TRƯỜNG ĐẠI HỌC NGÂN HÀNG TP. HCM
KHOA HỆ THỐNG THÔNG TIN QUẢN LÝ

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

TP. Hồ Chí Minh, ngày 16 tháng 01 năm 2023

ĐỀ CƯƠNG MÔN HỌC
AN TOÀN BẢO MẬT THÔNG TIN

A. THÔNG TIN CHUNG VỀ MÔN HỌC

1. **Tên môn học (tiếng Việt)** : **AN TOÀN BẢO MẬT THÔNG TIN**
2. **Tên môn học (tiếng Anh)** : **Information Security**
3. **Mã số môn học** : **ITS307**
4. **Trình độ đào tạo** : **Đại học chính quy**
5. **Ngành đào tạo áp dụng** : **Hệ thống thông tin quản lý**
6. **Số tín chỉ** 03
   - Lý thuyết : 02
   - Thảo luận và bài tập : 00
   - Thực hành : 01
   - Khác (ghi cụ thể) : Tự học, bài tập cá nhân và bài tập nhóm
7. **Phân bổ thời gian**:
   - Tại giảng đường : 60 tiết
   - Tự học ở nhà : 20 giờ để đọc tài liệu
   - Trực tuyến : Giảng viên có thể bố trí học online nhưng tổng số không quá 30% số tiết của toàn môn học
   - Khác (ghi cụ thể) : làm bài tập cá nhân và bài tập nhóm chiếm tối thiểu 2 lần so với thời gian học tập trên lớp
8. **Khoa quản lý môn học** : Khoa Hệ Thống Thông Tin Quản Lý
9. **Môn học trước** : Mạng máy tính và truyền thông
10. **Mô tả môn học**:

An toàn bảo mật thông tin là môn học bắt buộc thuộc khối kiến thức ngành.

Môn học giới thiệu tổng quan về an toàn bảo mật, các thành phần, nguyên tắc, cũng như các vấn đề về hacker, virus, thiên tai…; giới thiệu hệ thống phát hiện tấn công; các nguyên lý, phương pháp cũng như mô hình, kỹ thuật mã hóa; phân tích rủi ro và lập kế hoạch phục hồi hệ thống khi có sự cố.

11. Mục tiêu và chuẩn đầu ra của môn học

11.1 Mục tiêu của môn học

Mục tiêu	Mô tả mục tiêu	Nội dung CĐR CTĐT phân bổ cho môn học	CĐR CTĐT
(a)	(b)	(c)	(d)
CO1	Môn học này cung cấp cho sinh viên những kiến thức cơ bản nhất về an toàn và bảo mật máy tính, bao gồm cả nguyên lí kiến thiết và các phương pháp bảo mật	Khả năng vận dụng kiến thức nền tảng và chuyên sâu một cách hệ thống để giải quyết các vấn đề chuyên môn trong ngành HTTTQL	PLO6
		Khả năng ứng dụng kỹ thuật và công cụ hiện đại cho thực hành kỹ thuật và thích ứng với các xu hướng thay đổi trong ngành HTTTQL	PLO8
CO2	Môn học này giúp cho sinh viên có các kỹ năng cần thiết để nhận dạng vấn đề về an toàn bảo mật trong hệ thống thông tin nhằm đánh giá, ngăn chặn, đưa ra giải pháp phù hợp	Thể hiện ý thức tuân thủ pháp luật, đạo đức nghề nghiệp và trách nhiệm xã hội đối với ngành HTTTQL	PLO5
		Khả năng vận dụng kiến thức nền tảng và chuyên sâu một cách hệ thống để giải quyết các vấn đề chuyên môn trong ngành HTTTQL	PLO6

		Khả năng ứng dụng kỹ thuật và công cụ hiện đại cho thực hành kỹ thuật và thích ứng với các xu hướng thay đổi trong ngành HTTTQL	PLO8

11.2. ***Chuẩn đầu ra của môn học (CĐR MH) và sự đóng góp vào chuẩn đầu ra của chương trình đào tạo (CĐR CTĐT)***

