BÁO CÁO ASSIGNMENT 01.02

Môn: An toàn và phục hồi dữ liệu

Thông tin sinh viên

Họ và tên	MSSV
Phan Trí Tài	20127318

Assignment 01.02

Câu a

	Data Safety	Data Recovery
Định nghĩa	Tập hợp các biện pháp bảo vệ dữ liệu khỏi truy cập trái phép, mất mát hoặc hỏng hóc, như mã hóa, kiểm soát truy cập, sao lưu định kỳ.	Quá trình phục hồi dữ liệu bị mất, hỏng do sự cố như xóa nhầm, hỏng phần cứng, hoặc tấn công mạng, bằng cách sử dụng các công cụ khôi phục và sao lưu.
Mục đích	Ngăn chặn mất mát và đảm bảo tính bảo mật, toàn vẹn của dữ liệu, tuân thủ các quy định pháp lý.	Phục hồi dữ liệu sau sự cố, đảm bảo duy trì hoạt động liên tục của doanh nghiệp.
Thành phần chính	Mã hóa, kiểm soát truy cập, sao lưu định kỳ, phần mềm bảo mật.	Khôi phục từ sao lưu, công cụ khôi phục, kế hoạch khôi phục sau thảm họa, sao chép dữ liệu.
Cách thức hoạt động	Chủ động ngăn chặn sự cố trước khi xảy ra.	Phản ứng sau khi xảy ra sự cố, phục hồi lại dữ liệu đã mất.
Tầm quan trọng	Bảo vệ uy tín doanh nghiệp, tránh các rủi ro pháp lý, duy trì niềm tin của khách hàng.	Giảm thiểu thời gian gián đoạn, hạn chế tổn thất tài chính và phục hồi hoạt động nhanh chóng sau sự cố.

Ví dụ thực tế	Sử dụng xác thực hai yếu tố (2FA) để bảo vệ truy cập, mã hóa dữ liệu trên đám mây.	Phục hồi dữ liệu từ bản sao lưu sau khi bị tấn công ransomware, dùng phần mềm khôi phục để lấy lại file đã xóa nhầm.

Câu b

	Data Security	**Data Privacy**	**Data Protection**
Định nghĩa	Đây là việc bảo vệ dữ liệu khỏi truy cập trái phép, hư hỏng, vi phạm và trộm cắp.	Điều này liên quan đến quyền giữ dữ liệu của một người ở hình thức riêng tư và đảm bảo rằng thông tin cá nhân được sử dụng theo cách tuân thủ với kỳ vọng của cá nhân và pháp luật.	Đây là một thuật ngữ toàn diện bao gồm cả bảo mật dữ liệu và quyền riêng tư. Nó về việc đảm bảo dữ liệu được bảo vệ khỏi bất kỳ rủi ro tiềm ẩn, lạm dụng hoặc truy cập trái phép nào.
Khía cạnh chính	Bao gồm việc sử dụng các biện pháp vật lý, phần mềm và chính sách để bảo vệ dữ liệu. Các kỹ thuật có thể bao gồm mã hóa, kiểm soát truy cập, tường lửa mạng, hệ thống phát hiện xâm nhập và kiểm tra thường xuyên.	Liên quan đến việc thu thập, lưu trữ, xử lý và chia sẻ dữ liệu cá nhân. Chính sách quyền riêng tư, cơ chế đồng ý của người dùng và các thực hành như ẩn danh dữ liệu đóng vai trò ở đây.	Liên quan đến khía cạnh pháp lý và quy định. Nhiều quốc gia có quy định về bảo vệ dữ liệu (như GDPR tại Liên minh châu Âu) quy định cách dữ liệu cá nhân nên được xử lý, lưu trữ và xử lý.
Mục tiêu	Đảm bảo tính toàn vẹn, sẵn sàng và bảo mật của dữ liệu.	Đảm bảo rằng dữ liệu cá nhân không bị lạm dụng hoặc truy cập mà không có sự ủy quyền thích hợp và rằng mọi người có quyền	Cung cấp một khung và hướng dẫn cho các tổ chức để đảm bảo an toàn, quyền riêng tư và sử dụng dữ liệu một cách đúng đắn.

		kiểm soát dữ liệu của mình.	
Tóm gọn	Bảo vệ dữ liệu khỏi bị truy cập, sử dụng hoặc phá hủy trái phép bằng cách triển khai các biện pháp kiểm soát, cơ chế và quy trình kỹ thuật phù hợp.	Đảm bảo sử dụng hợp lý dữ liệu cá nhân bằng cách trao cho các cá nhân quyền kiểm soát cách truy cập, sử dụng hoặc chia sẻ dữ liệu của họ.	Bao gồm tính khả dụng của dữ liệu, tính bất biến, bảo quản, xóa/hủy và "bảo mật dữ liệu" và "bảo mật dữ liệu".

Nguồn tham khảo

https://www.businesstechweekly.com/operational-efficiency/business-continuity/it-resilience/

https://adivi.com/blog/data-backup-and-recovery-strategies/

https://termly.io/resources/articles/data-privacy-vs-data-security-vs-data-protection/

https://www.geeksforgeeks.org/difference-between-data-privacy-and-data-security/