ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
VNUHCM - UIT

HỌC KỲ: 1	**NĂM HỌC: 2024 – 2025**		**Lớp: NT207.P21.ANTT**
Môn học: Quản lý rủi ro và an toàn thông tin trong doanh nghiệp			
Giảng viên: Nguyễn Văn Thiện	**Mã giảng viên: 11185**		

MẪU BÀI KIỂM TRA QLRR ATTT

+ NỘI DUNG THI: CÁC CHƯƠNG ĐÃ HỌC

+ HÌNH THỨC: TRẮC NGHIỆM VÀ TỰ LUẬN - SINH VIÊN LÀM BÀI TRÊN GIẤY

+ THỜI GIAN LÀM BÀI: …….

MỘT SỐ MẪU CÂU HỎI TRẮC NGHIỆM VÀ TỰ LUẬN GIÚP SINH VIÊN TÌM HIỂU TRƯỚC KHI DỰ KIỂM TRA

I. BẢNG TRẢ LỜI

(Sinh viên chỉ đánh dấu X vào 1 ô trả lời cho mỗi câu hỏi, khoanh tròn để bỏ chọn, tô đen để chọn lại)

	Câu số 01	Câu số 02	Câu số 03	Câu số 04	Câu số 05	Câu số 06	Câu số 07	Câu số 08	Câu số 09	Câu số 10	Câu số 11	Câu số 12	Câu số 13	Câu số 14	Câu số 15
a															
b	X														
c															
d															
e		X	X												
f															

Chú ý: Dấu X có trong bảng trên đây chỉ là ví dụ, không phải là đáp án để sinh viên chọn khi làm bài

II. CÂU HỎI

1. Theo yêu cầu trong Phụ lục A - ISO 27001:2013 tại Nhóm A.10 Yêu cầu A.10.1 Điều A.10.1.1 thì doanh nghiệp phải thực hiện biện pháp kiểm soát *"A policy on the use of cryptographic controls for protection of information shall be developed and implemented."*. Để đáp ứng yêu cầu này, doanh nghiệp dùng giao thức SSL để bảo mật kết nối Internet. SSL là công nghệ tiêu chuẩn để bảo mật kết nối Internet bằng cách mã hóa dữ liệu được gửi giữa trang web và trình duyệt (hoặc giữa hai máy chủ). SSL giúp ngăn chặn tin tặc nhìn thấy hoặc đánh cắp bất kỳ thông tin nào được truyền đi, bao gồm cả dữ liệu cá nhân hoặc tài chính. SSL sử dụng thuật toán mã hóa đối xứng (*"symmetric encryption algorithm"*) để mã hóa dữ liệu và sử dụng thuật toán khóa bất đối xứng (*"asymmetric key algorithm*") để mã hóa khóa được sử dụng bởi thuật toán mã hóa đối xứng. Chứng chỉ SSL hỗ trợ xác thực danh tính dựa trên chứng chỉ của máy chủ và máy khách bằng cách sử dụng chữ ký số.

Theo bạn, thuật toán nào sau đây là thuật toán mã hóa đối xứng an toàn nhất dùng cho SSL - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) RSA	b) AES	c) DES	d) TDEA	e) RC4	f) Blowfish

2. Theo yêu cầu trong Phụ lục A - ISO 27001:2013 tại Nhóm A.9 Yêu cầu A.9.4 Điều A.9.4.2 thì doanh nghiệp phải thực hiện biện pháp kiểm soát (control) *"Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure."*. Để đáp ứng với yêu cầu này, theo bạn, doanh nghiệp nên triển khai các biện pháp nào sau đây *(chọn một câu trả lời (a/b/c/d/e) dưới đây làm đáp án của bạn cho câu hỏi này):*

a) Quy định về độ phức tạp của mật khẩu đăng nhập (có sự kết hợp giữa chữ hoa và chữ thường, số và ký tự đặc biệt hay không; có yêu cầu về độ dài và độ phức tạp tối thiểu);

b) Xác thực 2 yếu tố khi đăng nhập để thêm một lớp bảo mật;

c) Khóa tài khoản người dùng sau 3 lần đăng nhập thất bại;

d) Giáo dục người dùng về cách dùng mật khẩu an toàn;

e) Chọn tất cả a, b, c và d. *Nếu chọn e, bạn phải bổ sung thêm ít nhất một biện pháp kiểm soát khác để đáp ứng yêu cầu A.9 Yêu cầu A.9.4 Điều A.9.4.2 như trên:*

(Ghi ra:) …… ……..

