TRƯỜNG ĐẠI HỌC VĂN HIẾN
KHOA CÔNG NGHỆ THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

1. Thông tin về học phần

- Tên học phần: **XÂY DỰNG CHUẨN AN TOÀN THÔNG TIN CHO DOANH NGHIỆP - INFORMATION SECURITY POLICIES, PROCEDURES, AND STANDARDS**
- Mã học phần: INT449
- Số tín chỉ: 3 (2/0/4)
- Bậc đào tạo: Đại học
- Loại học phần: Tự chọn
- Học phần tiên quyết/ Học phần trước: An toàn mạng máy tính
- Đơn vị phụ trách: Khoa Công Nghệ Thông Tin
- Số giờ tín chỉ: 60 tiết , trong đó:
- Lý thuyết: 30 tiết (1 tín chỉ LT = 15 tiết)
- Thực hành: 30 tiết (1 tín chỉ TH = 30 tiết)
- Thực tập: 0 (1 tín chỉ TT = 60 giờ TT tại cơ sở)
- Đồ án/ Khóa luận: 0 (1 tín chỉ ĐA/KL = 45 giờ làm ĐA/KL)

2. Thông tin về giảng viên

- Họ và tên: Nguyễn Hữu Hương Xuân
- Chức danh, học vị: Thạc sĩ
- Thời gian làm việc: Giờ hành chính (8:00 -16:00)
- Địa điểm làm việc: Khoa CNTT - Trường Đại học Văn Hiến
- Điện thoại: 0907981812
- Email: xuannhh@vhu.edu.vn

3. Tóm tắt nội dung học phần

Môn học này giới thiệu tổng quan các vấn đề nền tảng và các chuẩn về bảo mật thông tin trong doanh nghiệp từ góc nhìn của nhà quản lý. Từ đó, những chủ đề mới được giới thiệu và bàn luận cụ thể cho các hệ thống quản lý bảo mật thông tin trong bối cảnh kinh tế-

xã hội-khoa học-kỹ thuật hiện đại. Những chủ đề mới liên quan đến an toàn và bảo mật thông tin của hệ thống thông tin quản lý trong doanh nghiệp cũng sẽ được lựa chọn để giới thiệu và thảo luận.

4. Mục tiêu của học phần

Sau khi hoàn thành môn học này, học viên sẽ có khả năng:

- Hiểu được các vấn đề cơ bản của bảo mật thông tin và tác động của chúng đối với sự phát triển của tổ chức/doanh nghiệp.
- Nhận biết và hiểu rõ vai trò của nhà quản lý trong bảo mật thông tin tại tổ chức/doanh nghiệp.
- Đề xuất và lập kế hoạch cho các chính sách bảo mật và an toàn thông tin tại tổ chức/doanh nghiệp.
- Tư vấn về các giải pháp liên quan đến chính sách bảo mật và an toàn thông tin trong quá trình phát triển các hệ thống thông tin quản lý.
- Đánh giá mức độ bảo mật của hệ thống thông tin trong tổ chức/doanh nghiệp.

5. Chuẩn đầu ra của học phần:

TT	Mã CĐR	Nội dung chuẩn đầu ra
4.1	**Về kiến thức**	
4.1.1	CLO1	**Hiểu** được các vấn đề cơ bản của bảo mật thông tin cũng như ảnh hưởng của chúng đến sự phát triển của tổ chức/doanh nghiệp
4.1.2	CLO2	**Nhận biết và hiểu rõ** vai trò của nhà quản lý đối với bảo mật thông tin trong tổ chức/doanh nghiệp
4.1.3	CLO3	**Đánh giá** được mức độ bảo mật của hệ thống thông tin trong tổ chức/doanh nghiệp
4.1.4	CLO4	**Tư vấn** các giải pháp về chính sách bảo mật và an toàn thông tin trong quá trình phát triển các hệ thống thông tin quản lý
4.2	**Về kỹ năng**	

