CHƯƠNG 5

XÂY DỰNG CHÍNH SÁCH AN TOÀN BẢO MẬT THÔNG TIN TRONG DOANH NGHIỆP

TS. Hoàng Thị Thanh Hà
Khoa Thống kê – Tin học
Trường Đại học Kinh Tế - Đại học Đà Nẵng

NỘI DUNG

1. Quản lý an toàn thông tin
2. Giới thiệu bộ chuẩn quản lý ATTT ISO/IEC 27000
3. Pháp luật và chính sách ATTT
4. Vấn đề đạo đức ATTT
5. Mô hình đảm bảo ATTT

1. Quản lý an toàn thông tin

1. Khái quát về quản lý ATTT

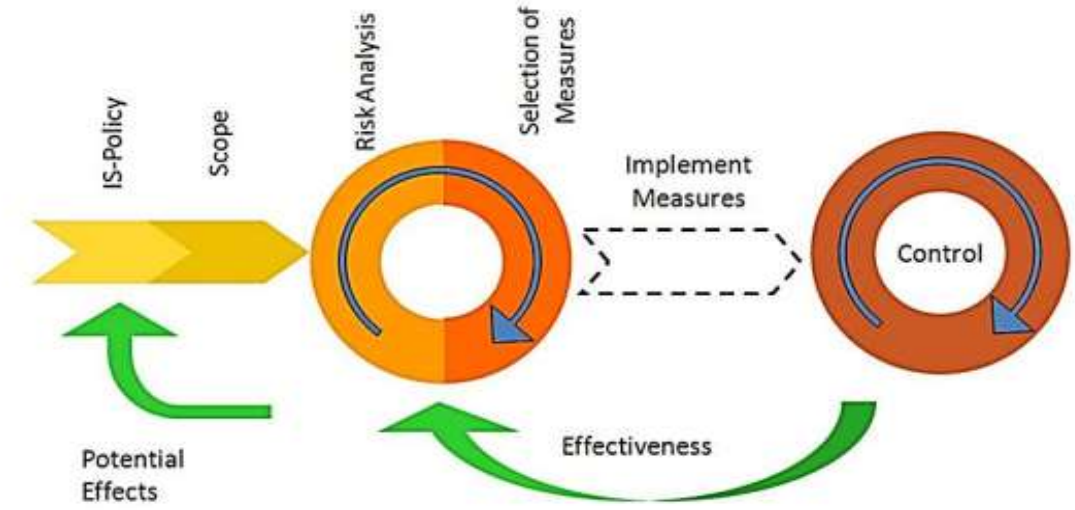
- Tài sản (Asset) trong lĩnh vực ATTT là thông tin, thiết bị, hoặc các thành phần khác hỗ trợ các hoạt động có liên quan đến thông tin.
- Tài sản ATTT có thể gồm:
  - Phần cứng (máy chủ, các thiết bị mạng,…)
  - Phần mềm (hệ điều hành, các phần mềm máy chủ dịch vụ,…)
  - Dữ liệu (khách hàng, nhà cung cấp, hoạt động kinh doanh,…)

- Quản lý an toàn thông tin 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;

1. Quản lý an toàn thông tin

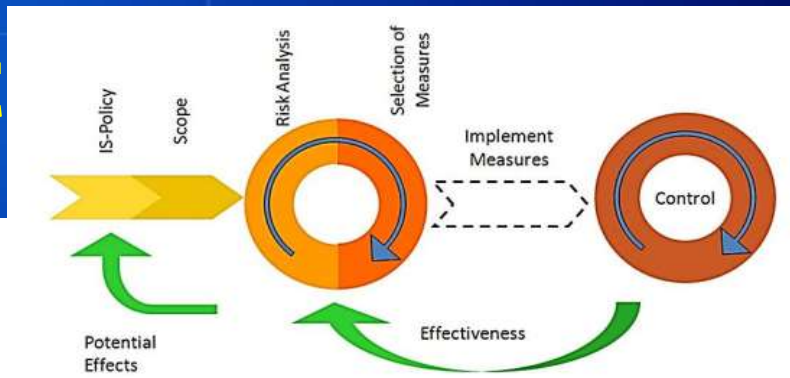
1. Khái quát về quản lý ATTT

- 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?