……

3. Phần mềm độc hại ("malware") có thể lây nhiễm vào mạng máy tính của các doanh nghiệp bất chấp việc doanh nghiệp có hay không đáp ứng yêu cầu ATTT tại Nhóm A.12 Yêu cầu A.12.2 Điều A.12.2.1*"Control: Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness."*. Tại sao như vậy? Điểm yếu cố hữu và xuất hiện khắp nơi là mức độ nhận thức ATTT khác nhau của người dùng máy tính tại doanh nghiệp. Người làm việc tại doanh nghiệp thường có nhận thức kém về bảo mật hay có hiểu biết lơ mơ về chính sách ATTT của doanh nghiệp cho dù họ ở cương vị nào tại doanh nghiệp.

Theo bạn, mạng máy tính của doanh nghiệp có thể bị lây nhiễm các loại mã độc khác nhau có nguyên nhân từ các hành động nào sau đây của người dùng máy tính tại doanh nghiệp *(chọn một câu trả lời (a/b/c/d/e) dưới đây làm đáp án của bạn cho câu hỏi này)*:

a) Nhấp chuột (click) máy tính vào một đường liên kết (link) có vẻ hợp pháp để bắt đầu quá trình '*download'*;

b) Truy cập một trang web bất kỳ mà chưa xác minh trang đó có hay không có chứng chỉ bảo mật (như SSL);

c) Nhấp chuột (click) máy tính vào chữ 'X' ở góc một cửa sổ của trang quảng cáo bật lên (*'pop up advert'*) trong khi đang duyệt web để đóng cửa số quảng cáo sau khi xem xong;

d) Tải xuống một tệp đính kèm trong email trông có vẻ an toàn để khởi động quá trình tải xuống ('*download')*;

e) *Ý kiến khác của bạn, xin ghi ra: ……a+b+c…….....*

.....

4. Theo yêu cầu trong Phụ lục A - ISO 27001:2013 tại Nhóm A.10 Yêu cầu A.10.1 Điều A.10.1.1 và A.10.1.2 thì doanh nghiệp phải thực hiện biện pháp kiểm soát (control) để đạt mục tiêu *"To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information*". Để đáp ứng yêu cầu này, nhằm lưu trữ dữ liệu nhạy cảm an toàn vào phương tiện lưu trữ (HDD/CD/DVD/USB/…) và không để dữ liệu nhạy cảm của công ty bị tiết lộ ngoài ý muốn, bạn sẽ đề xuất với công ty dùng thuật toán nào sau đây để mã hóa dữ liệu - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) MD5 (Message-Digest algorithm),

b) AES (The Advanced Encryption Standard),

c) SHA (Secure ***Hash*** Algorithm) gồm SHA-2 hoặc SHA-256,

d) DES (Data Encryption Standard),

e) Triple DES (3DES) – also known as Triple Data Encryption Algorithm (TDEA),

f) Không dùng thuật toán mã hóa dữ liệu mà bảo mật dữ liệu bằng cách khác như kiểm soát truy cập (logic và/hoặc vật lý), thuê dịch vụ lưu trữ vào đám mây của nhà cung cấp dịch vụ (ISP Cloud) v.v.

