CHƯƠNG 05

XÂY DỰNG, TRIỂN KHAI, KIỂM TRA VÀ CẢI TIẾN LIÊN TỤC CSATTT

Chương 05 - MỤC TIÊU

- Nắm được quy trình phát triển, thực hiện và duy trì các loại chính sách an toàn thông tin
- Viết được chính sách An toàn thông tin

XÂY DỰNG, TRIỂN KHAI, KIỂM TRA VÀ CẢI TIẾN LIÊN TỤC CSATTT

- Thiết kế CS
- Xem xét tổ chức tài liệu
- Triển khai CS an toàn thông tin
- Thực thi CS an toàn thông tin
- Cập nhật, sửa đổi CS
- Câu hỏi ôn tập

Những nguyên tắc phát triển CS và chuẩn ...

1. **Trách nhiệm**
   - Cần phải rõ ràng
   - Đảm bảo mọi người hiểu về trách nhiệm của mình trước hành động mà họ thực hiện khi sử dụng tài nguyên của tổ chức
2. **Nhận thức**
   - Chủ sở hữu, nhà cung cấp và người sử dụng HTTT cũng như các bên khác phải được biết về CS, trách nhiệm, cách thức thực hiện (practice), thủ tục và tổ chức đối với sự AT của HTTT
3. **Đạo đức**
   - HTTT và AT HTTT phải được cung cấp và sử dụng theo chuẩn đạo đức được áp dụng đối với môi trường vận hành của tổ chức

Những nguyên tắc phát triển CS và chuẩn ...

4. **Đa ngành, đa lĩnh vực**
   - Viết các tài liệu thư viện CS và chuẩn phải xem xét tất cả những người bị ảnh hưởng, bao gồm nhân viên kĩ thuật, quản trị, tổ chức, vận hành, thương mại, giáo dục và pháp luật
5. **Tỉ lệ (Proportionality)**
   - Các mức AT, chi phí, thực hành và thủ tục nên phù hợp và cân đối với giá trị dữ liệu cũng như mức độ tin cậy trên hệ thống
6. **Tích hợp**
   - Các tài liệu phải được phối hợp và tích hợp với nhau, đồng thời tích hợp với các biện pháp, thực hành và thủ tục có liên quan cho hệ thống AT chặt chẽ

Những nguyên tắc phát triển CS và chuẩn ...

7. **Phòng thủ chiều sâu**
   - Áp dụng các lớp kiểm soát và bảo vệ với khả năng phòng ngừa, phát hiện và ứng phó sẽ làm tăng tính AT
   - Cơ chế AT được phân tầng để điểm yếu của một cơ chế bảo vệ được hai hay nhiều cơ chế khác ngăn chặn
8. **Kịp thời**
   - Tất cả nhân viên, nhân viên được chỉ định và nhà cung cấp bên thứ 3 phải hành động kịp thời và phối hợp với nhau để ngăn chặn và ứng phó với những vi phạm AT
9. **Đánh giá lại**
   - Sự AT nên được đánh giá định kì vì rủi ro thay đổi hàng ngày
   - Cũng cần đánh giá lại chuẩn ít nhất 1 lần/năm để đảm bảo chúng vẫn phù hợp

Những nguyên tắc phát triển CS và chuẩn ...

10. **Dân chủ:** ATTT phải cân bằng các quyền của khách hàng, người dùng và những người khác bị ảnh hưởng bởi HT so với các quyền của người sở hữu và người vận hành HT
11. **Kiểm soát nội bộ**
    - ATTT là nòng cốt của hệ thống kiểm soát nội bộ thông tin của tổ chức
    - Hệ thống kiểm soát phải đặt đúng vị trí và hoạt động chính xác
    - Tổ chức sử dụng công nghệ để duy trì các bản ghi hoạt động

    → Công nghệ này phải gồm cả các cơ chế kiểm soát nội bộ (duy trì toàn vẹn thông tin)

Những nguyên tắc phát triển CS và chuẩn ...

12. **Đối thủ (Adversary):**
    - Các biện pháp kiểm soát, chiến lược AT, kiến trúc và tài liệu thư viện CS phải được phát triển và thực thi để dự phòng tấn công từ những đối thủ
13. **Đặc quyền tối thiểu**
14. **Phân chia nhiệm vụ**
15. **Tính liên tục**
    - Xác định nhu cầu của tổ chức đối với việc phục hồi thảm họa và hoạt động liên tục
    - Chuẩn bị tổ chức và HTTT của tổ chức phù hợp

Những nguyên tắc phát triển CS và chuẩn ...