Quan hệ giữa các khâu trong quản lý an toàn thông tin theo tiêu chuẩn
Tiêu chuẩn ISO 27001 *(con người, quy trình và hệ thống CNTT bằng cách áp dụng quy trình quản lý rủi ro)*

1. Quản lý an toàn t



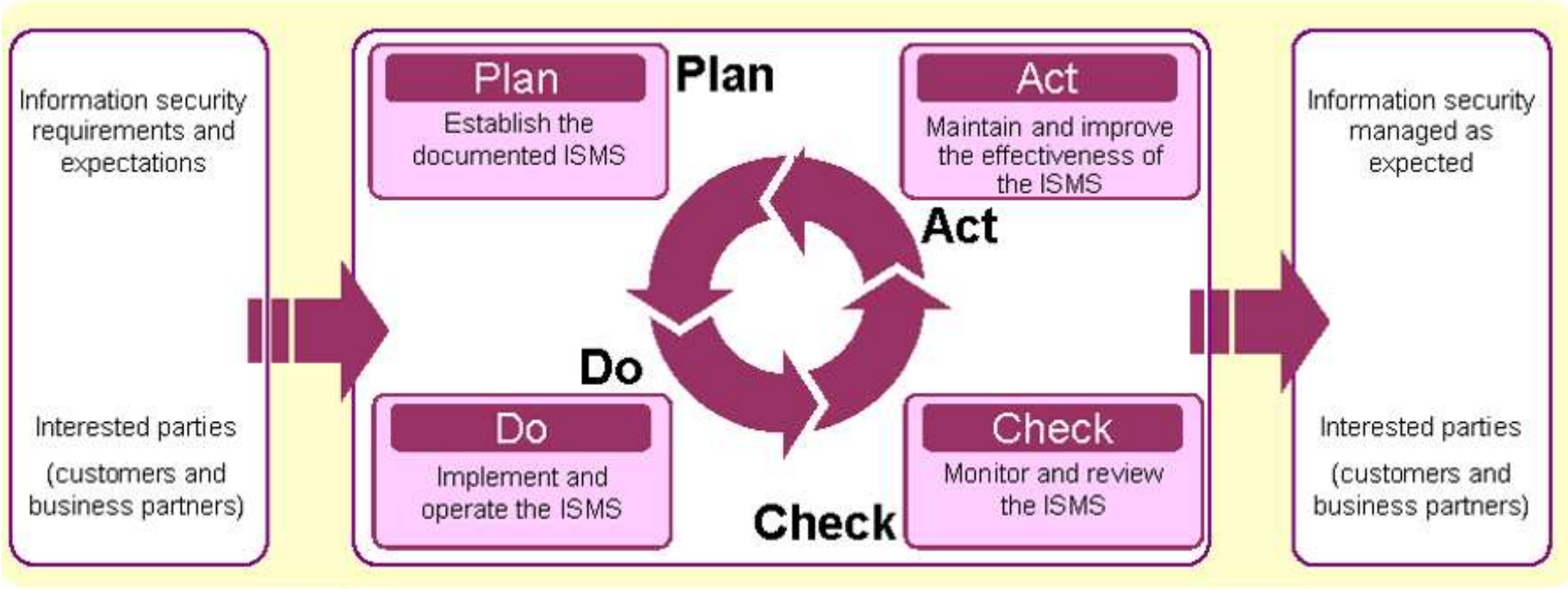
1. Khái quát về quản lý ATTT

- Quản lý ATTT có thể gồm các khâu.
  1. **Xác định** rõ **mục đích** đảm bảo ATTT và xây dựng hồ sơ tổng hợp về các rủi ro;
  2. **Đánh giá rủi ro** với từng tài sản ATTT cần bảo vệ;
  3. **Xác định và triển khai các biện pháp** quản lý, kỹ thuật kiểm soát, giảm rủi ro về mức chấp nhận được.
- Quá trình quản lý ATTT cần được thực hiện **liên tục** theo chu trình (vòng đời) 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.

1. Quản lý an toàn thông tin

1. Khái quát về quản lý ATTT

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



1. Quản lý an toàn thông tin

2. Đánh giá rủi ro an toàn thông tin (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.

1. Quản lý an toàn thông tin

2. Đánh giá rủi ro an toàn thông tin

❑ 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)

1. Quản lý an toàn thông tin

2. Đánh giá rủi ro an toàn thông tin

❑ Các phương pháp tiếp cận đánh giá rủi ro

- 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.

