TRƯỜNG ĐẠI HỌC NGUYỄN TẤT THÀNH
KHOA CÔNG NGHỆ THÔNG TIN

Bài giảng môn học: AN TOÀN THÔNG TIN

Chương 8:

QUẢN LÝ, CHÍNH SÁCH VÀ PHÁP LUẬT AN TOÀN THÔNG TIN

Số tín chỉ: 2
Số tiết: 30 tiết
(Lý Thuyết)

GV: ThS. **Nguyễn Thị Phong Dung**
Email : ntpdung@ntt.edu.vn

- **Khái quát về quản lý ATTT**
  - Tài sản (Asset) trong lĩnh vực ATTT là thông tin, thiết bị, hoặc các thành phần khác hỗ trợ các hoạt động có liên quan đến thông tin.
  - Tài sản ATTT có thể gồm:

❑ **Phần cứng** (máy chủ, các thiết bị mạng,…)

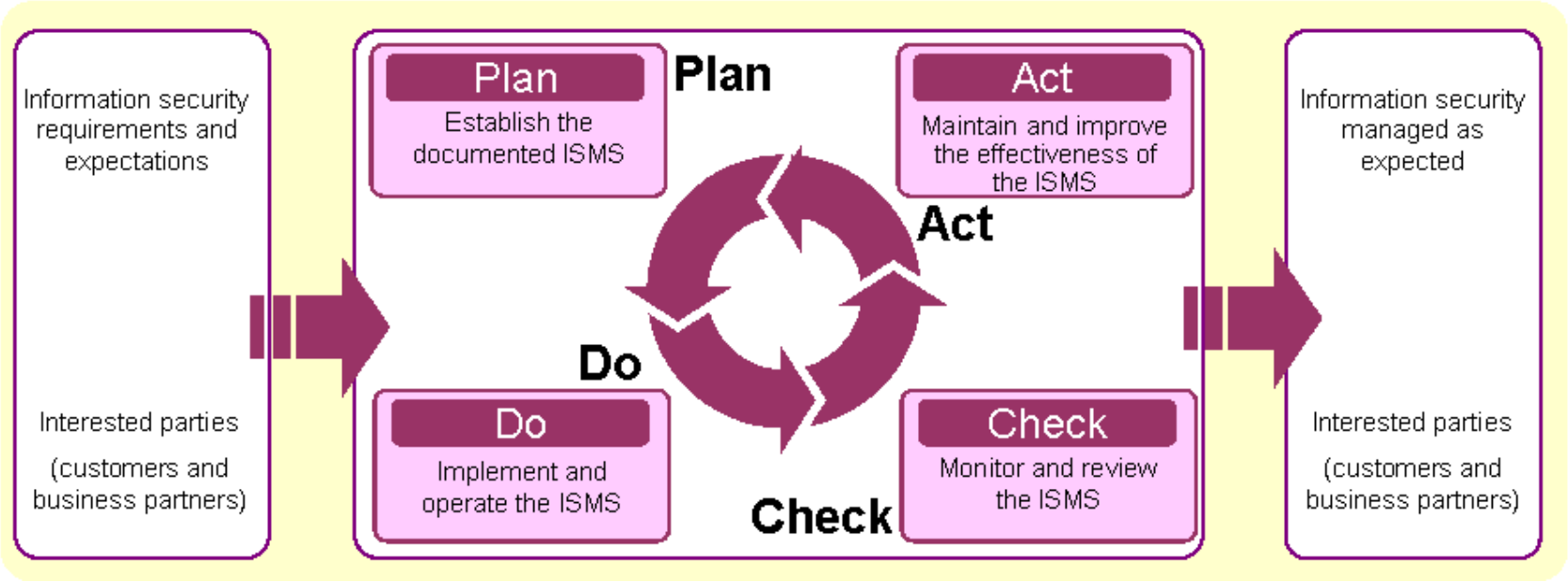
❑ **Phần mềm** (hệ điều hành, các phần mềm máy chủ dịch vụ,…)

❑ **Thông tin** (thông tin khách hàng, nhà cung cấp, hoạt động kinh doanh …)

