**QUY CHẾ AN TOÀN THÔNG TIN**

*(Ban hành theo Quyết định số …/QĐ- CÔNG TY X ngày …/09/2021)*

Mục lục

[CHƯƠNG I. QUY ĐỊNH CHUNG 2](#_Toc82966318)

[Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng 2](#_Toc82966319)

[Điều 2. Giải thích từ ngữ 2](#_Toc82966320)

[Điều 3. Nguyên tắc chung 3](#_Toc82966321)

[Điều 4. Quản lý rủi ro hệ thống Công Ty X 3](#_Toc82966322)

[Điều 5. Quản lý tài sản 5](#_Toc82966323)

[Điều 6. Quản lý tài sản thông tin 5](#_Toc82966324)

[Điều 7. Quản lý tài sản vật lý 7](#_Toc82966325)

[Điều 8. Quản lý Tài sản phần mềm 7](#_Toc82966326)

[Điều 9. Trách nhiệm của các cá nhân, phòng ban liên quan 8](#_Toc82966327)

[Điều 10. Quy định đối với đối tác hoặc bên thứ ba 9](#_Toc82966328)

[Điều 11. An ninh thông tin mức vật lý 10](#_Toc82966329)

[Điều 12. Quy định sử dụng Tài sản vật lý 12](#_Toc82966330)

[Điều 13. Quy định vận hành hệ thống 13](#_Toc82966331)

[Điều 14. Quy định quản lý truy cập 17](#_Toc82966332)

[Điều 15. Quy định quản lý mã hóa 20](#_Toc82966333)

[Điều 16. Quy định xây dụng, phát triển và duy trì hệ thống 21](#_Toc82966334)

[Điều 17. Kế hoạch dự phòng đảm bảo hoạt động liên tục 23](#_Toc82966335)

[Điều 18. Quản lý sự cố ATTT 24](#_Toc82966336)

[Điều 19. Quy định đối với nhân sự tham gia hệ thống 25](#_Toc82966337)

[Điều 20. Quy định tuân thủ 31](#_Toc82966338)

[CHƯƠNG II. TỔ CHỨC THỰC HIỆN 31](#_Toc82966339)

[Điều 21. Đào tạo và truyền thông 31](#_Toc82966340)

[Điều 22. Điều khoản chung 32](#_Toc82966341)

**CHƯƠNG I. QUY ĐỊNH CHUNG**

**Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng**

1. **Phạm vi điều chỉnh**

Quy chế này quy định về bảo đảm an toàn hệ thống thông tin trong hoạt động của hệ thống Công Ty X

1. **Đối tượng áp dụng**

Các Phòng/Ban tham gia vào hệ thống Công Ty X phải tuân thủ các nguyên tắc về an toàn thông tin nêu tại Quy chế này.

**Điều 2. Giải thích từ ngữ**

1. **ATTT:** An toàn thông tin
2. **CNTT:** Công nghệ thông tin.
3. **ANM:** An ninh mạng.
4. **CN:** Công nghệ.
5. **Administrator:** Quản trị hệ thống.
6. **Nhân viên:** Là người có ký kết hợp đồng lao động toàn thời gian/hợp đồng lao động bán thời gian/hợp đồng tư vấn/hợp đồng thời vụ/hợp đồng tập sự hoặc hình thức khác.
7. **Tính bảo mật:** Bảo đảm thông tin chỉ được sử dụng bởi những người được cấp phép, không bị truy cập trái phép.
8. **Tính toàn vẹn:** Bảo vệ sự chính xác và đầy đủ của thông tin và thông tin không bị thay đổi trái phép.
9. **Tính sẵn sàng:** Bảo đảm thông tin phải sẵn sàng để sử dụng khi cần, đảm bảo tính hữu dụng của thông tin cho hoạt động nghiệp vụ của Công ty.
10. **Tài sản thông tin dữ liệu khách hàng (DLKH):** Là tất cả các thông tin liên quan đến khách hàng, bao gồm nhưng không hạn chế: Họ tên, thông tin liên lạc, dữ liệu lịch sử giao dịch.
11. **Tài sản thông tin dữ liệu tri thức (DLTT):** Là thông tin do tri thức của toàn bộ cán bộ nhân viên công ty phục vụ cho hoạt động của công ty, bao gồm nhưng không hạn chế: các quy trình nghiệp vụ, các tài liệu và quy trình đào tạo, sơ đồ hệ thống, quy trình vận hành, tài liệu hướng dẫn sử dụng.
12. **Tài sản thông tin hồ sơ ngưòi dùng (HSND):** Là thông tin khai báo của người dùng và các thuộc tính kèm theo, bao gồm nhưng không giới hạn: Tài khoản, mật khẩu, phân quyền hệ thống.
13. **Mức rủi ro chấp nhận được:** Là mức độ rủi ro không cần phải xử lý mà chỉ cần theo dõi. Thông thường là mức độ rủi ro chưa vượt ngưỡng cho phép.
14. **NDA** (Non-Disclosure Agreement): Thỏa thuận m kết không tiết lộ thông tin.
15. **LAN:** Mạng nội bộ có dây

