UNIT 4 Client Privacy Policy & Data

Learning Objectives:
By the end of this unit the learner will be able to:
• Adapt your current client privacy policy • Develop a data breach procedure

Unit 4

Client Privacy Policy & Data Breach Procedure

Many of the policies we are developing are designed for internal use within an organization. The client Privacy Policy however is designed for your customers and individuals outside of the organization to learn about your privacy practices, and become informed about what personal information will be collected, and how it will be used. The privacy policy is the first point of contact your potential customers will have with your privacy practices, and should ideally answer any questions they have about your use of their data. The privacy policy will pull in elements of data protection from many of the internal policies and procedures that have already been developed.

The privacy policy should be written concisely and in plain language to allow for better customer accessibility. A privacy policy that is long, or that doesn't make sense, will not be useful to a customer, and will not show good transparency on the part of the organization.

A privacy policy should also be written specifically for the organization without the use of boilerplates or straight templates. Use the privacy policy as an opportunity to be clear with your customers, and explain the specific ways your organization is dealing with privacy.

A privacy policy should address the following questions:

- What information is the organization collecting?
- How is the information being used?
- What choices or rights does the individual have in relation to their data?
- Which external parties (if any) will this information be shared with?
- What safeguards are in place to protect data?
- How will the policy be enforced?
- Who can be contacted with questions about privacy?

TEXT YOUR KNOWLEDGE

Update your company's Privacy Policy from the Pre-Assignment considering the things that you have learned in this course.

Updated Privacy Policy

DATA BREACH PROCEDURE

If an organization has a good data security infrastructure, the risk of a data breach can be minimized. Regardless, there is always a chance that information could be accidentally leaked, or that a skilled hacker could infiltrate an organization's defenses, no matter how strong. If a data breach occurs, a procedure must be in place to inform the actions of employees, and to ensure a structured and appropriate response to the incident.

A Data Breach Procedure will outline the following information:

- How an employee can report a suspected data protection incident
- Who will be responsible for leading the containment effort (often a member of the IT department), and who should be involved in this process
- Who will lead an investigation into the incident, and who else may become involved
- A process for notifying individuals and supervising authorities if a data breach is severe
- A procedure for evaluating the incident after the fact to make informed decisions for the future

The Data Breach Procedure should make it clear that any significant data breaches must be reported to individuals and the supervising authority within **72 hours**.

TEXT YOUR KNOWLEDGE

Develop a Data Breach Procedure that covers all the information outlined in this session.

Data Breach Procedure