requires it.

03

Performance analysis

The learning targets decisions agents control

Knowledge gap

Agents confuse identity verification with permission to disclose any account detail.

Decision gap

Agents need a clear boundary for what they can share, change, or escalate.

Environment gap

Policy information exists, but agents cannot locate the right rule quickly during a live contact.

Training boundary

The course does not ask agents to memorize policy language. It gives them repeated practice using a four-step decision process under realistic time pressure.

Design implication

Scenario practice plus an on-demand job aid fits the performance need better than a policy overview.

Learning objectives

After the experience, agents can make four observable decisions

01	**Verify**	Confirm identity with the approved method before accessing or discussing account data.
02	**Limit**	Share only the information needed to resolve the stated request.
03	**Document**	Record the request, verification method, action, and outcome.
04	**Escalate**	Recognize exceptions that require a privacy or security specialist.

05

Experience map

A short scenario moves from supported practice to independent judgment

1

Context

Meet the customer and understand the request

2

Decision

Choose a response with access to the guide

3

Consequence

See customer and compliance impact

4

Transfer

Handle a new case without prompts

Estimated seat time: 8–10 minutes

A customer asks for help with a family account

MAYA, SUPPORT AGENT

“Thanks for calling Nexa Mobile. How can I help today?”

CUSTOMER

“My husband is traveling. I need the last four digits of the payment card and I also need to reset his account PIN.”

What matters

The caller knows account details, but the account belongs to another person. The request combines information disclosure and an account change.

What should Maya do first?

A. Provide the card digits because the caller knows the account address and recent payment amount.

B. Verify whether the caller is an authorized user, then use the approved identity process before discussing data.

C. Reset the PIN after sending a one-time code to the phone number the caller provides.

Policy reference available

Agents can open the decision guide before choosing. This models the real work environment and reduces memorization burden.

Verify authorization before discussing account data

Why this works

The caller’s knowledge of account details does not prove authorization. Maya should confirm the caller’s role on the account and complete the approved identity process before accessing or disclosing sensitive information.

Decision rule

Identity verified

Authorization confirmed

Request within role

If any condition fails, stop and follow the escalation path.

The job aid supports decisions during live customer contacts

Customer data decision guide

Use before sharing data or changing account access

1	**Verify identity**	Use only approved channels and factors.
2	**Confirm authority**	Check the caller’s role and permissions.
3	**Match the request**	Share or change only what the role permits.
4	**Document or escalate**	Record the outcome. Escalate suspected fraud, coercion, or policy exceptions.

A new situation tests transfer

A verified account owner says an abusive partner may know the account PIN and asks to hide recent call records. What should the agent do?

A. Delete recent call records after the owner passes identity verification.

B. Explain that records cannot be hidden and end the interaction.

C. Protect the interaction, avoid unsafe disclosure, and use the specialized safety and privacy escalation path.

The plan connects learning data to workplace behavior

Evidence	Measure	Use
During learning	Decision accuracy by branch	Find misconceptions and revise feedback or policy guidance.
After learning	Final scenario accuracy and confidence	Confirm independent performance and identify coaching needs.
30–60 days	Privacy escalation quality and repeat error themes	Check whether agents apply the decision process on the job.
Quarterly	Quality review trends and avoidable escalations	Determine whether the solution improves consistency without adding unnecessary escalations.

Targets would be set with compliance, operations, and quality partners after baseline review.

What this project demonstrates

Performance analysis	Focused the solution on decisions agents control.
Scenario design	Used realistic consequences and progressive support.
Policy translation	Turned privacy requirements into a usable decision process.
Measurement	Connected prototype data to quality and escalation signals.

Charles Lee | Senior Instructional Designer

Independent project • Fictional company • Created for portfolio demonstration