- **Khái quát về quản lý ATTT**
  - Quản lý an toàn thông tin (Information security management) là một tiến trình (process) nhằm đảm bảo các tài sản quan trọng của cơ quan, tổ chức, doanh nghiệp được bảo vệ đầy đủ với chi phí phù hợp.
  - Quản lý ATTT phải trả lời được 3 câu hỏi:
    - *Những tài sản nào cần được bảo vệ?*
    - *Những đe dọa nào có thể có đối với các tài sản này?*
    - *Những biện pháp có thể thực hiện để ứng phó với các đe dọa đó?*

- ***Quá trình quản lý ATTT cần được thực hiện liên tục theo chu trình* do:**
  - **Sự thay đổi nhanh chóng của công nghệ:**
    - Nhiều công nghệ, kỹ thuật và công cụ mới xuất hiện
    - Độ phức tạp của hệ thống tăng nhanh.
  - **Môi trường xuất hiện rủi ro liên tục thay đổi:**
    - Xuất hiện nhiều công cụ cho tấn công, phá hoại
    - Xuất hiện nhiều mối đe dọa mới
    - Trình độ của tin tặc được nâng lên nhanh chóng.

- ***Chu trình Plan-Do-Check-Act (PDCA) thực hiện quản lý ATTT liên tục:***



❖ Đánh giá rủi ro ATTT (Security risk assessment)

- Là một bộ phận quan trọng của vấn đề quản lý rủi ro
- Mỗi tài sản của tổ chức cần được xem xét, nhận dạng các rủi ro có thể có và đánh giá mức rủi ro
- Là một trong các cơ sở để xác định mức rủi ro chấp nhận được với từng loại tài sản;
- Trên cơ sở xác định mức rủi ro, có thể đề ra các biện pháp xử lý, kiểm soát rủi ro trong mức chấp nhận được, với mức chi phí phù hợp.

- **Các phương pháp tiếp cận đánh giá rủi ro:**
  - Phương pháp đường cơ sở (Baseline approach)
  - Phương pháp không chính thức (Informal approach)
  - Phương pháp phân tích chi tiết rủi ro (Detailed risk analysis)
  - Phương pháp kết hợp (Combined approach)

❖ Phương pháp đường cơ sở (Baseline approach)

- **Mục đích của *Phương pháp đường cơ sở*** là thực thi các kiểm soát an ninh ở mức cơ bản dựa trên:
  - Các tài liệu cơ bản
  - Các quy tắc thực hành
  - Các thực tế tốt nhất của ngành đã được áp dụng
- **Ưu điểm:**
  - Không đòi hỏi các chi phí cho các tài nguyên bổ sung
  - Cùng nhóm các biện pháp có thể triển khai trên nhiều hệ thống.
- **Nhược điểm:**
  - Không xem xét kỹ đến các điều kiện nảy sinh các rủi ro
  - Mức quá cao: gây tốn kém, quá thấp: có thể gây mất an toàn.

Phù hợp với các tổ chức với hệ thống CNTT có quy mô nhỏ, nguồn lực hạn chế.

- **Phương pháp phân tích chi tiết rủi ro (Detailed risk analysis)**
  - Nhận dạng các tài sản
  - Nhận dạng các mối đe dọa và lỗ hổng đối với các tài sản này
  - Xác định xác suất xuất hiện các rủi ro và các hậu quả có thể có nếu rủi ro xảy ra.
  - Lựa chọn các biện pháp xử lý rủi ro dựa trên kết quả đánh giá rủi ro của các giai đoạn
  - **Ưu điểm:**
  - Cho phép xem xét chi tiết các rủi ro đối với hệ thống CNTT của tổ chức, và lý giải rõ ràng các chi phí cho các biện pháp kiểm soát rủi do đề xuất
  - Cung cấp thông tin tốt nhất cho việc tiếp tục quản lý vấn đề an ninh của các hệ thống CNTT khi chúng được nâng cấp, sửa đổi.
  - **Nhược điểm:**
  - Chi phí lớn về thời gian, các nguồn lực và yêu cầu kiến thức chuyên gia trình độ cao
  - Có thể dẫn đến chậm trễ trong việc đưa ra các biện pháp xử lý, kiểm soát rủi ro phù hợp
- ***Phù hợp các tổ chức có hệ thống CNTT quy mô lớn, hoặc các tổ chức cung cấp nền tảng hạ tầng truyền thông cho quốc gia,***