4.2.1	CLO5	**Ứng dụng** tốt và làm chủ các công cụ cần thiết; có khả năng phân tích và tổng hợp kiến thức, cập nhật được những thay đổi về công nghệ theo xu thế hiện đại
4.2.2	CLO6	**Thành thạo** kỹ năng làm việc hiệu quả theo nhóm; kỹ năng giao tiếp hiệu quả thông qua viết, thuyết trình, thảo luận. Vận dụng xây dựng, tổ chức, điều hành và quản lý các dự án liên quan có hiệu quả
4.2.3	CLO7	**Có kỹ năng** tự cập nhật những thay đổi, nắm bắt các tiến bộ khoa học kỹ thuật, có khả năng tự học, tự nghiên cứu, làm việc độc lập.
4.3	**Mức tự chủ và trách nhiệm**	
4.3.1	CLO8	**Tuân thủ** bảo vệ tính riêng tư trong tổ chức
4.3.2	CLO9	**Tự học tập, tích lũy kiến thức**, kinh nghiệm để nâng cao trình độ chuyên môn nghiệp vụ

Ma trận liên kết giữa Chuẩn đầu ra chương trình đào tạo và Chuẩn đầu ra học phần

Chuẩn đầu ra	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8	PLO9
CLO1	X	X							
CLO2	X	X							
CLO3		X	X						
CLO4				X					
CLO5				X			X		
CLO6					X	X			
CLO7						X	X		
CLO8									X
CLO9									

***Ghi chú: PLOs** (ProgrammeLearningOutcomes): Chuẩn đầu ra cấp CTĐT*

***CLOs**(Course LearningOutcomes): Chuẩn đầu ra học phần*

6. Nội dung chi tiết của học phần

6.1. Lý thuyết

Chương	Nội dung	Đáp ứng CLOs
Chương 1.	**Tổng quan về bảo mật an toàn thông tin doanh nghiệp**	CLO1, CL08
1.1.	Tầm quan trọng của an toàn bảo mật thông tin trong doanh nghiệp	
1.2.	Rủi ro và nguy cơ	
1.3.	Chính sách và quy trình bảo mật	
1.4.	Giới thiệu về Information security management system (ISMS)	
Chương 2.	**Hệ thống quản lý bảo mật thông tin theo chuẩn ISO 27001**	CLO1, CL06, CL08, CL09
2.1.	Giới thiệu về ISO 27001	
2.2.	Cấu trúc và yêu cầu của ISO 27001	
2.3.	Quá trình triển khai ISO 27001:	
2.4.	Lợi ích của việc tuân thủ ISO 27001:	
2.5.	Thách thức và chi phí của việc triển khai ISO 27001:	
Chương 3.	Quản lý Rủi ro và Tuân thủ Pháp luật	CLO1, CL02, CL03, CL06, CL07, CLO9
3.1.	**Quản lý Rủi ro:** • Hiểu về quy trình quản lý rủi ro và các bước chính trong quá trình này, bao gồm: xác định rủi ro, đánh giá rủi ro, xử lý rủi ro và theo dõi và đánh giá. • Phát triển kế hoạch quản lý rủi ro dựa trên phân tích rủi ro và xác định các biện pháp kiểm soát phù hợp để giảm thiểu hoặc loại bỏ rủi ro.	
3.2.	**Tuân thủ Pháp luật về Bảo mật Thông tin:** Nắm vững các quy định và yêu cầu của các pháp luật quan trọng như GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), PCI-DSS (Payment Card Industry Data Security Standard),	

Chương	Nội dung	Đáp ứng CLOs
3.3.	**Đánh giá Rủi ro và Tuân thủ Pháp luật:** • Thực hiện đánh giá rủi ro để xác định mức độ tuân thủ hiện tại của doanh nghiệp với các quy định pháp luật liên quan đến bảo mật thông tin. • Đưa ra các biện pháp cần thiết để cải thiện tuân thủ và giảm thiểu rủi ro theo các quy định pháp luật	
3.4.	**Giám sát và Đánh giá:** • Thực hiện giám sát liên tục để đảm bảo rằng các hoạt động của doanh nghiệp tuân thủ các quy định pháp luật và các biện pháp quản lý rủi ro đã được triển khai. • Đánh giá hiệu quả của các biện pháp kiểm soát và các chính sách và quy trình tuân thủ và thực hiện điều chỉnh khi cần thiết.	
Chương 4.	**Quản lý tài sản và bảo mật thông tin liên quan đến yếu tố con người**	CL02, CL03, CL04, CL05, CL06, CL07, CL09
4.1.	**Khái niệm về quản lý tài sản thông tin:** 4.1.1. Định nghĩa và ý nghĩa của quản lý tài sản thông tin trong bảo mật thông tin. 4.1.2. Mô tả cách quản lý tài sản thông tin có thể giúp đảm bảo sự bảo vệ hiệu quả cho thông tin quan trọng của tổ chức.	
4.2.	**Tài sản thông tin và phân loại:** 4.2.1. Mô tả các loại tài sản thông tin phổ biến trong tổ chức, bao gồm dữ liệu khách hàng, thông tin tài chính, thông tin nhân viên, và các tài liệu quan trọng khác. 4.2.2. Phân loại tài sản thông tin dựa trên mức độ quan trọng và nhạy cảm, từ đó xác định các biện pháp bảo mật phù hợp.	