**Điều 3. Nguyên tắc chung**

1. Công Ty X tập trung nguồn nhân lực nhằm tăng cường khả năng bảo đảm an toàn hệ thống thông tin.
2. Mỗi đơn vị, cá nhân phải đảm bảo an toàn thông tin trên mạng. Hoạt động an toàn thông tin của các đơn vị, cá nhân phải phù hợp với quy định của pháp luật và tuân thủ các nội dung tại quy chế này.
3. Các đơn vị, cá nhân sử dụng các hệ thống thông tin không được xâm phạm an toàn thông tin của đơn vị, cá nhân khác; trường hợp phát hiện hành vi vi phạm an ninh thông tin hoặc sự cố mất an toàn thông tin, phải có trách nhiệm thông báo kịp thời đến bộ phận an ninh thông tin của Công ty để nhận biết, phân loại, đánh giá và xử lý hiệu quả các rủi ro CNTT có thể xảy ra.
4. Xây dựng, triển khai quy chế an toàn hệ thống thông tin trên cơ sở hài hòa giữa lợi ích, chi phí và mức độ chấp nhận rủi ro của Công ty.
5. Xác định rõ quyền hạn, trách nhiệm của Lãnh đạo công ty và các Đơn vị, Ban, Bộ phận, cá nhân đối với công tác bảo đảm an toàn hệ thống thông tin.
6. Định kỳ rà soát, chỉnh sửa, hoàn thiện Quy chế an toàn thông tin, hoặc khi phát hiện những bất cập, bất hợp lý gây mất mát an toàn hệ thống CNTT.
7. Các tài liệu, hợp đồng bằng văn bản khi được ban hành phải thực hiện theo quy định đánh mã mà công ty Công Ty X đặt ra.

**Điều 4. Quản lý rủi ro**

1. Quản lý rủi rohệ thống của tập đoàn Công Ty X bao gồm nhận diện, đánh giá và xử lý các rủi ro có thể xảy ra nhằm giảm thiểu thiệt hại và mất mát với tài sản, thông tin và uy tín của Công Ty X.
2. Nhân sự của hệ thống Công Ty X và các bên liên quan có trách nhiệm xây dựng và triển khai Quy trình quản lý rủi ro hệ thống Công Ty X.
3. Nhân sự của hệ thống Công Ty X và các bên liên quan phải nhận diện, đánh giá rủi ro khi đưa một hệ thống thông tin mới vào vận hành hoặc có sự thay đổi đáng kể đối với hệ thống thông tin hiện tại và phải thực hiện đánh giá rủi ro tối thiểu hàng năm nhằm nhận biết phạm vi các rủi ro cũng như các mối đe dọa tiềm tàng có thể xảy ra với một hoặc nhiều loại tài sản CNTT của Công Ty X
4. Công tác nhận diện, đánh giá rủi ro hệ thống của tập đoàn Công Ty X bao gồm:
5. Nhận biết, phân loại các điểm yếu và mối đe doạ đối với hệ thống của tập đoàn Công Ty X.
6. Đánh giá khả năng xảy ra của rủi ro đối với hệ thống: Phải cân nhắc các yếu tố nguyên nhân và khả năng xảy ra mối đe dọa; bản chất của điểm yếu tồn tại trong hệ thống Công Ty X tương ứng; rà soát tính hiệu quả các giải pháp kiểm soát rủi ro hiện hành.
7. Phân tích mức độ ảnh hưởng của rủi ro: Phải phân tích và xác định mức độ ảnh hưởng bất lợi khi một mối đe doạ khai thác thành công điểm yếu của hệ thống Công Ty X.
8. Định lượng rủi ro để đánh giá cấp độ của rủi ro xảy ra với hệ thống Công Ty X .
9. Phân tích và lựa chọn biện pháp kiểm soát rủi ro: Phải phân tích và chọn ra các giải pháp khả thi hoặc lên kế hoạch thực hiện để có thể hạn chế đến mức thấp nhất hoặc loại trừ các rủi ro có nguy cơ xảy ra cho hệ thống Công Ty X .
10. Kết quả của việc đánh giá rủi ro phải được lập thành báo cáo, giúp xác định các biện pháp kiểm soát phù hợp để hạn chế tác hại của các rủi ro hoặc triệt tiêu rủi ro có thể xảy ra một cách hợp lý.
11. Công tác xử lý rủi ro bao gồm:
12. Xác định biện pháp xử lý rủi ro: Lựa chọn một trong các biện pháp xử lý chấp nhận rủi ro; chuyển giao rủi ro; giảm thiểu tác động của rủi ro; né tránh rủi ro.
13. Lập chiến lược xử lý rủi ro bao gồm việc phân chia các cấp độ rủi ro và lựa chọn biện pháp xử lỷ rủi ro tương ứng.
14. Phải chỉ rõ tất cả các biện pháp kiểm soát thích hợp có thể làm hạn chế hoặc loại trừ rủi ro phù hợp với hoạt động của hệ thống Công Ty X .
15. Lập kế hoạch xử lý rủi ro với các thông tin: Các rủi ro xảy ra với tài sản và đánh giá mức độ; đề xuất giải pháp xử lý rủi ro; nguồn lực cần thiết cho việc thực hiện giải pháp được lựa chọn; phòng/nhân viên thực hiện; ngày bắt đầu triển khai; ngày dự kiến hoàn thành; các yếu tố cần thiết để duy trì thực hiện kế hoạch.
16. Kết quả của việc xử lý rủi ro phải được lập thành báo cáo, kết hợp với báo cáo đánh giá rủi ro và phải có sự phê duyệt của lãnh đạo hệ thống Công Ty X .