1. Quản lý an toàn thông tin

2. Đánh giá rủi ro an toàn thông tin

❑ Các phương pháp tiếp cận đánh giá rủi ro

- ➢ Phương pháp đường cơ sở (Baseline approach)
  - Ưu điểm:
    - ✓ Không đòi hỏi các chi phí cho các tài nguyên bổ sung sử dụng trong đánh giá rủi ro chính thức;
    - ✓ 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 ở các hệ thống của các tổ chức khác nhau;
    - ✓ Mức đường cơ sở được xác định chung nên có thể không phù hợp với từng tổ chức cụ thể. 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.

6.1 Quản lý an toàn thông tin

2. Đánh giá rủi ro an toàn thông tin

❑ Phương pháp không chính thức (Informal approach)

Phương pháp không chính thức liên quan đến việc:

- Thực hiện một số dạng phân tích rủi ro hệ thống CNTT của tổ chức một cách không chính thức;
- Sử dụng kiến thức chuyên gia của các nhân viên bên trong tổ chức, hoặc các nhà tư vấn từ bên ngoài;
- Không thực hiện đánh giá toàn diện các rủi ro đối với tất cả các tài sản CNTT của tổ chức.

6.1 Quản lý an toàn thông tin

2. Đánh giá rủi ro an toàn thông tin

❑ Phương pháp không chính thức

- ❖ Ưu điểm:
  - Không đòi hỏi các nhân viên phân tích rủi ro có các kỹ năng bổ sung, nên có thể thực hiện nhanh với chi phí thấp;
  - Việc có phân tích hệ thống CNTT của tổ chức giúp cho việc đánh giá rủi ro, lỗ hổng chính xác hơn và các biện pháp kiểm soát đưa ra cũng phù hợp hơn phương pháp đường cơ sở.
- ❖ Nhược điểm:
  - Do đánh giá rủi ro không được thực hiện toàn diện nên có thể một rủi ro không được xem xét kỹ, nên có thể để lại nguy cơ cao cho tổ chức;
  - Kết quả đánh giá dễ phục thuộc vào quan điểm của các cá nhân.
- ❖ Phù hợp với các tổ chức với hệ thống CNTT có quy mô nhỏ và vừa, nguồn lực tương đối hạn chế

1. Quản lý an toàn thông tin

2. Đánh giá rủi ro an toàn thông tin

❑ Phương pháp phân tích chi tiết rủi ro (Detailed risk analysis)

❖ Là PP đánh giá toàn diện, được thực hiện một cách chính thức và được chia thành nhiều giai đoạn:

1. Nhận dạng các **tài sản**;
2. Nhận dạng các **mối đe dọa** và **lỗ hổng** đối với các tài sản này;
3. Xác định **xác suất xuất hiện các rủi ro** và các hậu quả có thể có nếu rủi ro xảy ra với tổ chức;
4. Lựa chọn **các biện pháp xử lý rủi ro** dựa trên kết quả đánh giá rủi ro của các giai đoạn trên.

1. Quản lý an toàn thông tin

2. Đánh giá rủi ro an toàn thông tin

❑ Phương pháp phân tích chi tiết rủi ro

❖ 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.

1. Quản lý an toàn thông tin

2. Đánh giá rủi ro an toàn thông tin

❑ Phương pháp phân tích chi tiết rủi ro

❖ Phù hợp với:

- ➢ Các tổ chức chính phủ cung cấp các dịch vụ thiết yếu cho người dân và doanh nghiệp;
- ➢ 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;
  - ✓ Các tổ chức tài chính, ngân hàng;
  - ✓ Các doanh nghiệp viễn thông, nhà mạng;
  - ✓ Các công ty, tập đoàn có hệ thống CNTT đủ lớn.

1. Quản lý an toàn thông tin

2. Đánh giá rủi ro an toàn thông tin

❑ Phương pháp kết hợp

- Kết hợp các thành phần của 3 PP đường cơ sở, không chính thức và phân tích chi tiết;
- Mục tiêu:
  - Cung cấp mức bảo vệ hợp lý càng nhanh càng tốt;
  - Sau đó kiểm tra và điều chỉnh các biện pháp bảo vệ trên các hệ thống chính theo thời gian.