- **Phương pháp kết hợp (Combined approach)**
  - Cung cấp mức bảo vệ hợp lý càng nhanh càng tốt
  - Kiểm tra và điều chỉnh các biện pháp bảo vệ trên các hệ thống chính theo thời gian.
  - **Ưu điểm:**
  - Bắt đầu bằng việc đánh giá rủi ro ở mức cao dễ nhận được sự ủng hộ của cấp quản lý, thuận lợi cho việc lập kế hoạch quản lý ATTT
  - Giúp sớm triển khai các biện pháp xử lý và kiểm soát rủi ro ngay từ giai đoạn đầu
  - Có thể giúp giảm chi phí với đa số các tổ chức.
  - **Nhược điểm:**
  - Nếu đánh giá ở mức cao trong giai đoạn đầu không chính xác có thể dẫn đến áp dụng các biện pháp kiểm soát không phù hợp, hệ thống có thể gặp rủi ro trong thời gian chờ đánh giá chi tiết.
- ***Phù hợp các tổ chức với hệ thống CNTT quy mô vừa và lớn.***

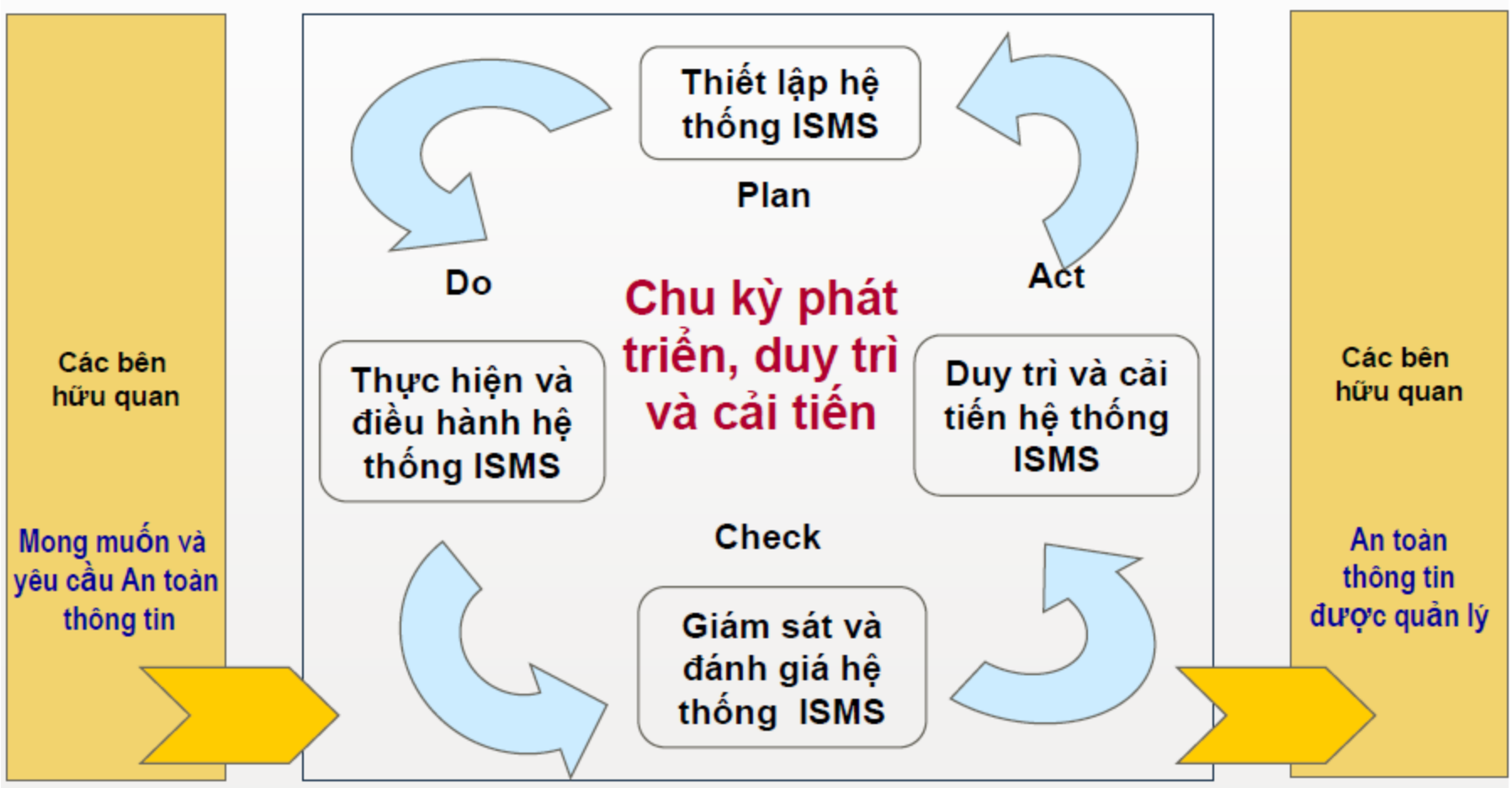
BỘ CHUẨN QUẢN LÝ ATTT ISO/IEC 27000

- **Bộ chuẩn ISO 27000** là bộ chuẩn về quản lý ATTT (*Information Technology - Code of Practice for Information Security Management*) được tham chiếu rộng rãi nhất
- **Bộ chuẩn ISO/IEC 17799** (được soạn thảo năm 2000 bởi International Organization for Standardization (ISO) và International Electrotechnical Commission (IEC)) là tiền thân của ISO 27000;