16. **Tính đơn giản**

- Cố gắng áp dụng những biện pháp bảo vệ đơn giản, gọn nhẹ hơn là các biện pháp cồng kềnh, phức tạp

17. **AT lấy chính sách làm trung tâm**

- Các CS, chuẩn và thủ tục phải được thiết lập như nền tảng hình thức đối với việc quản lí việc lập kế hoạch, kiểm soát và đánh giá tất cả các hoạt động ATTT

Thiết kế CSATTT…

- Cách tiếp cận hiệu quả có sáu giai đoạn:
  - Phát triển (viết và phê duyệt)
  - Phổ biến (phân phối)
  - Xem xét (đọc)
  - Hiểu (hiểu)
  - Tuân thủ (thỏa thuận)
  - Thực thi thống nhất.

Thiết kế CSATTT…

- CS có hiệu lực và có thể bảo vệ được về mặt pháp lý:
  - Được phát triển bằng cách sử dụng các thông lệ được ngành công nghiệp chấp nhận và được ban quản lý chính thức phê duyệt
  - Phân phối bằng tất cả các phương pháp thích hợp
  - Được tất cả nhân viên đọc
  - Được tất cả nhân viên hiểu rõ
  - Chính thức đồng ý bằng hành động hoặc lời khẳng định
  - Được áp dụng và thực thi một cách thống nhất

Thiết kế CSATTT…

- Các vấn đề cần xem xét…:
  - Chiến lược và hướng triển khai hoạt động của tổ chức
  - Bản chất và kiểu TT tổ chức sử dụng
  - Các lớp người dùng TT và kiểu TT sử dụng
  - Nhu cầu chia sẻ và bảo vệ TT giữa các bộ phận trong tổ chức
  - Nhu cầu chia sẻ và bảo vệ TT giữa tổ chức với các bên có liên quan như nhà cung cấp, khách hàng, …
  - Các yêu cầu, nghĩa vụ và bổn phận tuân thủ tính riêng tư TT
  - Văn hóa AT của tổ chức và thời cơ thay đổi văn hóa
  - Hạ tầng cơ sở công nghệ hiện tại và cải tiến

Thiết kế CSATTT…

- Các vấn đề cần xem xét:
  - Kinh nghiệm từ những lần bị mất TT
  - Nhu cầu khác về tính bí mật, toàn vẹn và sẵn sàng đối với TT
  - CS và chuẩn hiện có
  - CS và chuẩn của các tổ chức khác
  - Xác định được 6 loại câu hỏi chính
    - Cái gì – Bảo vệ cái gì?
    - Ai – Ai chịu trách nhiệm?
    - Ở đâu – Phạm vi áp dụng của CS ở đâu trong tổ chức?
    - Thế nào – Giám sát sự tuân thủ như thế nào?
    - Khi nào – Khi nào CS có hiệu lực?
    - Tại sao – Tại sao lại phát triển CS?

Thiết kế CSATTT…

- Phương pháp tiếp cận để xây dựng:
  - Từ trên xuống
    - Chỉ sử dụng luật, quy định và thực hành tốt
  - Từ dưới lên
    - Chỉ dựa vào kiến thức của người quản trị hệ thống

→ **Cần phối hợp cả 2 phương pháp tiếp cận**

Thiết kế CSATTT…

- Xây dựng CS như một dự án gồm ba phần:
  - CS được thiết kế và viết (hoặc trong trường hợp CS lỗi thời, được thiết kế lại và viết lại)
  - Phê duyệt: quản lý hoặc điều hành cấp cao ở cấp thích hợp và cố vấn pháp lý của tổ chức xem xét và chính thức phê duyệt tài liệu
  - Quản lý: các quy trình quản lý được thiết lập để duy trì CS trong tổ chức

Thiết kế CSATTT…

- Thường được phát triển bằng cách sử dụng cách tiếp cận quản lý dự án giống như của SDLC:
  - Phải được lập kế hoạch, cấp vốn hợp lý và quản lý chặt chẽ để đảm bảo rằng nó được hoàn thành đúng thời hạn và trong ngân sách.
  - Giai đoạn khảo sát
  - Giai đoạn phân tích
  - Giai đoạn thiết kế
  - Giai đoạn thực thi
  - Giai đoạn bảo trì./.