CĐR MH	Nội dung CĐR MH	Mức độ theo thang đo của CĐR MH	Mục tiêu môn học	CĐR CTĐT
(a)	(b)	(c)	(d)	(e)
CLO1	Biết được kiến thức cơ bản về an toàn bảo mật thông tin	1	CO1	PLO6
CLO2	Hiểu được các kiến thức trong môn học, để có cách	2	CO1	PLO5, PLO6
	nhìn nhận tổng quan về các vấn đề liên quan đến an toàn bảo mật các hệ thống thông tin			
CLO3	Làm việc thực hành theo nhóm để nắm bắt các kỹ năng cơ bản cần có khi hoạt động nhóm, triển khai các công cụ đã được giới thiệu	3	CO1, CO2	PLO5, PLO6, PLO8
CLO4	Vận dụng các kiến thức đã học để áp dụng các giải pháp xây dựng an toàn và bảo mật hệ thống thông tin	3	CO2	PLO5, PLO6, PLO8

11.3 Ma trận đóng góp của môn học cho PLO

Mã CĐR MH	PLO5	PLO6	PLO8
CLO1		1	
CLO2	2	2	
CLO3	3	3	3
CLO4	3	3	3

12. Phương pháp dạy và học

- Phương pháp "Người học là trung tâm" sẽ được sử dụng trong môn học để giúp sinh viên tham gia tích cực. Kết quả học tập dự kiến sẽ đạt được thông qua một loạt các hoạt động học tập ở trường và ở nhà.

- Giảng dạy, liên hệ thực tế và hỗ trợ sinh viên khi thực hành, thảo luận, đặt câu hỏi và trả lời câu hỏi.

- Tại lớp, giảng viên giải thích các định nghĩa, nền tảng lý thuyết, cách sử dụng các ứng dụng có liên quan; đặt ra các vấn đề, hướng dẫn và khuyến khích sinh viên giải quyết; sau đó tóm tắt nội dung của bài học, giải đáp các câu hỏi của sinh viên. Giảng viên cũng trình bày và thực hành làm mẫu cho sinh viên.

- Sinh viên cần lắng nghe và ghi chép và được khuyến khích nêu lên các câu hỏi, giải quyết các vấn đề và thực hành các bài tập dưới sự hướng dẫn của giảng viên.

- Quy định về hình thức giảng dạy: Giảng viên có thể chủ động lựa chọn hình thức giảng dạy là trực tuyến (online) kết hợp trực tiếp (offline), đảm bảo tổng thời gian giảng dạy trực tuyến không vượt quá 30% thời gian giảng dạy của cả môn học.

13. Yêu cầu môn học

- Sinh viên tuân thủ nghiêm túc các nội quy và quy định của Khoa và Trường.

- Đọc và nghiên cứu các tài liệu bài giảng trước khi lên lớp.

- Chấp hành nghiêm túc nội quy phòng máy.

- Thực hiện đầy đủ các bài tập thực hành được giao.

- Tham dự đầy đủ các buổi học trên lớp và các buổi thực hành do giảng viên trực tiếp hướng dẫn.

- Tự tìm hiểu thêm thông tin trên mạng Internet về các kiến thức liên quan đến môn học.

- Tham gia đầy đủ và tích cực các hoạt động trong quá trình học tập.

- Đối với bất kỳ sự gian lận nào trong quá trình làm bài tập hay bài thi, sinh viên phải chịu mọi hình thức kỷ luật theo quy định của Trường và bị 0 điểm cho nội dung đó.

14. Học liệu của môn học

14.1 Giáo trình

Tập bài giảng và bài thực hành tình huống được biên soạn và sử dụng thống nhất trong bộ môn. Giảng viên sẽ cung cấp cho cho sinh viên các file tài liệu.

14.2 Tài liệu tham khảo

- Emmett Dulaney and Chuck Easttom, CompTIA® Security+™ Study Guide: Exam SY0-501, Seventh Edition, Sybex 2017

- Joel Scambray, Stuart Mcclure, George Kurtz, Hacking Exposed: Network Security Secrets & Solutions 7th, McGraw Hill 2012

B. PHƯƠNG THỨC ĐÁNH GIÁ MÔN HỌC

1. Các thành phần đánh giá môn học

Thành phần đánh giá	Phương thức đánh giá	Các CĐR MH	Trọng số
A.1. Đánh giá quá trình	A.1.1. Chuyên cần	CLO1, CLO2	10%
	A.1.2. Kiểm tra	CLO1, CLO2,	20%
	A.1.3. Tiểu luận nhóm	CLO1, CLO2,	20%
A.2. Đánh giá cuối kỳ	A.2.1. Thi cuối kỳ	CLO1, CLO2	50%

2. Nội dung và phương pháp đánh giá

A.1. Đánh giá quá trình

A.1.1. **Chuyên cần**

Hình thức đánh giá dựa vào điểm danh (số buổi đi học)

A.1.2. Bài kiểm tra

Hình thức đánh giá: kết quả tổng hợp 5 bài thực hành cá nhân và thi trắc nghiệm giữa kỳ. Sinh viên thực hành và ghi báo cáo kết quả gửi về cho giảng viên cho từng bài thực hành.