6.1 Quản lý an toàn thông tin

2. Đánh giá rủi ro an toàn thông tin

❑ Phương pháp kết hợp

❖ Các bước thực hiện:

1. Thực hiện PP đường cơ sở với tất cả các thành phần của hệ thống CNTT của tổ chức;
2. Tiếp theo, các thành phần có mức **rủi ro cao, hoặc trọng yếu** được xem xét đánh giá theo PP không chính thức;
3. Cuối cùng hệ thống được xem xét đánh giá toàn diện rủi ro ở mức chi tiết.

1. Quản lý an toàn thông tin

2. Đánh giá rủi ro an toàn thông tin

❑ Phương pháp kết hợp

❖ Ưu điểm:

- Việc 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 ko phù hợp, HT có thể gặp rủi ro trong thời gian chờ đánh giá chi tiết.

❖ Phù hợp các tổ chức với HTTT quy mô vừa và lớn.

2. 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; (Việt Nam chấp thuận nguyên vẹn một số chuẩn)
- 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.

2. Bộ chuẩn quản lý ATTT ISO/IEC 27000

- ISO/IEC 27002 gồm 127 điều, cung cấp cái nhìn tổng quan về nhiều lĩnh vực trong ATTT;
- ISO/IEC 27002 đề ra các khuyến nghị về quản lý ATTT cho những người thực hiện việc khởi tạo, thực hiện và duy trì an ninh an toàn trong tổ chức của họ;
- ISO/IEC 27002 được thiết kế cung cấp nền tảng cơ sở giúp đề ra các chuẩn ATTT cho tổ chức và các thực tế quản lý ATTT một cách hiệu quả.

2. Bộ chuẩn quản lý ATTT ISO/IEC 27000

❑ 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, và
- 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)

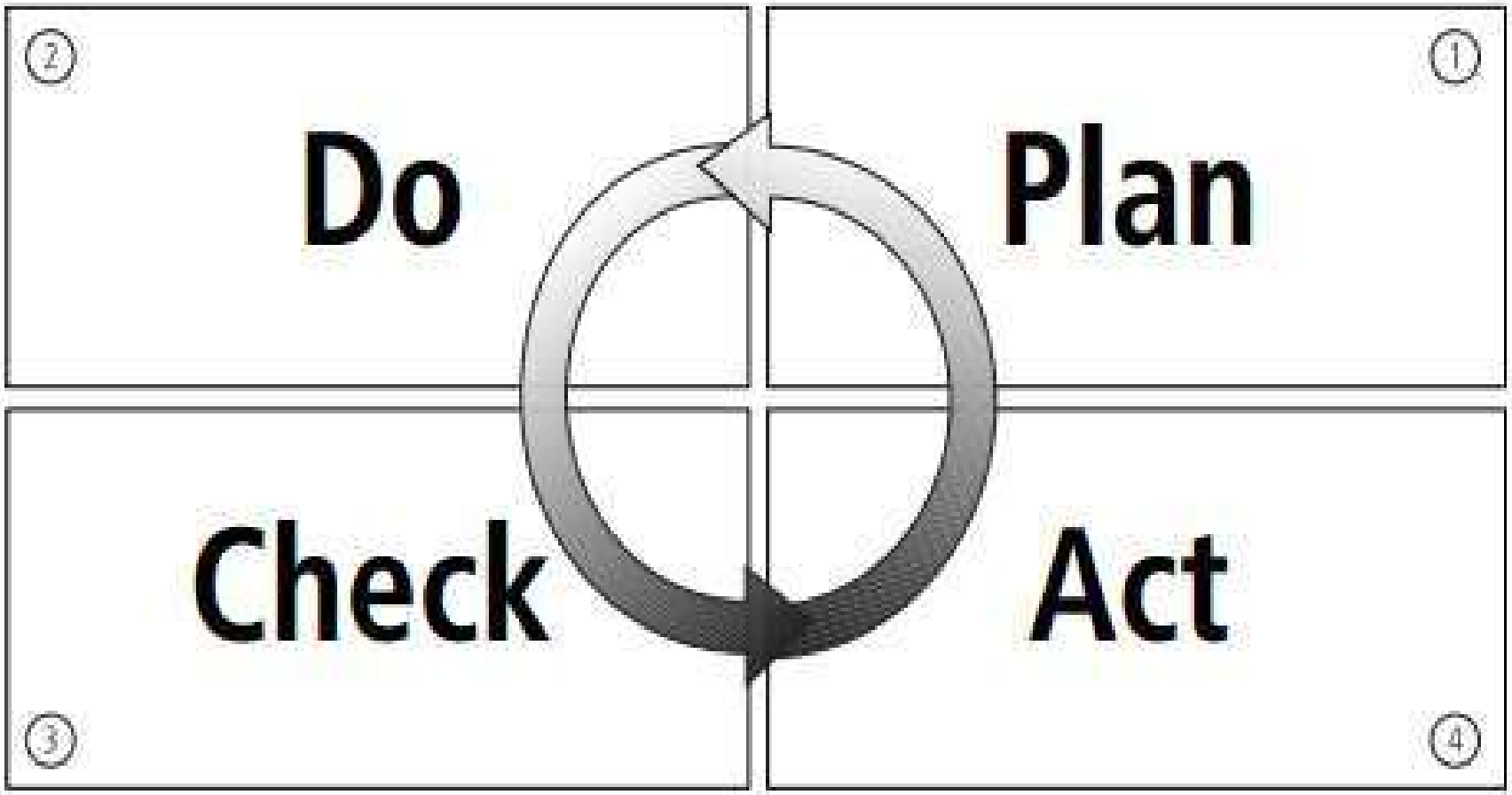
❖ISO 27001 cung cấp các thông tin để thực hiện việc quản lý ATTT, nhưng:

- Nó chỉ tập trung vào các phần việc phải thực hiện;
- Không chỉ rõ cách thức thực hiện.

2. Bộ chuẩn quản lý ATTT ISO/IEC 27000

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

❖ISO/IEC 27001:2005: Plan-Do-Check-Act



2. Bộ chuẩn quản lý ATTT ISO/IEC 27000

❑ 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 tuyến bố/báo cáo áp dụng.

2. Bộ chuẩn quản lý ATTT ISO/IEC 27000

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

❖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.

2. Bộ chuẩn quản lý ATTT ISO/IEC 27000

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

❖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;

2. Bộ chuẩn quản lý ATTT ISO/IEC 27000

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

❖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.

3 Pháp luật và chính sách ATTT

1. Giới thiệu về pháp luật và chính sách an toàn thông tin
2. Luật quốc tế về an toàn thông tin
3. Luật Việt Nam về an toàn thông tin

3 Pháp luật và chính sách ATTT

❑ Giới thiệu về 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 ATTT 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.

3 Pháp luật và chính sách ATTT

❑ Giới thiệu về pháp luật và chính sách ATTT

❖ Phân biệt Luật (Law) và Đạo đức (Ethics):

- Luật: Gồm những điều khoản bắt buộc hoặc cấm những hành vi cụ thể;
  - Các điều luật thường được xây dựng từ các vấn đề đạo đức.
- Đạo đức: Định nghĩa những hành vi xã hội chấp nhận được;
  - Đạo đức thường dựa trên các đặc điểm văn hóa. Do đó hành vi đạo đức giữa các dân tộc, các nhóm người khác nhau là khác nhau;
  - Một số hành vi vi phạm đạo được được luật hóa trên toàn thế giới: trộm, cướp, cưỡng dâm, bạo hành trẻ em,...
- Khác biệt giữa luật và đạo đức:
  - Luật được thực thi bởi các cơ quan chính quyền;
  - Đạo đức không được thực thi bởi các cơ quan chính quyền.

3 Pháp luật và chính sách ATTT

❑ Giới thiệu về pháp luật và chính sách ATTT

❖ Trách nhiệm của tổ chức (Organization Liaibility):

- 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 .

3 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.

3 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.

3 Pháp luật và chính sách ATTT

- Các kiểu luật:
  - Luật dân sự (Civil Law): là luật điều chỉnh các quan hệ dân sự giữa các tổ chức và cá nhân trong một quốc gia;
  - Luật hình sự (Criminal Law): là luật điều chỉnh các hành vi gây hại cho xã hội và nhà nước chủ động thực thi;
  - Luật công cộng (Public Law): quy định cấu trúc của các đơn vị hành chính (quốc hội, chính phủ và các đơn vị trực thuộc), các quan hệ giữa công dân với công dân, giữa các tổ chức và quan hệ với các chính phủ các nước khác;
    - VD: Hiến pháp, luật hành chính.
  - Luật riêng (Private Law): điều chỉnh các quan hệ trong phạm vi hẹp, như quan hệ gia đình, thương mại, lao động và quan hệ giữa các cá nhận với các tổ chức

3 Pháp luật và chính sách ATTT

❑ 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.