Chương	Nội dung	Đáp ứng CLOs
4.3.	**Quản lý nhân viên và bảo mật thông tin:** 4.3.1. Đào tạo nhân viên về quy định, chính sách và thực tiễn bảo mật thông tin để đảm bảo sự nhận thức và tuân thủ. 4.3.2. Kiểm soát truy cập và quản lý quyền:	
4.4.	**Kiểm soát truy cập và quản lý quyền:** 4.4.1. Mô tả cách quản lý quyền truy cập vào tài sản thông tin, bao gồm việc thiết lập các phân quyền và kiểm soát truy cập dựa trên nguyên tắc "cần biết, cần dùng". 4.4.2. Đề xuất các biện pháp kiểm soát để đảm bảo rằng chỉ những người có nhu cầu và quyền hạn cần thiết mới có thể truy cập vào thông tin.	
4.5.	**Bảo mật thông tin liên quan đến người dùng cuối:** Đề cập đến việc bảo vệ thông tin cá nhân của người dùng cuối, bao gồm các biện pháp như mã hóa dữ liệu, quản lý danh sách phân quyền, và kiểm soát truy cập.	
4.6.	**Quản lý rủi ro và tuân thủ:** 4.6.1. Hướng dẫn về cách quản lý và đánh giá rủi ro liên quan đến quản lý tài sản thông tin và bảo mật thông tin liên quan đến yếu tố con người. 4.6.2. Mô tả cách đảm bảo tuân thủ các chuẩn mực và quy định pháp lý liên quan đến bảo mật thông tin và quản lý tài sản thông tin.	
Chương 5:	**Bảo mật Hạ tầng Mạng**	CL02, CL03, CL04, CL05, CL06,
5.1.	**Kiến thức về cấu trúc và hoạt động của mạng máy tính:** • Giới thiệu về cấu trúc của mạng máy tính, bao gồm các thành phần chính như máy chủ, thiết bị mạng, và kết nối mạng.	

Chương	Nội dung	Đáp ứng CLOs
	• Hiểu về các giao thức mạng như TCP/IP, DNS, DHCP và cách chúng hoạt động.	CL07, CL09
5.2.	**Phương pháp bảo mật mạng như firewall, IDS/IPS, VPN, v.v.:** • Giải thích vai trò và chức năng của các công nghệ bảo mật mạng như Firewall (Tường lửa), IDS/IPS (Hệ thống phát hiện/ Ngăn chặn xâm nhập), VPN (Mạng riêng ảo). • Hướng dẫn về việc triển khai và cấu hình các giải pháp bảo mật mạng này để bảo vệ mạng và dữ liệu. •	
5.3.	**Bảo mật các công nghệ không dây và di động:** • Đánh giá các nguy cơ bảo mật đặc biệt của mạng không dây và thiết bị di động. • Phân tích các biện pháp bảo mật như mã hóa, quản lý thiết bị di động (MDM), và cách tạo mạng Wi-Fi an toàn.	
Chương 6	**Bảo mật Hệ thống và Ứng dụng**	CL02, CL03, CL04, CL05, CL06, CL07, CL09
6.1.	**Bảo mật hệ điều hành và phần mềm cơ sở dữ liệu:** Hướng dẫn về việc cài đặt và cấu hình hệ điều hành và phần mềm cơ sở dữ liệu một cách an toàn. Phân tích các biện pháp bảo mật như cập nhật phần mềm, cấu hình an toàn và mã hóa dữ liệu.	
6.2.	**Phương pháp phát hiện và ngăn chặn các lỗ hổng bảo mật trong ứng dụng phần mềm:** Hiểu về các lỗ hổng bảo mật phổ biến trong ứng dụng phần mềm và cách khai thác chúng. Hướng dẫn về việc sử dụng công cụ kiểm thử bảo mật để phát hiện và khắc phục các lỗ hổng bảo mật này.	