Bài tập thực hành 1: Tìm hiểu về các chương trình diệt virus thông dụng. Tìm hiểu một số công cụ hữu ích trong Hiren Boot CD.

Bài tập thực hành 2: Tìm hiểu chương trình tìm lại mật khẩu Ophcrack.

Bài tập thực hành 3: Tìm hiểu và triển khai cấu hình cho wireless access point.

Bài tập thực hành 4: Tìm hiểu các phần mềm phân tích tín hiệu, phát hiện gói tin.

Bài tập thực hành 5: Tìm hiểu và thực hiện kiểm tra tính an toàn mạng không dây triển khai theo cơ chế bảo mật WEP, WPA bằng công cụ Backtrack CD/DVD.

A.1.3. Tiểu luận nhóm

Mỗi nhóm sẽ chọn tùy ý một đề tài liên quan đến An toàn bảo mật thông tin; sau đó đọc hiểu và viết lại báo cáo dưới dạng Word và trình bày trước lớp về đề tài nhóm đã chọn và đọc hiểu.

- Sinh viên làm việc theo nhóm (không quá 5 thành viên)

- Sản phẩm: bài tiểu luận không quá 30 trang

A.2.1 Thi cuối kỳ

Đề thi được chọn ngẫu nhiên từ ngân hàng đề thi môn An Toàn Bảo Mật Thông Tin, 02 đề. Các câu hỏi trắc nghiệm có 4 phương án lựa chọn và chỉ có một phương án đúng.

- Thời gian làm bài thi: 75 phút.
- Phương thức đánh giá: Được chấm 2 lượt độc lập bởi 2 giảng viên. Điểm bài thi được chấm theo đáp án Ngân hàng đề thi môn An Toàn Bảo Mật Thông Tin.
- Điểm số tối đa là 100 điểm. Sẽ được quy đổi về điểm 10.

3. Các rubrics đánh giá

A.1.1. Chuyên cần

Tiêu chí đánh giá	Trọng số	Thang điểm
Số buổi hiện diện của sinh viên	80%	Được tính theo công thức *Điểm hiện diện* = *số buổi hiện diện* x $\frac{10}{\text{Tổng số buổi học của môn học}}$
Tính tích cực tham gia hoạt động tại giảng	20%	0 / 10 điểm khi "không tham gia" / "có tham gia" quá trình thảo luận về nội dung bài học

A.1.2. Bài kiểm tra cá nhân

Bao gồm điểm đánh giá 5 bài thực hành và điểm kiểm tra giữa kỳ

Tiêu chí đánh giá	Trọng số	Thang điểm	
		0	10
Bài thực hành	50%	Không tham dự buổi thực hành	Tham dự tất cả các buổi thực hành và nộp báo cáo kết quả (đánh giá 2đ cho mỗi buổi tham dự và nộp báo cáo)
Kiểm tra giữa kỳ	50%	Trả lời sai đáp án	Trả lời đúng đáp án (Bài kiểm tra giữa kỳ có 20 câu hỏi. Mỗi câu trả lời đúng được 0.5đ)

A.1.3. Tiểu luận nhóm

Tiêu chí đánh giá	Trọng số	Thang điểm tối đa
		10
Nội dung đề tài	20%	Tên và nội dung đề tài phù hợp với môn học
Tính mới của đề tài	20%	Đề tài có tính mới tại thời điểm học môn học
Hình thức trình bày báo cáo	20%	- Số liệu cập nhật, trích dẫn tham chiếu nguồn tài liệu rõ ràng. - Đáp ứng đúng quy định về kết cấu của một báo cáo thực tập - Không sai lỗi chính tả, đánh máy, định dạng, in ấn

Trình bày báo cáo trước lớp	20%	Kỹ năng thuyết trình, tương tác với người nghe
Trả lời câu hỏi	20%	Trả lời đúng các câu hỏi được đặt ra
		Điểm trả lời câu hỏi = *số câu trả lời đúng x* $\frac{10}{\text{Tổng số câu hỏi được đặt ra}}$