- **Năm 2005, ISO 17799** được chỉnh sửa và trở thành **ISO 17799:2005**
- **Năm 2007, ISO 17799:2005** được đổi tên thành **ISO 27002** song hành với **ISO 27001**

❖ Bộ chuẩn ISO/IEC 27000 - ISO/IEC 27001

- **ISO 27001** cung cấp các thông tin để:
  - Thực thi các yêu cầu của ISO/IEC 27002
  - Cài đặt một hệ thống quản lý an toàn thông tin (information security management system - ISMS).
- **ISO/IEC 27001:2005**: chuyên về hệ thống quản lý an toàn thông tin (Information Security Management System):
  - Cung cấp các chi tiết cho thực hiện chu kỳ Lập kế hoạch – Thực hiện – Kiểm tra – Hành động (**Plan-Do-Check-Act**)
- ISO 27001 cung cấp các thông tin để thực hiện việc quản lý ATTT, nhưng:
  - Nó chỉ tập trung vào các phần việc phải thực hiện
  - Không chỉ rõ cách thức thực hiện

❖ Bộ chuẩn ISO/IEC 27000 - ISO/IEC 27001



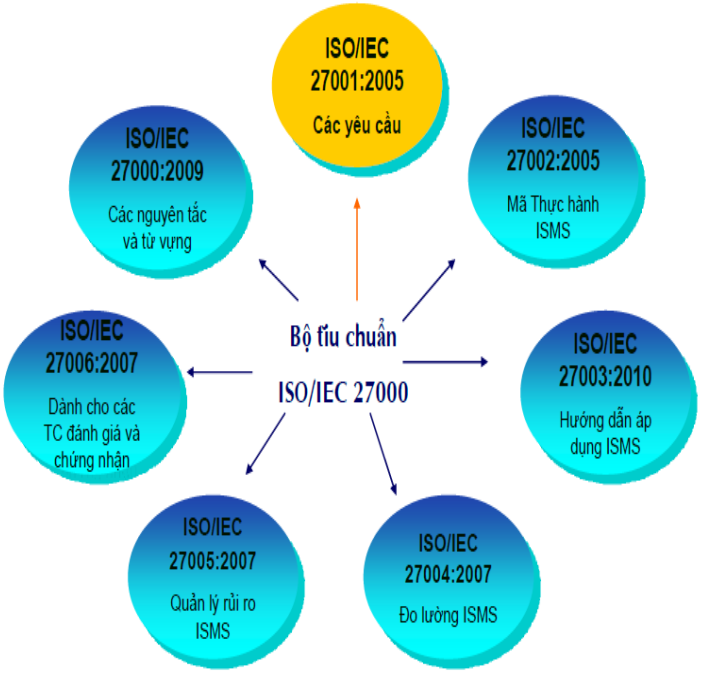
- **ISO/IEC 27001:2005: Plan-Do-Check-Act => Plan**
  - Đề ra phạm vi của ISMS
  - Đề ra chính sách của ISMS
  - Đề ra hướng tiếp cận đánh giá rủi ro
  - Nhận dạng các rủi ro
  - Đánh giá rủi ro
  - Nhận dạng và đánh giá các lựa chọn phương pháp xử lý rủi ro
  - Lựa chọn các mục tiêu kiểm soát và biện pháp kiểm soát
  - Chuẩn bị tuyên bố/báo cáo áp dụng