5. Để đáp ứng yêu cầu tại Nhóm A.11 Yêu cầu A.11.1.2 "Physical entry controls" Phụ lục A – ISO 27001:2013, một Giám đốc doanh nghiệp đã có quy định ra vào phòng máy chủ của công ty theo ngày giờ làm việc. Cụ thể, các nhân viên chuyên trách của Phòng CNTT chỉ được ra vào phòng máy chủ của doanh nghiệp từ Thứ Hai đến Thứ Sáu

trong khoảng thời gian từ 12g00 – 17g00 trong các ngày đó. Khi phát sinh nhu cầu ra vào ngoài thời gian trên, Trưởng Phòng CNTT phải xin ý kiến Giám đốc doanh nghiệp để có giấy phép ra vào phòng máy chủ ngoài giờ quy định.

Theo bạn, doanh nghiệp đã áp dụng mô hình nào trong 4 mô hình kiểm soát truy cập sau đây để kiểm soát việc ra vào phòng máy chủ - *chọn một câu trả lời (a/b/c/d) dưới đây làm đáp án của bạn cho câu hỏi này*

a) Discretionary access control (DAC) *(Kiểm soát truy cập tùy ý);*
b) Mandatory access control (MAC) *(Kiểm soát truy cập bắt buộc);*
c) Role-based access control (RBAC) *(Kiểm soát truy cập dựa vào vai trò);*
d) Rule-based access control (RuBAC) *(Kiểm soát truy cập dựa vào quy tắc).*

6. Theo yêu cầu trong Phụ lục A - ISO 27001:2013 tại Nhóm A.8 Yêu cầu A.8.1 thì doanh nghiệp phải thực hiện 4 biện pháp kiểm soát (controls) về quản lý tài sản để đạt mục tiêu (objective) *"To identify organizational assets and define appropriate protection responsibilities"*. Là một nhân viên phụ trách ATTT, yêu cầu nào là thách thức nhất trong 4 yêu cầu tại điều Yêu cầu A.8.1 này *(chọn một câu trả lời (a/b/c/d) dưới đây làm đáp án của bạn cho câu hỏi này). Sau khi chọn xong, hãy ghi ra lý do bạn chọn câu trả lời như vậy:*

a) Kiểm kê tài sản ("Inventory of assets");

b) Quyền sở hữu tài sản ("Ownership of assets");

c) Sử dụng hợp lý tài sản ("Acceptable use of assets");

d) Bàn giao tài sản ("Return of assets").

7. Người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng nước mưa kết hợp triều cường tại thành phố HCM đã tràn vào phòng máy chủ của doanh nghiệp đặt tại tầng trệt của một tòa nhà. Phòng máy chủ này bị ngập nước sâu hơn 20cm từ 21g00 hôm trước và đến 06g00 sáng hôm nay nước mới rút hết. Do các phương tiện xử lý thông tin như máy chủ, thiết bị mạng,…trong phòng máy chủ không bị tổn hại gì nên doanh nghiệp vẫn làm việc như bình thường.

Theo bạn, sự kiện ngập nước phòng máy chủ có phải là sự kiện ảnh hưởng đến ATTT hay không; và có hay không doanh nghiệp trên đã không đáp ứng (hay không phù hợp với) với Điều nào trong Yêu cầu A.16.1 Nhóm A.16 của Phụ lục A - ISO 27001:2013? - *chọn một câu trả lời (a/b/c/d/e) trong số các trả lời sau đây làm đáp án của bạn cho câu hỏi này*:

a) Đó là một sự kiện ATTT; không đáp ứng Điều A.16.1.6 và A.16.1.7.
b) Đó là một sự kiện ATTT; không đáp ứng Điều A.16.1.2 và A.16.1.3;
c) Đó là một sự kiện ATTT; không đáp ứng Điều A.16.1.1 và A.16.1.2;
d) Đó không là một sự kiện ATTT vì không có tổn hại đến tài sản CNTT của doanh nghiệp; không đáp ứng Điều A.16.1.2 và A.16.1.3;
e) Đó không là một sự kiện ATTT vì không có gián đoạn vận hành hệ thống thông tin tại doanh nghiệp; không đáp ứng Điều A.16.1.1 và A.16.1.4.

---------- ./. ----------