A.2.1 Thi cuối kỳ

Tiêu chí đánh giá	**Trọng số**	**Thang điểm**	
		0	**Điểm tương ứng cho từng câu trả lời đúng với**
Nội dung ý đáp án	100%	Trả lời sai	Trả lời đúng

C. NỘI DUNG CHI TIẾT GIẢNG DẠY

Thời lượng (tiết)	Nội dung giảng dạy chi tiết	CĐR MH	Hoạt động dạy và học	Phương pháp đánh giá	Học liệu
(a)	(b)	(c)	(d)	(e)	(f)
3 LT	**CHƯƠNG 1: CÁC KHÁI NIỆM TỔNG QUAN VỀ BẢO MẬT** **1.1 Bảo mật thông tin** 1.1.1 Các khái niệm 1.1.2 Bảo mật vật lý 1.1.3 Bảo mật hoạt động 1.1.4 Quản lý và các chính sách **1.2 Mục đích của bảo mật thông tin** **1.3 Quá trình bảo mật** 1.3.1 Triển khai phần mềm chống virus 1.3.2 Hiện thực kiểm soát truy cập 1.3.3 Chứng thực 1.3.4 Các dịch vụ và các giao thức mạng **1.4 Phân biệt các mô hình bảo mật** 1.4.1 Mục đích thiết kế 1.4.2 Các vùng bảo mật	CLO1, CLO2	Trực tiếp (offline) hay trực truyến (online) Giảng viên: trình bày tổng quan về bảo mật Sinh viên: lắng nghe, biết và hiểu nội dung bài	A1.1, A1.2, A1.3, A2.1	Bài giảng chương 1

	1.4.3 Các kỹ thuật 1.4.4 Các yêu cầu của doanh nghiệp				
3 LT 7 TH	**CHƯƠNG 2: CÁC RỦI RO TIỀM TÀNG** **2.1 Tính toán các chiến thuật tấn công** 2.1.1 Tấn công truy xuất 2.1.2 Tấn công phản đối, chỉnh sửa 2.1.3 Tấn công từ chối dịch vụ (DoS) **2.2 Các tấn công phổ biến** 2.2.1 Back-door 2.2.2 Spoofing 2.2.3 Man in the middle 2.2.4 Replay 2.2.5 Đoán mật khẩu **2.3 Những vấn đề về bảo mật TCP/IP** 2.3.1 Làm việc với các giao thức 2.3.2 Xác định các tấn công TCP/IP **2.4 Các chương trình nguy hại** 2.4.1 Virus 2.4.2 Trojan 2.4.3 Logic bomb 2.4.4 Worm	CLO1, CLO2, CLO3	Trực tiếp (offline) hay trực truyến (online) Giảng viên: trình bày các rủi ro tiềm tàng. Giới thiệu bài thực hành 1, 2 nhằm tìm hiểu về các chương trình diệt virus thông dụng, đĩa công cụ Hiren, phần mềm OphCrack. Sinh viên: lắng nghe, biết và hiểu nội dung bài. Thực hành bài thực hành số 1, 2.	A1.1, A1.2, A1.3, A2.1	Bài giảng chương 2

	2.4.5 Ransomware 2.4.6 Vấn đề con người				
4 LT, 3 TH	**CHƯƠNG 3: HẠ TẦNG VÀ KẾT NỐI** **3.1 Bảo mật cơ sở hạ tầng** 3.1.1 Các thành phần phần cứng 3.1.2 Các thành phần phần mềm **3.2 Sự khác biệt của các thiết bị mạng nền tảng** 3.2.1 Tường lửa 3.2.2 Hub 3.2.3 Bộ định tuyến (Router) 3.2.4 Bộ chuyển mạch (Switch) 3.2.5 Điểm truy cập không dây (Wireless Acess Point) 3.2.6 Các dịch vụ truy cập từ xa (RAS) 3.2.7 Hệ thống Telecoms/PBX 3.2.8 Các mạng riêng ảo (VPN)	CLO1, CLO2, CLO3	Trực tiếp (offline) hay trực truyến (online) Giảng viên: trình bày các nội dung của chương và đưa ra tình huống cụ thể mô hình mạng được triển khai trong phòng máy. Qua đó giới thiệu bài tập số 3 Sinh viên: lắng nghe, biết và hiểu. Thực hành bài thực hành 3	A1.1, A1.2, A1.3, A2.1	Bài giảng chương 3
5 LT, 10 TH	**CHƯƠNG 4: KIỂM TRA CÁC HOẠT ĐỘNG GIAO TIẾP** **4.1 Kiểm tra mạng** 4.1.1 Nhận dạng các luồng thông tin mạng 4.1.2 Quản lý các hệ thống mạng	CLO1, CLO2, CLO3	Trực tiếp (offline) hay trực truyến (online) Giảng viên: trình bày các nội dung của chương, giới thiệu các phần mềm gửi nhận thông điệp Giảng viên giới thiệu thêm về các công cụ phát hiện gói, phân	A1.1, A1.2, A1.3, A2.1	Bài giảng chương 4