Thiết kế CSATTT…

- Giai đoạn khảo sát: Nhóm phát triển CS cần đạt được:
  - Hỗ trợ từ quản lý cấp cao
  - Hỗ trợ và tham gia tích cực vào quản lý CNTT, đặc biệt là CIO
  - Mô tả rõ ràng các mục tiêu
  - Sự tham gia của các cá nhân phù hợp từ các cộng đồng có lợi ích bị ảnh hưởng bởi các CS
  - Đề cương chi tiết về phạm vi của dự án phát triển CS và các ước tính hợp lý về chi phí và lịch trình của dự án.

Thiết kế CSATTT…

- Giai đoạn phân tích
  - Đánh giá rủi ro mới hoặc gần đây hoặc kiểm toán CNTT ghi lại các nhu cầu ATTT hiện tại của tổ chức.
  - Tập hợp các tài liệu tham khảo chính, bao gồm CS hiện hành.
  - Xác định triết lý cơ bản của tổ chức khi đưa ra CS. Triết lý này thường thuộc một trong hai nhóm:
    - “Điều nào không được phép sẽ bị cấm” (phương pháp “danh sách trắng”)
    - "Điều nào không bị cấm được cho phép” (phương pháp “danh sách đen”).

Thiết kế CSATTT…

- Giai đoạn thiết kế…:
  - Nhiệm vụ đầu tiên trong giai đoạn thiết kế là soạn thảo văn bản CS thực tế.
  - Nguồn tài liệu:
    - Web - tìm kiếm các CS tương tự khác
    - Trang web của chính phủ - như http://csrc.nist.gov và http://csrc.nist.gov/groups/SMA/fasp/index.html
    - Tác phẩm chuyên nghiệp - Một số tác giả đã xuất bản sách về chủ đề này
    - Mạng ngang hang
    - Các nhà tư vấn chuyên nghiệp

Thiết kế CSATTT…

- Giai đoạn thiết kế:
  - Thông số kỹ thuật cho bất kỳ công cụ tự động nào
  - Sửa đổi báo cáo phân tích khả thi dựa trên chi phí và lợi ích được cải thiện khi thiết kế được làm rõ
  - Chuyển đến người quản lý hoặc điều hành phê duyệt để thực thi.

Thiết kế CSATTT…

- Giai đoạn thực thi:
  - Người dùng hoặc các thành viên của tổ chức phải thừa nhận một cách rõ ràng rằng họ đã nhận và đọc CS (tuân thủ).
    - Các chính sách sẽ được phân phối như thế nào
    - Việc xác minh phân phối sẽ được thực hiện như thế nào