3 Pháp luật và chính sách ATTT

❑ Luật quốc tế về ATTT – Luật Mỹ

❖ Các luật về tội phạm máy tính:

- Computer Fraud and Abuse Act of 1986 (CFA Act) – quy định về các tội phạm lừa đảo và lạm dụng máy tính;
- Computer Security Act, 1987: đề ra các nguyên tắc đảm bảo an toàn cho HT máy tính;
- National Information Infrastructure Protection Act of 1996 là bản sửa đổi của CFA Act, tăng khung hình phạt một số tội phạm máy tính đến 20 năm tù;
- USA PATRIOT Act, 2001: cho phép các cơ quan chính quyền một số quyền nhằm phòng chống khủng bố hiệu quả hơn;
- USA PATRIOT Improvement and Reauthorization Act: Mở rộng của USA PATRIOT Act, 2001, cấp cho các cơ quan chính quyền nhiều quyền hạn hơn cho nhiệm vụ phòng chống khủng bố.

3 Pháp luật và chính sách ATTT

❑ Luật quốc tế về ATTT – Luật Mỹ

❖ Các luật về sự riêng tư: bảo vệ quyền riêng tư của người dùng, bảo vệ các thông tin cá nhân của người dùng:

- Federal Privacy Act, 1974: luật Liên bang Mỹ bảo vệ quyền riêng tư của người dùng;
- Electronic Communications Privacy Act , 1986: luật bảo vệ quyền riêng tư trong các giao tiếp điện tử;
- Health Insurance Portability and Accountability Act, 1996 (HIPAA): bảo vệ tính bí mật và an toàn của các dữ liệu y tế của người bệnh;
  - Tổ chức/cá nhân vi phạm có thể bị phạt đến 250.000 USD hoặc 10 năm tù;
- Financial Services Modernization Act or Gramm-Leach-Bliley Act, 1999: điều chỉnh các hoạt động liên quan đến ATTT của các ngân hàng, bảo hiểm và các hãng an ninh.

3 Pháp luật và chính sách ATTT

❑ Luật quốc tế về ATTT – Luật Mỹ

❖ Luật xuất khẩu và chống gián điệp: hạn chế việc xuất khẩu các công nghệ và hệ thống xử lý thông tin và phòng chống gián điệp kinh tế;

- Economic Espionage Act, 1996: phòng chống việc thực hiện giao dịch có liên quan đến bí mật kinh tế và công nghệ;
- Security and Freedom through Encryption Act, 1999: quy định về các vấn đề có liên quan đến sử dụng mã hóa trong đảm bảo an toàn và tự do thông tin.

3 Pháp luật và chính sách ATTT

❑ Luật quốc tế về ATTT – Luật Quốc tế

❖ Các luật ATTT và tổ chức luật quốc tế:

- Hội đồng châu Âu về chống tội phạm mạng (Council of Europe Convention on Cybercrime): Hiệp ước về chống tội phạm mạng được Hội đồng châu Âu phê chuẩn vào năm 2001;
- Hiệp ước bảo vệ quyền sở hữu trí tuệ (Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)): do Tổ chức Thương mại thế giới WTO chủ trì đàm phán trong giai đoạn 1986–1994;
- Digital Millennium Copyright Act (DMCA): luật bản quyền số Thiên niên kỷ.

3 Pháp luật và chính sách ATTT

❑ Luật Việt Nam về ATTT

- ❖ Luật ATTT mạng của Việt Nam được thông qua vào 11.2015 (86/2015/QH13) và có hiệu lực từ 1/7/2016: Đây là cơ sở pháp lý quan trọng nhất cho các hoạt động có liên quan đến ATTT.
- ❖ Luật ATTT mạng gồm 8 chương với 54 điều:
  - Chương I: NHỮNG QUY ĐỊNH CHUNG
  - Chương II: BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG
  - Chương III: MẬT MÃ DÂN SỰ
  - Chương IV: TIÊU CHUẨN, QUY CHUẨN KỸ THUẬT ATTT MẠNG
  - Chương V: KINH DOANH TRONG LĨNH VỰC ATTT MẠNG
  - Chương VI: PHÁT TRIỂN NGUỒN NHÂN LỰC ATTT MẠNG
  - Chương VII: QUẢN LÝ NHÀ NƯỚC VỀ ATTT MẠNG
  - Chương VIII: ĐIỀU KHOẢN THI HÀNH

3 Pháp luật và chính sách ATTT

❑ 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.