	4.2 Các hệ thống phát hiện xâm nhập 4.2.1 Network-Based IDS 4.2.2 Host-Based IDS 4.2.3 Honey Pot 4.2.4 Đáp ứng rắc rối **4.3 Các hệ thống không dây** 4.3.1 Lớp vận chuyển không dây an toàn 4.3.2 Các giao thức không dây IEEE 802.11x 4.3.3 WEP/WAP **4.4 Các đặc điểm của các phần mềm gửi nhận thông điệp** **4.5 Phát hiện gói** **4.6 Phân tích tín hiệu** 4.6.1 Foot-printing 4.6.2 Scanning		tích tín hiệu Sinh viên: lắng nghe, biết và hiểu nội dung bài. Thực hành bài thực hành 4		
2 LT, 10 TH	**CHƯƠNG 5: HIỆN THỰC VÀ BẢO TRÌ MẠNG AN TOÀN** **5.1 Tổng quan về các mối đe dọa của mạng** **5.2 Nền tảng bảo mật** **5.3 Củng cố OS và NOS** **5.4 Củng cố các thiết bị mạng** 5.4.1 Cập nhật phần mềm điều khiển thiết bị	CLO1, CLO2, CLO3	Trực tiếp (offline) hay trực truyến (online) Giảng viên: trình bày các nội dung của chương Sinh viên: lắng nghe, biết và hiểu nội dung bài. Thực hành cập nhật củng cố phần mềm điều khiển thiết bị, củng cố các ứng dụng. Thực hành bài thực hành số 5	A1.1, A1.2, A1.3, A2.1	Bài giảng chương 5

	5.4.2 Cài đặt cấu hình bộ định tuyến/bộ chuyển mạch **5.5 Củng cố các ứng dụng** 5.5.1 Dịch vụ web 5.5.2 Dịch vụ email 5.5.3 Dịch vụ truyền nhận tập tin 5.5.4 Dịch vụ tên miền 5.5.5 Các dịch vụ chia sẻ tập tin và máy in 5.5.6 Dịch vụ DHCP				
3 LT	**CHƯƠNG 6: BẢO MẬT MẠNG VÀ MÔI TRƯỜNG** **6.1 Bảo mật vật lý và mạng** 6.1.1 Hiện thực kiểm soát truy cập 6.1.2 Tìm hiểu tâm lý người dùng 6.1.3 Quét môi trường **6.2 Kế hoạch kinh doanh** 6.2.1 Phân tích tác động an toàn trong việc kinh doanh 6.2.2 Đánh giá rủi ro **6.3 Phát triển các chính sách, các chuẩn và các hướng dẫn** 6.3.1 Hiện thực các chính sách 6.3.2 Các chuẩn kết hợp	CLO1, CLO2	Trực tiếp (offline) hay trực truyến (online) Giảng viên: trình bày các nội dung của chương Sinh viên: lắng nghe, biết và hiểu nội dung bài	A1.1, A1.2, A1.3, A2.1	Bài giảng chương 6