Thiết kế CSATTT

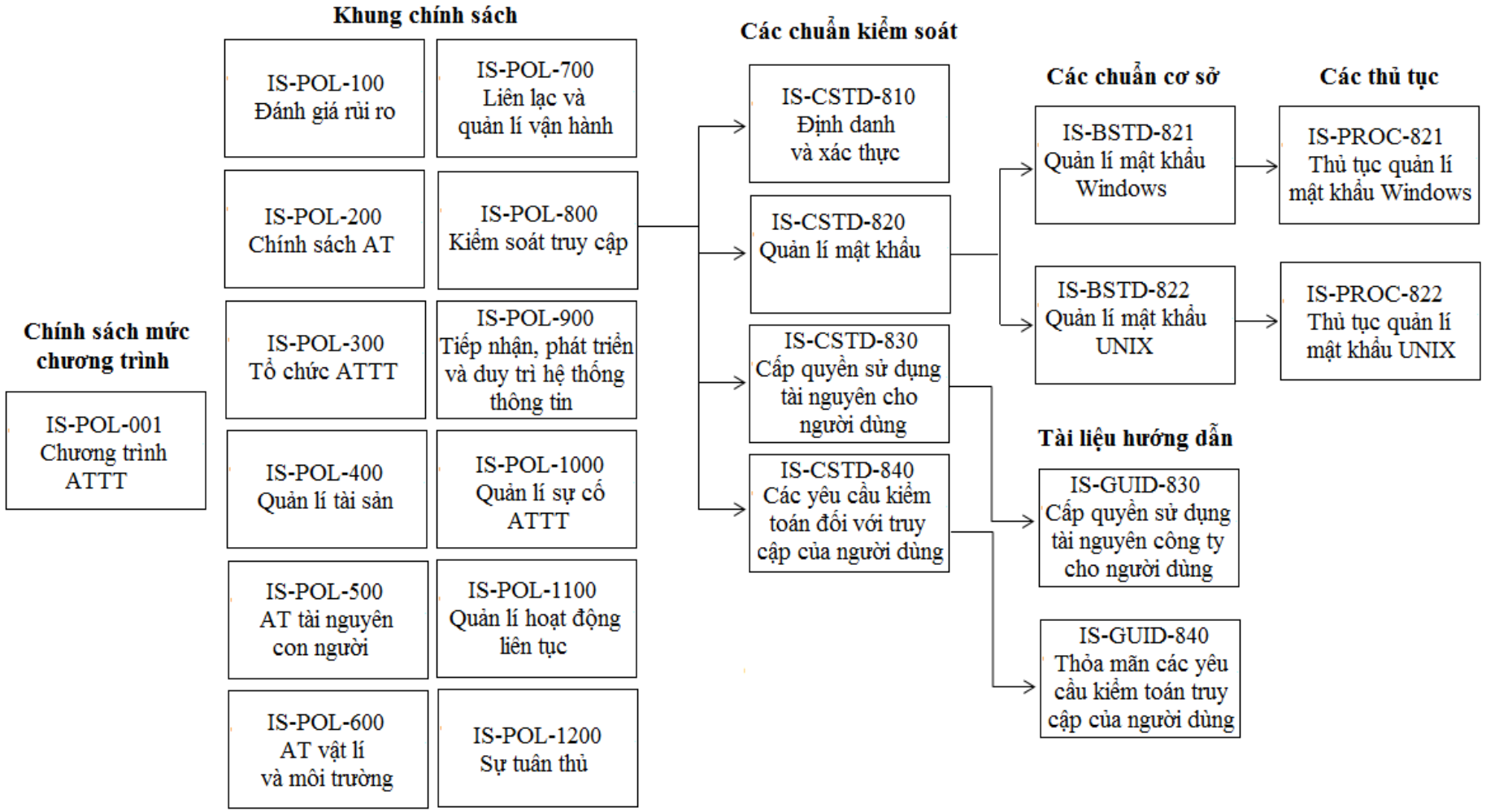
- Giai đoạn bảo trì:
  - Nhóm phát triển CS giám sát duy trì và sửa đổi CS khi cần thiết để đảm bảo rằng CS đó vẫn hiệu quả như một công cụ để đáp ứng các mối đe dọa đang thay đổi.
  - Phải có một cơ chế tích hợp để người dùng có thể báo cáo sự cố, tốt nhất là ẩn danh thông qua biểu mẫu Web được giám sát bởi nhóm pháp lý của tổ chức hoặc một ủy ban được giao nhiệm vụ thu thập và xem xét nội dung đó.
  - Phải đảm bảo rằng mọi người được yêu cầu tuân theo CS một cách bình đẳng và các CS không được thực hiện khác nhau trong các lĩnh vực hoặc thứ bậc khác nhau của tổ chức.

XÂY DỰNG, TRIỂN KHAI, KIỂM TRA VÀ CẢI TIẾN LIÊN TỤC CSATTT

- Thiết kế CS
- **Xem xét tổ chức tài liệu**
- Triển khai CS an toàn thông tin
- Thực thi CS an toàn thông tin
- Cập nhật, sửa đổi CS
- Câu hỏi ôn tập

Xem xét tổ chức tài liệu…

- Khi xây dựng CS nên tổ chức thư viện tài liệu theo một lược đồ có đánh số thứ tự
- Có thể tự tạo ra một khung CS, tuy nhiên nên tuân theo một chuẩn, ví dụ ISO/IEC 27002



Xem xét tổ chức tài liệu

- Giải thích:
  - IS (Information Security): ATTT
  - POL (Policy): Chính sách
  - XYZ: số thứ tự
    - 001: tài liệu đầu tiên
    - 100 – 1200: thứ tự các tài liệu trong tài liệu 001
    - …