- **ISO/IEC 27001:2005: Plan-Do-Check-Act => Do**
  - Xây dựng kế hoạch xử lý rủi ro
  - Thực thi kế hoạch xử lý rủi ro
  - Thực thi các kiểm soát
  - Thực thi các chương trình đào tạo chuyên môn và giáo dục ý thức
  - Quản lý các hoạt động
  - Quản lý các tài nguyên
  - Thực thi các thủ tục phát hiện và phản ứng lại các sự cố an ninh

- **ISO/IEC 27001:2005: Plan-Do-Check-Act => Check**
  - Thực thi các thủ tục giám sát
  - Thực thi việc đánh giá thường xuyên tính hiệu quả của ISMS;
  - Thực hiện việc kiểm toán (audit) nội bộ với ISMS;
  - Thực thi việc đánh giá thường xuyên với ISMS bởi bộ phận quản lý
  - Ghi lại các hành động và sự kiện ảnh hưởng đến ISMS

- **ISO/IEC 27001:2005: Plan-Do-Check-Act => Act**
  - Thực hiện các cải tiến đã được nhận dạng
  - Thực hiện các hành động sửa chữa và ngăn chặn
  - Áp dụng các bài đã được học
  - Thảo luận kết quả với các bên quan tâm
  - Đảm bảo các cải tiến đạt được các mục tiêu.

❖ Danh sách các chuẩn con



ISO 27000 Series Standard	Pub Date	Title or Topic	Comment
27000	2009	Series Overview and Terminology	Defines terminology and vocabulary for the standard series
27001	2005	Information Security Management System Specification	Drawn from BS 7799:2
27002	2007	Code of Practice for Information Security Management	Renamed from ISO/IEC 17799; drawn from BS 7799:1
27004	2009	Information Security Measurements and Metrics	
27005	2008	ISMS Risk Management	Supports 27001, but doesn't recommend any specific risk method
27006	2007	Requirements for Bodies Providing Audit and Certification of an ISMS	Largely intended to support the accreditation of certification bodies providing ISMS certification

❖ Giới thiệu pháp luật và chính sách ATTT

- **Các chính sách và pháp luật có vai trò rất quan trọng trong việc đảm bảo an toàn cho thông tin, hệ thống và mạng:**
  - Trong đó vai trò của nhân viên đảm bảo an toàn cho thông tin là rất quan trọng trong việc giảm thiểu rủi ro, đảm bảo an toàn cho thông tin, hệ thống và mạng và giảm thiệt hại nếu xảy ra sự cố
  - Các nhân viên đảm bảo an toàn cho thông tin phải hiểu rõ những khía cạnh pháp lý và đạo đức ATTT
    - Luôn nắm vững môi trường pháp lý hiện tại và các luật và các quy định luật pháp
    - Luôn thực hiện công việc nằm trong khuôn khổ cho phép của luật pháp.
  - Thực hiện việc giáo dục ý thức về luật pháp và đạo đức ATTT cho cán bộ quản lý và nhân viên trong tổ chức, đảm bảo sử dụng đúng mục đích các công nghệ đảm bảo ATTT

❖ Giới thiệu pháp luật và chính sách ATTT

- **Trách nhiệm của tổ chức (Organization Liaibility):**
- Trách nhiệm của một tổ chức là trách nhiệm trước luật pháp của tổ chức đó được mở rộng ngoài phạm vi luật hình sự và luật hợp đồng
- Gồm cả trách nhiệm pháp lý phải hoàn trả và đền bù cho những hành vi sai trái
- Nếu một nhân viên của 1 công ty/tổ chức thực hiện hành vi phạm pháp hoặc phi đạo đức, gây thiệt hại cho cá nhân, tổ chức khác, thì công ty/tổ chức đó phải chịu trách nhiệm về pháp lý, tài chính
- Ví dụ: Bảo vệ của 1 siêu thị giam giữ hoặc hành hung khách hàng gây thương tích
  - NV bảo vệ có thể bị bắt tạm giam để điều tra
  - Siêu thị phải có trách nhiệm đền bù cho khách hàng.