	6.3.3 Một số hướng dẫn **6.4 Phân loại thông tin** 6.4.1 Thông tin chung 6.4.2 Thông tin cá nhân 6.4.3 Vai trò trong quy trình an toàn 6.4.4 Kiểm soát truy cập thông tin				
6 LT	**CHƯƠNG 7: MẬT MÃ, CÁC PHƯƠNG PHÁP, VÀ CÁC CHUẨN MÃ HÓA** **7.1 Tổng quan về mật mã** 7.1.1 Tìm hiểu mã hóa vật lý 7.1.2 Tìm hiểu mã hóa toán học 7.1.3 Tìm hiểu mã hóa lượng tử **7.2 Các thuật giải mã hóa** 7.2.1 Hashing 7.2.2 Các thuật giải mã hóa đối xứng 7.2.3 Các thuật giải mã hóa bất đối xứng **7.3 Các vấn đề sử dụng hệ thống mã hóa** 7.3.1 Bảo mật 7.3.2 Nhất quán 7.3.3 Xác thực 7.3.4 Không thoái thác 7.3.5 Kiểm soát truy cập	CLO1, CLO2	Trực tiếp (offline) hay trực truyến (online) Giảng viên: trình bày các nội dung của chương Sinh viên: lắng nghe, biết và hiểu nội dung bài	A1.1, A1.2, A1.3, A2.1	Bài giảng chương 7

	7.4 Kiến trúc hạ tầng khóa công cộng 7.4.1 Sử dụng chứng thực quyền 7.4.2 Hiện thực các chứng chỉ 7.4.3 Thu hồi các chứng chỉ 7.4.4 Hiện thực các mô hình tin cậy **7.5 Đối phó với các tấn công mã hóa** **7.6 Các chuẩn và các giao thức mã hóa** 7.6.1 Các chuẩn mã hóa cổ điển 7.6.2 X.509 7.6.3 SSL và TLS 7.6.4 SSH 7.6.5 HTTPS **7.7 Quản trị khóa và chu kỳ thời gian của khóa** 7.7.1 So sánh khóa tập trung và khóa không tập trung 7.7.2 Lưu trữ và phân phối khóa 7.7.3 Sử dụng mô hình ký quỹ khóa 7.7.4 Hạn sử dụng khóa 7.7.5 Thu hồi khóa 7.7.6 Tạm hoãn khóa 7.7.7 Phục hồi và lưu giữ khóa 7.7.8 Cấp mới khóa 7.7.9 Hủy khóa				

2 LT	**CHƯƠNG 8: CÁC CHÍNH SÁCH VÀ THỦ TỤC BẢO MẬT** **8.1 Tính liên tục của kinh doanh** 8.1.1 Lợi ích 8.1.2 Tính sẵn có cao 8.1.3 Phục hồi sự cố **8.2 Củng cố hỗ trợ các nhà cung cấp** 8.2.1 Các bản thỏa thuận dịch vụ 8.2.2 Ký quỹ mã nguồn **8.3 Tạo các chính sách và thủ tục** 8.3.1 Chính sách nguồn nhân lực 8.3.2 Chính sách kinh doanh 8.3.3 Chính sách chứng chỉ 8.3.4 Chính sách đáp ứng rắc rối **8.4 Củng cố quản trị quyền** 8.4.1 Vai trò quản trị user và nhóm 8.4.2 Quyền tăng cường 8.4.3 Quyền ra quyết định	CLO1, CLO2	Trực tiếp (offline) hay trực truyến (online) Giảng viên: trình bày các nội dung của chương Sinh viên: lắng nghe, biết và hiểu nội dung bài	A1.1, A1.2, A1.3, A2.1	Bài giảng chương 8
2 LT	**CHƯƠNG 9: QUẢN TRỊ BẢO MẬT** **9.1 Các pháp lý về máy tính** 9.1.1 Phương pháp luận của điều tra pháp lý 9.1.2 Thi hành chuỗi liên đới 9.1.3 Bảo vệ chứng cứ 9.1.4 Thu thập chứng cứ	CLO1, CLO2	Trực tiếp (offline) hay trực truyến (online) Giảng viên: trình bày các nội dung của chương Sinh viên: lắng nghe, biết và hiểu nội dung bài	A1.1, A1.2, A1.3, A2.1	Bài giảng chương 9

	9.2 Quản trị bảo mật **9.3 Kiến thức và giáo dục bảo mật** 9.3.1 Sử dụng truyền thông và nâng cao nhận thức 9.3.2 Giáo dục 9.3.3 Điều lệ bí mật cá nhân và bảo mật				
Môn học được giảng dạy trực tuyến tối đa không quá 30% tổng thời lượng chương trình.					

TRƯỞNG BỘ MÔN	NGƯỜI BIÊN SOẠN
TS. Hà Bình Minh	ThS. Đặng Hoàng Huy
TRƯỞNG KHOA	**HIỆU TRƯỞNG**
ThS. Nguyễn Văn Thi	PHÓ HIỆU TRƯỞNG PGS.,TS. Nguyễn Đức Trung