XÂY DỰNG, TRIỂN KHAI, KIỂM TRA VÀ CẢI TIẾN LIÊN TỤC CSATTT

- Thiết kế CS
- Xem xét tổ chức tài liệu
- **Triển khai CS an toàn thông tin**
- Thực thi CS an toàn thông tin
- Cập nhật, sửa đổi CS
- Câu hỏi ôn tập

Khuôn mẫu CS ATTT

- *Tên CS và thông tin định danh*

1. *Mục đích*
2. *Tổng quan*
3. *Phạm vi*
4. *Chính sách*
5. *Vai trò và trách nhiệm*
6. *Luật/Hướng dẫn áp dụng*
7. *Tính hiệu lực*
8. *Thông tin và hỗ trợ*
9. *Phê chuẩn*
10. *Tài liệu tham chiếu./.*

Ví dụ về CSATTT…

- Tên chính sách và thông tin định danh
  - **Chính sách bàn làm việc sạch sẽ**

1. **Mục đích:** chỉ ra mục đích của CS
   - Mục đích của CS này là để thiết lập các yêu cầu tối thiểu cho việc duy trì "bàn làm việc sạch sẽ" – nơi mà thông tin nhạy cảm/quan trọng về các nhân viên, sở hữu trí tuệ, khách hàng và nhà cung cấp AT, cất vào chỗ được khóa và thoát khỏi trang Web. CS bàn làm việc sạch sẽ tuân thủ cả ISO 27001/17700 lẫn các biện pháp kiểm soát riêng tư cơ bản.

Ví dụ về CSATTT…

2. **Tổng quan:** giới thiệu tổng quan về CS

   - CS bàn làm việc sạch sẽ có thể là một công cụ để đảm bảo các dữ liệu nhạy cảm/bí mật phải được người dùng loại bỏ khỏi chỗ làm việc và được khóa khi không sử dụng hoặc khi nhân viên rời khỏi chỗ làm. Đây là một trong những chiến lược hàng đầu được áp dụng để hạn chế rủi ro từ những vi phạm AT ở nơi làm việc. Một CS như vậy cũng có thể nâng cao nhận thức của nhân viên về việc bảo vệ thông tin nhạy cảm.

Ví dụ về CSATTT…

3. **Phạm vi:** phạm vi áp dụng của CS
   - CS này áp dụng cho tất cả các nhân viên và các chi nhánh của công ty X
4. **Chính sách:** liệt kê ra các nội dung CS
   - Phải khóa các máy tính khi không sử dụng
   - Hết ngày làm việc phải tắt hoàn toàn các máy tính
   - Tủ tài liệu chứa thông tin nhạy cảm hoặc thông tin không được phổ biến rộng phải được đóng và khóa khi không sử dụng hoặc khi không có mặt ở đó
   - …

Ví dụ về CSATTT…

3. **Phạm vi:** phạm vi áp dụng của CS
   - CS này áp dụng cho tất cả các nhân viên và các chi nhánh của công ty X
4. **Chính sách:** liệt kê ra các nội dung CS
   - Phải khóa các máy tính khi không sử dụng
   - Hết ngày làm việc phải tắt hoàn toàn các máy tính
   - Tủ tài liệu chứa thông tin nhạy cảm hoặc thông tin không được phổ biến rộng phải được đóng và khóa khi không sử dụng hoặc khi không có mặt ở đó
   - …

Ví dụ về CSATTT…

5. **Vai trò và trách nhiệm:**
   - Liệt kê các thực thể và trách nhiệm liên quan tới việc thực thi CS
6. **Luật/Hướng dẫn áp dụng:**
   - Liệt kê các luật hoặc hướng dẫn mà CS có liên quan tới
7. **Tính hiệu lực**
   - Thông tin về thời gian thi hành và thời hạn điều chỉnh/xóa bỏ

Ví dụ về CSATTT…

8. Thông tin và hỗ trợ:

- Chỉ ra nơi có thể liên hệ để biết thêm thông tin về CS

9. Phê chuẩn:

- Đưa ra người và ngày phê chuẩn

10. Tài liệu tham chiếu

- Chỉ ra tài liệu bổ sung cho CS

XÂY DỰNG, TRIỂN KHAI, KIỂM TRA VÀ CẢI TIẾN LIÊN TỤC CSATTT

- Thiết kế CS
- Xem xét tổ chức tài liệu
- Triển khai CS an toàn thông tin
- **Thực thi CS an toàn thông tin**
- Cập nhật, sửa đổi CS
- Câu hỏi ôn tập