❖ Giới thiệu pháp luật và chính sách ATTT

▸ Chính sách (Policy) và Luật (Law):

- Trong một tổ chức, nhân viên ATTT có trách nhiệm duy trì an toàn thông qua việc thiết lập và các chính sách ATTT;
- Chính sách (còn gọi là quy định, nội quy) là các quy định về các hành vi chấp nhận được của các nhân viên trong tổ chức tại nơi làm việc;
- Chính sách là các "luật" của tổ chức có giá trị thực thi trong nội bộ, gồm một tập các quy định và các chế tài xử phạt bắt buộc phải thực hiện;
- Các chính sách/nội quy cần được nghiên cứu, soạn thảo kỹ lưỡng;
- Chính sách cần đầy đủ, đúng đắn và áp dụng công bằng với mọi nhân viên;
- Khác biệt giữa chính sách và luật:
  - Luật luôn bắt buộc
  - Chính sách: thiếu hiểu biết chính sách là 1 cách bào chữa chấp nhận được

❖ Giới thiệu pháp luật và chính sách ATTT

▸ Các yêu cầu của chính sách

- ***Phổ biến (Dissemination):*** có khả năng phổ biến rộng rãi, bằng tài liệu giấy hoặc điện tử
- ***Xem xét (Review):*** Nhân viên có thể xem, hiểu được – cần thực hiện trên nhiều ngôn ngữ, ví dụ bằng tiếng Anh và tiếng địa phương
- ***Có thể hiểu (Comprehension):*** Chính sách cần rõ ràng dễ hiểu – tổ chức cần có các điều tra/khảo sát về mức độ hiểu biết/nắm bắt các chính sách của nhân viên
- ***Tuân thủ (Obligation):*** Cần có biện pháp để nhân viên cam kết thực hiện – thông qua ký văn bản cam kết hoặc tick vào ô xác nhận tuân thủ
- ***Áp dụng đồng đều, bình đẳng (Uniform enforcement):*** Chính sách cần được thực hiện đồng đều, bình đẳng, nhất quán, không có ưu tiên với bất kỳ nhân viên nào, kể cả người quản lý.

❖ Luật quốc tế về ATTT

- **Các luật ATTT của Mỹ**
  - Các luật tội phạm máy tính
  - Các luật về sự riêng tư
  - Luật xuất khẩu và chống gián điệp
  - Luật bản quyền
  - Luật tự do thông tin
- **Các luật ATTT và tổ chức luật quốc tế:**
  - Hội đồng châu Âu về chống tội phạm mạng
  - Hiệp ước bảo vệ quyền sở hữu trí tuệ.

❖ Luật Việt Nam về ATTT

- **Luật An ninh mạng của Việt Nam được Quốc hội thông qua vào tháng 6 năm 2018 và có hiệu lực từ 1/1/2019:**
  - Quy định đầy đủ các biện pháp phòng ngừa, đấu tranh, xử lý nhằm loại bỏ các nguy cơ đe dọa, phát hiện và xử lý hành vi vi phạm pháp luật trên không gian mạng.
- **Một số văn bản khác có liên quan đến ATTT**
  - Luật CNTT số 67/2006/QH11 của Quốc hội, ngày 12/07/2006
  - Nghị định số 90/2008/NĐ-CP của Chính Phủ "Về chống thư rác", ngày 13/08/2008.
  - Quyết định số 59/2008/QĐ-BTTTT của Bộ Thông tin và Truyền thông "Ban hành Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số", ngày 31/12/2008.
  - Quyết định 63/QĐ-TTg của Thủ tướng CP "Phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020", ngày 13/01/2010.
  - Chỉ thị số 897/CT-TTg của Thủ tướng CP "V/v tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số", 10/06/2011.

❖ Luật Việt Nam về ATTT

Một số văn bản khác có liên quan đến ATTT

- Thông tư số 23/2011/TT-BTTTT của Bộ TT&TT "Quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước", ngày 11/08/2011.
- Nghị định số 77/2012/NĐ-CP của Chính Phủ "Sửa đổi, bổ sung một số điều của Nghị định số 90/2008/NĐ-CP ngày 13 tháng 8 năm 2008 của Chính phủ về chống thư rác", ngày 05/10/2012.
- Nghị định 72/2013/NĐ-CP của Chính Phủ về Quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng; quy định về việc chia sẻ thông tin trên các trang mạng xã hội.
- Dự thảo Luật An ninh mạng được được đưa ra lấy ý kiến Quốc hội và các chuyên gia trong năm 2017. Dự kiến thông qua trong năm 2018.