Chương	Nội dung	Đáp ứng CLOs
Chương 7	**Quản lý Quyền Truy Cập và Xác Thực**	CL02, CL03, CL04, CL05, CL06, CL07, CL09
7.1.	**Thiết lập và quản lý hệ thống quyền truy cập dựa trên nguyên tắc "least privilege":** Giải thích nguyên tắc "least privilege" và tại sao nó quan trọng trong bảo mật thông tin. Hướng dẫn về việc thiết lập và quản lý quyền truy cập để giảm thiểu rủi ro bảo mật.	
7.2.	**Xác thực hai yếu tố (2FA) và các phương pháp xác thực mạnh mẽ khác:** Giới thiệu về xác thực hai yếu tố (2FA) và các phương pháp xác thực mạnh mẽ khác như biometrics (nhận dạng sinh học), token OTP (One-Time Password), v.v. Hướng dẫn về việc triển khai và quản lý các phương pháp xác thực này để tăng cường bảo mật.	

6.2. Thực hành

Modul	Nội dung	Đáp ứng CLOs
6.2.1	**Bài tập thực hành**	
1	**Phân tích Rủi ro:** • Chọn một hệ thống hoặc ứng dụng cụ thể và thực hiện một bài phân tích rủi ro. Xác định các rủi ro tiềm ẩn và ảnh hưởng của chúng đối với hệ thống hoặc ứng dụng đó. • Đề xuất các biện pháp kiểm soát để giảm thiểu hoặc loại bỏ các rủi ro đã xác định.	CLO5, CLO6, CLO7, CLO8, CLO9
2	**Xác định Tuân thủ Pháp luật:**	

	• Nghiên cứu và phân tích các yêu cầu của một pháp luật bảo mật thông tin cụ thể như GDPR, HIPAA hoặc PCI-DSS. • Áp dụng các yêu cầu này vào một môi trường doanh nghiệp cụ thể và xác định mức độ tuân thủ hiện tại của doanh nghiệp.	
3	**Triển khai Công cụ Bảo mật:** • Chọn một công cụ bảo mật như firewall, IDS/IPS hoặc mã hóa và thực hiện việc triển khai và cấu hình. • Thực hiện các bài kiểm tra và thử nghiệm để đảm bảo rằng công cụ hoạt động hiệu quả và đáp ứng các yêu cầu bảo mật.	
4	**Triển khai Xác thực Hai Yếu Tố (2FA):** • Lập kế hoạch và triển khai một hệ thống xác thực hai yếu tố cho một ứng dụng hoặc hệ thống cụ thể. • Sử dụng các phương tiện như mã OTP (One-Time Password), thông điệp SMS, ứng dụng xác thực di động, hoặc thiết bị token để tạo lớp bảo vệ bổ sung cho quá trình đăng nhập.	
5	**Xác thực qua Email hoặc OTP:** • Phát triển một hệ thống xác thực dựa trên email hoặc mã OTP được gửi đến email hoặc điện thoại di động của người dùng. • Kiểm tra tính năng và độ tin cậy của việc sử dụng email hoặc tin nhắn điện thoại để xác thực người dùng.	

7. Phân bổ thời gian theo tiết và điều kiện thực hiện:

Chương	Tên chương	Số tiết tín chỉ					Ghi chú
		Lý thuyết	Bài tập	Thực hành	Tự học	Tổng	
1	Tổng quan về bảo mật an toàn thông tin doanh nghiệp	2	0	0	4	6	

Chương	Tên chương	Số tiết tín chỉ					Ghi chú
		Lý thuyết	Bài tập	Thực hành	Tự học	Tổng	
2	Hệ thống quản lý bảo mật thông tin theo chuẩn ISO 27001	3	0	5	6	14	
3	Quản lý Rủi ro và Tuân thủ Pháp luật	5	0	5	10	20	
4	Quản lý tài sản và bảo mật thông tin liên quan đến yếu tố con người	7	0	5	14	26	
5	Bảo mật Hạ tầng Mạng	5	0	5	10	20	
6	Bảo mật Hệ thống và Ứng dụng	5	0	5	10	20	
7	Quản lý Quyền Truy Cập và Xác Thực	3	0	5	6	14	
Tổng		**30**	**0**	**30**	**60**	**120**	