Thực thi CSATTT

- Việc thực thi CS phải có khả năng chịu được sự giám sát từ bên ngoài
- Tìm ra cách để thu hút nhân viên trong việc thực thi CS
- Công việc:
  - Phân phối CS
  - Đọc CS
  - Hiểu CS
  - Tuân thủ CS

Thực thi CSATTT…

- **Phân phối chính sách:**
  - Chính sách trao tay cho nhân viên
  - Đăng chính sách trên bảng thông báo công khai
  - E-mail
  - Intranet
  - Hệ thống quản lý tài liệu

Thực thi CSATTT…

- **Đọc chính sách:**
  - Kiểm tra xem tất cả các bên bị ảnh hưởng đã đọc chính sách chưa
- **Hiểu chính sách**
  - Ngôn ngữ:
    - Ở mức độ đọc hợp lý
    - Tối thiểu hoá các thuật ngữ kỹ thuật và thuật ngữ quản lý
  - Đánh giá sự hiểu biết về các vấn đề
    - Câu đố

Thực thi CSATTT…

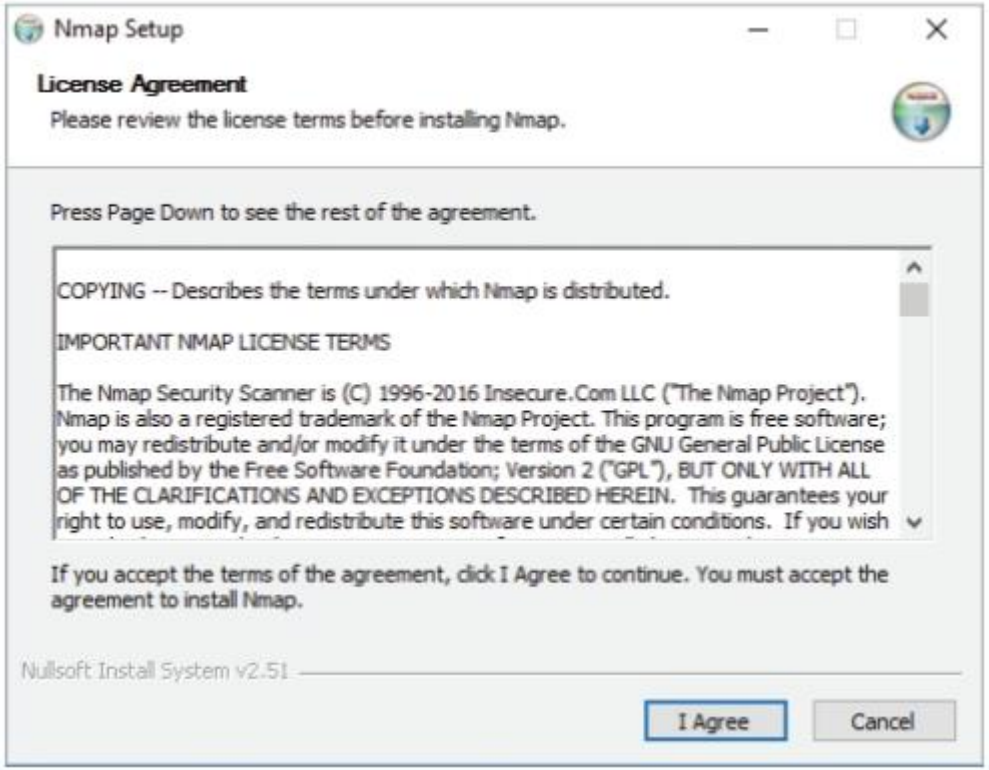
- **Tuân thủ chính sách….:**
  - Các chính sách phải được đồng ý bằng hành động hoặc sự khẳng định
  - Các tổ chức kết hợp các tuyên bố xác nhận chính sách vào hợp đồng lao động, đánh giá hàng năm