VẤN ĐỀ ĐẠO ĐỨC ATTT

- **Nhiều tổ chức xã hội nghề nghiệp đã ban hành các quy tắc ứng xử (Code of Conduct) bắt buộc tại nơi làm việc:**
  - Luật sư, bác sỹ nếu vi phạm nghiêm trọng các quy tắc ứng xử có thể bị cấm hành nghề.
  - Các vận động viên thể thao vi phạm bộ quy tắc ứng xử có thể bị cấm thi đấu có thời hạn hoặc vĩnh viễn
- **CNTT và ATTT không có bộ quy tắc ứng xử bắt buộc**
  - Một số tổ chức nghề nghiệp như ACM (Association for Computing Machinery) và ISSA (Information Systems Security Association) hợp tác để đề ra các quy tắc ứng xử trong ATTT
  - Tuy nhiên, các quy tắc ứng xử trong ATTT chỉ có tính khuyến nghị mà các tổ chức trên không có thẩm quyền buộc phải thực hiện
  - Hiệp hội ATTT Việt Nam đã công bố Bộ Qui tắc ứng xử ATTT vào đầu năm 2015, đưa ra một số quy tắc và khuyến nghị về những việc không được làm cho các thành viên và các nhân viên của các tổ chức hoạt động trong lĩnh vực ATTT

VẤN ĐỀ ĐẠO ĐỨC ATTT

- **Bộ Quy tắc ứng xử 10 điểm (Ten Commandments of Computer Ethics) đề xuất bởi Viện đạo đức máy tính (Mỹ):**

1. Không được sử dụng máy tính để gây hại cho người khác
2. Không được can thiệp vào công việc của người khác trên máy tính
3. Không trộm cắp các files trên máy tính của người khác
4. Không được sử dụng máy tính để trộm cắp
5. Không được sử dụng máy tính để tạo bằng chứng giả
6. Không sao chép hoặc sử dụng phần mềm không có bản quyền
7. Không sử dụng các tài nguyên máy tính của người khác khi không được phép hoặc không có bồi thường thỏa đáng
8. Không chiếm đoạn tài sản trí tuệ của người khác
9. Nên suy nghĩ về các hậu quả xã hội của chương trình mình đang xây dựng hoặc hệ thống đang thiết kế
10. Nên sử dụng máy tính một cách có trách nhiệm, đảm bảo sự quan tâm và tôn trọng đến đồng bào của mình

VẤN ĐỀ ĐẠO ĐỨC ATTT

- **Sự khác biệt về vấn đề đạo đức giữa các nền văn hóa:**
  - Nhận thức về vấn đề đạo đức trong sử dụng các tài nguyên của cơ quan, tổ chức là rất khác biệt giữa các quốc gia có nền văn hóa khác nhau
  - Trong nhiều trong hợp, hành vi được phép của một số cá nhân trong một quốc gia lại vi phạm quy tắc đạo đức của quốc gia khác;
    - VD: Vấn đề vi phạm bản quyền phần mềm ở các nước tiên tiến như Mỹ và châu Âu ở mức tương đối thấp, nhưng ở mức rất cao ở các nước châu Á và châu Phi.
    - Tỷ lệ vi phạm bản quyền phần mềm ở Việt Nam khoảng 90%
- **Vấn đề vi phạm bản quyền phần mềm:**
  - Vấn đề vi phạm bản quyền phần mềm ở mức rất nghiêm trọng, đặc biệt là tại các nước đang phát triển ở châu Á và châu Phi

VẤN ĐỀ ĐẠO ĐỨC ATTT

- **Vấn đề lạm dụng các tài nguyên của công ty, tổ chức:**
  - Một số công ty/tổ chức chưa có các quy định cấm nhân viên sử dụng các tài nguyên của công ty, tổ chức vào việc riêng. Một số có quy định nhưng chưa được thực thi chặt chẽ và chưa có chế tài xử phạt nghiêm minh
  - ***Các hành vi lạm dụng thường gặp***
  - In ấn tài liệu riêng
  - Sử dụng email cá nhân cho việc riêng
  - Tải các tài liệu/files không được phép
  - Cài đặt và chạy các chương trình/phần mềm không được phép
  - Sử dụng máy tính công ty làm việc riêng
  - Sử dụng các loại phương tiện làm việc khác như điện thoại công ty quá mức vào việc riêng

Cám ơn !