8. Phương pháp giảng dạy:

Giảng viên giảng dạy với sự kết hợp của một số phương pháp sau:

Gợi ý:

- Thuyết trình
- Phát vấn
- Hỏi lại hoặc vấn đáp

Ma trận liên kết giữa Chuẩn đầu ra với phương pháp giảng dạy

Phương pháp giảng dạy	CLO1	CLO2	CLO3	CLO4	CLO5	CLO6	CLO7	CLO8	CLO9
Thuyết trình	X	X	X	X	X	X	X	X	X
Phát vấn	X								
Hỏi lại hoặc vấn đáp			X	X	X	X	X	X	X

9. Phương pháp học tập

Sinh viên học tập với sự kết hợp của một số phương pháp sau:

Gợi ý:

- Làm việc nhóm
- Tự học, tự nghiên cứu

Ma trận liên kết giữa Chuẩn đầu ra với phương pháp học tập

Phương pháp học tập	CLO1	CLO2	CLO3	CLO4	CLO5	CLO6	CLO7	CLO8	CLO9
Làm việc nhóm	X		X	X				X	X
Tự học, tự nghiên cứu	X	X	X	X			X	X	X

10. Nhiệm vụ của sinh viên

Gợi ý:

- Chủ động tổ chức thực hiện giờ tự học.
- Tham gia đầy đủ các giờ lên lớp và giờ thuyết trình (sinh viên chỉ được vắng mặt tối đa 20% thời gian lên lớp của học phần).
- Đọc tài liệu tham khảo bắt buộc và bổ trợ do giảng viên giới thiệu.
- Hoàn thành đầy đủ các bài tập cá nhân, bài tập nhóm.
- Tham gia kỳ thi kết thúc học phần.

11. Thang điểm đánh giá: Điểm đánh giá quá trình và điểm thi kết thúc học phần được chấm theo thang điểm 10 (từ 0 đến 10), làm tròn đến 1 chữ số thập phân.

12. Phương pháp kiểm tra, đánh giá kết quả học tập

Sinh viên được đánh giá kết quả học tập trên cơ sở hai điểm thành phần như sau:

1. *Điểm đánh giá quá trình: trọng số 40% bao gồm:*

a. Điểm chuyên cần: 10, trọng số 50%

b. Điểm kiểm tra giữa kỳ: 10, trọng số 50%

2. *Điểm thi kết thúc học phần: trọng số 60%*

Hình thức thi: Trắc nghiệm theo ngân hàng đề thi

Ma trận quan hệ giữa Chuẩn đầu ra và phương pháp kiểm tra, đánh giá

Hình thức đánh giá	CLO1	CLO2	CLO3	CLO4	CLO5	CLO6	CLO7	CLO8	CLO9
Chuyên cần								X	X
Giữa kỳ	X				X	X	X	X	
Trắc nghiệm	X	X	X	X	X	X	X	X	

13. Tài liệu phục vụ cho học phần (các tài liệu xuất bản trong 05 năm trở lại đây và cung cấp được cho Trung tâm Học liệu nơi đặt tài liệu)

13.1. Tài liệu chính

[1]. Landoll, D. J. (2017). *Information Security Policies, Procedures, and Standards: A Practitioner's Reference*. Auerbach Publications.

[2]. Calder, A. (2021). *ISO 22301: 2019 and business continuity management–Understand how to plan, implement and enhance a business continuity management system (BCMS)*. IT Governance Publishing.

13.2. Tài liệu tham khảo

[3]. Calder, A., & Watkins, S. G. (2010). Information security risk management for ISO27001/ISO27002. It Governance Ltd.

[4]. Field, A. (2023). Risk Management and ISO 31000-A pocket guide. IT Governance Ltd.

[5]. Parry, P. (2020). The bottom line: how to build a business case for ISO 14001. CRC Press.

TP.Hồ Chí Minh, ngày 27 tháng 03 năm 2024

Hiệu trưởng	Phó trưởng Khoa	Giảng viên biên soạn
Duyệt	(Ký và ghi rõ họ tên)	(Ký và ghi rõ họ tên)
		
	NGUYỄN THỊ DIỆU ANH	**NGUYỄN HỮU HƯƠNG XUÂN**