Thực thi CSATTT…

- **Tuân thủ chính sách…:**
  - Phương pháp:
    - **Nhận thức**: Các chương trình giáo dục, đào tạo và nhận thức về ATTT
    - **Văn hóa:** Các thông điệp hàng ngày, Ví dụ: Trách nhiệm cá nhân, chỉ thị, sự bắt buộc
    - **Công nghệ** có thể hỗ trợ việc tuân thủ dễ dàng hơn
      - Dùng bộ lọc để chặn một số trang Web mà cấm nhân viên truy nhập
      - CS và chuẩn về mật khẩu từ chối chấp nhận mật khẩu yếu
      - Sử dụng hạ tầng cơ sở công nghệ để giám sát và ghi nhật kí sự tuân thủ của người dùng

Thực thi CSATTT…

- Cách đơn giản nhất để ghi nhận CS bằng văn bản là đính kèm một tờ bìa có nội dung “Tôi đã nhận, đọc, hiểu và đồng ý với CS này”. Chữ ký và ngày tháng của nhân viên cung cấp dấu vết trên giấy về việc họ đã nhận được CS.
- Ví dụ về màn hình EULA yêu cầu đầu vào của người dùng cụ thể

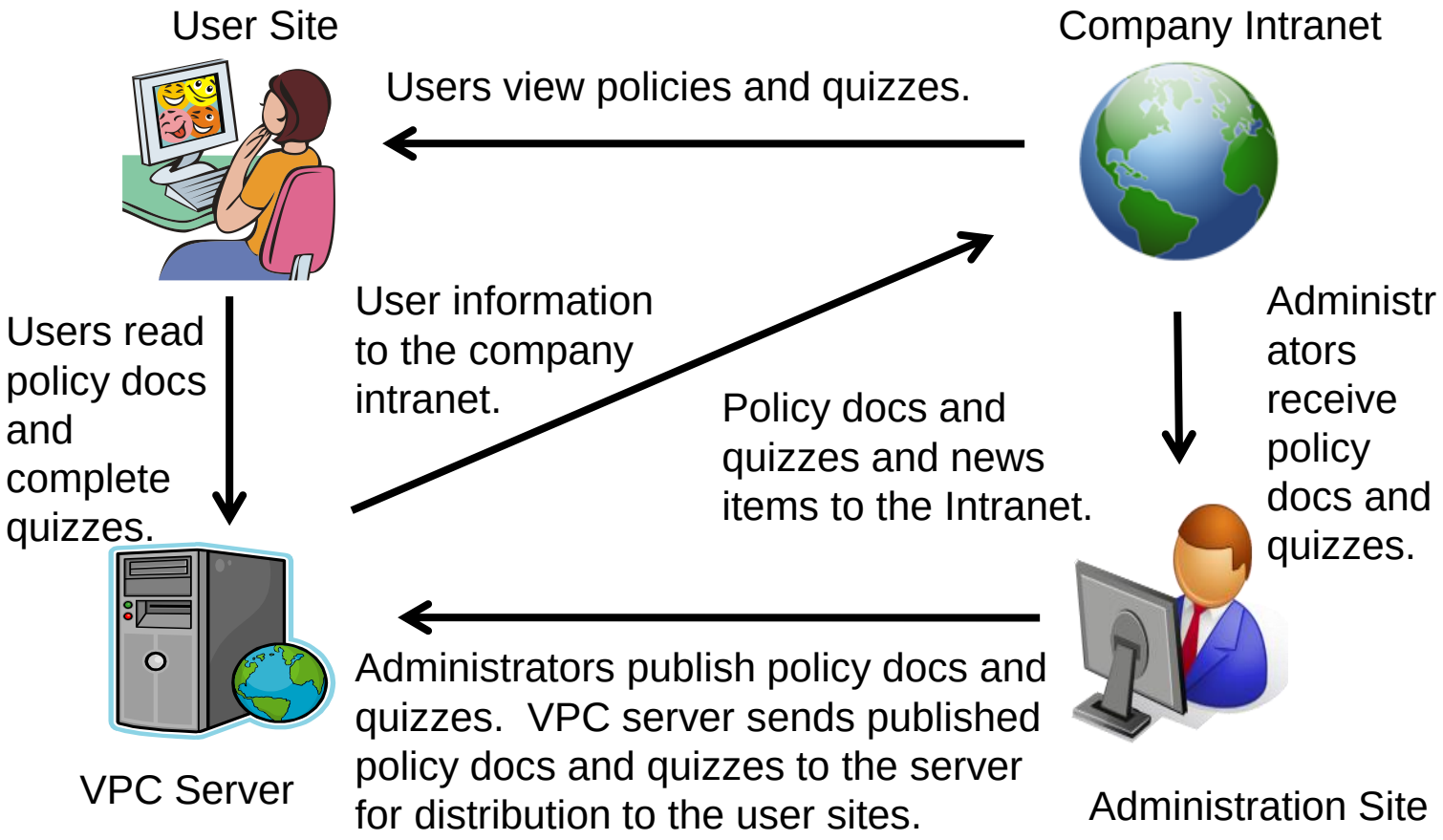


Thực thi CSATTT…

- Một cơ chế mạnh mẽ hơn:
  - Đánh giá tuân thủ: một bài kiểm tra ngắn, để đảm bảo rằng người dùng vừa đọc CS vừa hiểu CS. Điểm tối thiểu thường được thiết lập trước khi nhân viên được chứng nhận tuân thủ.
  - Một video đào tạo ngắn, bài kiểm tra tuân thủ là phương pháp hay nhất hiện nay để thực thi và tuân thủ CS.
- Muốn bắt buộc tuân thủ thành công cần:
  - Sự hỗ trợ cả về tài chính lẫn quyền lực của người quản lí
  - Mọi người trong tổ chức thấm nhuần CS
  - Những hình thức kỉ luật nhất định nếu không tuân thủ./.

Thực thi CSATTT…

- Công cụ tự động:
  - Trung tâm CS VigilEnt - trung tâm thực hiện và phê duyệt CS tập trung
    - Quản lý quy trình phê duyệt
    - Giảm nhu cầu phân phối các bản sao giấy
    - Quản lý biểu mẫu xác nhận CS