3 Pháp luật và chính sách ATTT

❑ Luật Việt Nam về ATTT

❖ 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.

3 Pháp luật và chính sách ATTT

❑ 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.

4 .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.

4 Vấn đề đạo đức ATTT

- 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.

4 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.

4 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%.

4 Vấn đề đạo đức ATTT

- 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;
  - Người dùng đa số có hiểu biết về vấn đề bản quyền phần mềm, nhưng coi việc sử dụng phần mềm bất hợp pháp là bình thường vì nhiều nước chưa có quy định hoặc không xử lý nghiêm vi phạm.

4 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;

5. Mô hình đảm bảo ATTT

1. Mô hình đảm bảo ATTT 4 lớp của Bộ TTTT

Lớp 1. Kiện toàn lực lượng tại chỗ;

Lớp 2. Lựa chọn tối thiểu một tổ chức, doanh nghiệp giám sát, bảo vệ chuyên nghiệp;

Lớp 3. Định kỳ thực hiện kiểm tra, đánh giá độc lập;

Lớp 4. Kết nối, chia sẻ TT với hệ thống giám sát quốc gia.

5. Mô hình đảm bảo ATTT

Mô hình đảm bảo ATTT 4 lớp của Bộ TTTT

- "Lớp 1": lực lượng tại chỗ, chỉ định, kiện toàn đầu mối đơn vị chuyên trách về ATTT mạng để làm tốt công tác tham mưu, tổ chức thực thi và kiểm tra, đôn đốc thực hiện các quy định của pháp luật về bảo đảm AT, AN mạng.
- "Lớp 2" tổ chức hoặc thuê doanh nghiệp giám sát, bảo vệ chuyên nghiệp, tự thực hiện giám sát, ứng cứu sự cố ATTT mạng, bảo vệ HTTT thuộc quyền quản lý hoặc lựa chọn/thuê tổ chức, doanh nghiệp có đủ năng lực để thực hiện cung cấp dịch vụ giám sát, ứng cứu sự cố, bảo vệ ATTT mạng.

5. Mô hình đảm bảo ATTT

Mô hình đảm bảo ATTT 4 lớp của Bộ TTTT

- "Lớp 3" tổ chức hoặc thuê doanh nghiệp độc lập **kiểm tra, đánh giá định kỳ**, giám sát, bảo vệ để định kỳ; đối với các HTTT cấp độ 3 và cấp độ 4, định kỳ hàng năm thực hiện kiểm tra, đánh giá và báo cáo Bộ TT&TT trước ngày 14/12 để tổng hợp, báo cáo TTCP; đối với HTTT quan trọng quốc gia (cấp độ 5), định kỳ 6 tháng thực hiện kiểm tra, đánh giá và báo cáo Bộ TT&TT trước ngày 14/6 và ngày 14/12 hàng năm để tổng hợp, báo cáo TTCP

- "Lớp 4" kết nối, chia sẻ TT với hệ thống giám sát quốc gia, và với Trung tâm Giám sát AT không gian mạng quốc gia trực thuộc Cục ATTT, Bộ TT&TT và cung cấp các dải địa chỉ IP Public của các HTTT thuộc phạm vi quản lý.

5. Mô hình đảm bảo ATTT

Xác định cấp độ ATTT cho HTTT (85/2016/NĐ-CP): 5 cấp độ

- **HTTT cấp độ 1** là HTTT phục vụ hoạt động nội bộ của cơ quan, tổ chức và chỉ xử lý TT công cộng.
- **HTTTcấp độ 2** là HTTT có một trong các tiêu chí:

a- HTTT phục vụ hoạt động nội bộ của cơ quan, tổ chức và có xử lý TT riêng, TT cá nhân của người dùng nhưng không xử lý TT bí mật nhà nước;

b- HTTT phục vụ người dân, doanh nghiệp thuộc: Cung cấp TT và dịch vụ công trực tuyến từ mức độ 2 trở xuống; Cung cấp dịch vụ trực tuyến không thuộc danh mục dịch vụ kinh doanh có điều kiện; Cung cấp dịch vụ trực tuyến khác có xử lý TT riêng, TT cá nhân của dưới 1.000 người dùng;

c- Hệ thống cơ sở hạ tầng TT phục vụ hoạt động của một cơ quan, tổ chức….

5. Mô hình đảm bảo ATTT

❖ HTTT cấp độ 3:

1. HTTT xử lý TT bí mật nhà nước/ HT phục vụ quốc phòng, AN khi bị phá hoại sẽ làm tổn hại tới quốc phòng, an ninh quốc gia.

2. HTTT phục vụ người dân, DN thuộc một trong các loại hình:

a) Cung cấp TT, dịch vụ công trực tuyến từ mức độ 3 trở lên;

b) Cung cấp dịch vụ trực tuyến thuộc danh Mục dịch vụ kinh doanh có Điều kiện;

c) Cung cấp dịch vụ trực tuyến khác có xử lý TT riêng, TT cá nhân của từ 10.000 người sử dụng trở lên.

3. HT CSHT TT dùng chung phục vụ hoạt động của các cquan, tổ chức trong phạm vi một ngành, một tỉnh hoặc một số tỉnh.

4. HTTT Điều khiển công nghiệp trực tiếp phục vụ Điều khiển, vận hành hoạt động bình thường của các công trình xây dựng cấp II, cấp III hoặc cấp IV theo phân cấp của PL về xây dựng.

5. Mô hình đảm bảo ATTT

❖ HTTT cấp độ 4:

1. HTTT xử lý TT bí mật nhà nước hoặc hệ thống phục vụ quốc phòng, an ninh, khi bị phá hoại sẽ làm tổn hại nghiêm trọng quốc phòng, an ninh quốc gia.

2. HTTT quốc gia phục vụ phát triển Chính phủ điện tử, yêu cầu vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước.

3. HT CSHT TT dùng chung phục vụ hoạt động của các cơ quan, tổ chức trên phạm vi toàn quốc, yêu cầu vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước.

4. HTTT Điều khiển công nghiệp trực tiếp phục vụ Điều khiển, vận hành hoạt động bình thường của các công trình xây dựng cấp I theo phân cấp của PL về xây dựng.

5. Mô hình đảm bảo ATTT

❖ **HTTT cấp độ 5:**

1. HTTT xử lý TT bí mật nhà nước/HT phục vụ quốc phòng, an ninh, khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia.

2. HTTT phục vụ lưu trữ dữ liệu tập trung đối với một số loại hình TT, dữ liệu đặc biệt quan trọng của quốc gia.

3. HT CSHT TT quốc gia phục vụ kết nối liên thông hoạt động của Việt Nam với quốc tế.

4. HTTT Điều khiển công nghiệp trực tiếp phục vụ Điều khiển, vận hành hoạt động bình thường của công trình xây dựng cấp đặc biệt theo phân cấp của PL về xây dựng hoặc công trình quan trọng liên quan đến an ninh quốc gia

5. HTTT khác theo quyết định của Thủ tướng Chính phủ.

5. Mô hình đảm bảo ATTT

Các doanh nghiệp cung cấp dịch vụ SOC (Security Operation Center) giám sát ATTT mạng

- Cục ATTT, Bộ TTTT đã triển khai xây dựng bộ tiêu chí và thực hiện đánh giá, chứng nhận các DN Việt Nam cung cấp dịch vụ SOC
- Các DN Việt Nam được cung cấp nền tảng dịch vụ SOC đáp ứng yêu cầu kết nối, chia sẻ TT với Trung tâm Giám sát AT không gian mạng quốc gia:

  (1) Viettel, (2) VNPT, (3) BKAV, (4) FPT IS, (5) CMC Cyber Security, (6) CyRadar, (7) VNCS Global, (8) SAVIS …

- Các DN được phép kinh doanh trong lĩnh vực ANTT: **https://ais.gov.vn/hoat-dong/danh-sach-doanh-nghiep-da-duoc-cap-giay-phep-kinh-doanh-san-pham-dich-vu-an-toan-thong-tin-mang/**