Thực thi CSATTT

- Giám sát CS:
  - Giám sát các hoạt động hàng ngày của tổ chức

    → Đảm bảo CS được tuân thủ một cách đúng đắn
  - Các bước thực hiện:
    - Đưa ra kết quả về hoạt động của người dùng
    - Kiểm toán và xem xét lại hệ thống
    - Kiểm tra phát hiện xâm nhập và kiểm tra xâm nhập
    - Phân tích vệt kiểm toán hoạt động của người dung
    - Tuân thủ CS kiểm toán

XÂY DỰNG, TRIỂN KHAI, KIỂM TRA VÀ CẢI TIẾN LIÊN TỤC CSATTT

- Thiết kế CS
- Xem xét tổ chức tài liệu
- Triển khai CS an toàn thông tin
- Thực thi CS an toàn thông tin
- **Cập nhật, sửa đổi CS**
- Câu hỏi ôn tập

Cập nhật, sửa đổi CS…

- Gồm các bước sau:
  - Xem xét lại báo cáo về sự cố ATTT
  - Xem xét lại ATTT và cơ sở hạ tầng công nghệ

    → Phát hiện ra những mối đe dọa mới
  - Xem xét lại các chiến lược hoạt động
  - Xem xét lại xu hướng và các sự kiện bất ngờ xảy ra
  - Xem xét lại các yêu cầu pháp lí
  - Sửa đổi yêu cầu đối với những thay đổi CS
  - Lặp lại vòng đời quản lí và phát triển CS

XÂY DỰNG, TRIỂN KHAI, KIỂM TRA VÀ CẢI TIẾN LIÊN TỤC CSATTT

- Thiết kế CS
- Xem xét tổ chức tài liệu
- Triển khai CS an toàn thông tin
- Thực thi CS an toàn thông tin
- Cập nhật, sửa đổi CS
- **Câu hỏi ôn tập**

Câu hỏi cuối chương…

- Câu 1.. Liệt kê và mô tả ba thách thức trong việc định hình CS.
- Câu 2. Trình bày về quy trình xây dựng CS theo cách tiếp cận quản lý dự án.
- Câu 3. Trình bày nguyên tắc trong xây dựng chính sách.
- Câu 4. Hãy soạn thảo một CSATTT mẫu cho từng vấn đề cụ thể cho một tổ chức. Ở phần đầu, hãy mô tả tổ chức mà Anh/Chị đang tạo CS và sau đó hoàn thành CS.

HỌC VIỆN KỸ THUẬT MẬT MÃ
AN TOÀN THÔNG TIN

Thank You!