**Điều 5. Quản lý tài sản**

1. Tất cả các tài sản của tập đoàn Công Ty X đều phải được lập danh sách, phân loại, đánh giá mức độ quan trọng, đánh giá mức độ rủi ro, áp dụng các biện pháp bảo vệ phù hợp.
2. Tập đoàn Công Ty X chia tài sản CNTT thành 03 loại:
3. Tài sản thông tin: Là các dữ liệu, tài liệu liên quan đến hệ thống công nghệ thông tin, được thể hiện bằng văn bản giấy hoặc dữ liệu điện tử.
4. Tài sản phần mềm: Bao gồm các chương trình ứng dụng, phần mềm hệ thống, cơ sở dữ liệu và công cụ phát triển.
5. Tài sản phần cứng: Là các trang thiết bị công nghệ thông tin và các thiết bị phục vụ cho hoạt động của hệ thống của tập đoàn Công Ty X.
6. Tập đoàn Công Ty X phân loại mức độ quan trọng của tài sản CNTT thành 05 mức như sau:
7. Thông tin tuyệt mật: Là các thông tin có nội dung rất quan trọng, mang tính công nghệ lõi, nếu mất/lộ sẽ ảnh hưởng nghiêm trọng đến các hoạt động Tập đoàn, chỉ lưu hành trong phạm vi những người cần phải biết và được bảo vệ đặc biệt. Việc tiết lộ/mất mát tài sản CNTT này có thể vi phạm pháp luật hoặc có khả năng gây ra thiệt hại đặc biệt nghiêm trọng cho tập đoàn, khách hàng hay các đối tác bên thứ ba.
8. Thông tin bí mật: Là thông tin có nội dung quan trọng, luôn được giám sát và kiểm soát chặt chẽ, chỉ hành trong phạm vi những người cần phải biết. Việc tiết lộ/mất mát tài sản CNTT này có thể vi phạm pháp luật hoặc có khả năng gây ra thiệt hại nghiêm trọng cho tập đoàn, khách hàng hay đối tác của bên thứ 3.
9. Thông tin hạn chế: Là các thông tin có nội dung quan trọng và mang tính chuyên môn của đơn vị, ban, bộ phận. Chỉ lưu hành trong phạm vi đơn vị, ban, bộ phận.
10. Thông tin nội bộ: Là các thông tin không có nội dung quan trọng. Chỉ lưu hành trong phạm vi tập đoàn.
11. Thông tin không kiểm soát: Là thông tin không kiểm soát.

**Điều 6. Quản lý tài sản thông tin**

1. Ban An ninh mạng làm đầu mối lập danh sách quản lý tài sản thông tin theo mẫu và có trách nhiệm thống kê, rà soát thiết bị định kỳ.
2. Cán bộ nhân viên không được sao chép, gửi, in ấn hoặc lưu trữ tài sản thông tin thuộc loại Mật và Tuyệt mật của tập đoàn Công Ty X để gửi ra ngoài hay lưu vào các thiết bị lưu trữ cắm ngoài. Trường hợp cần thông tin loại này phải đề xuất và được sự phê duyệt cùa cấp có thẩm quyền.
3. Các nguyên tắc khi trao đổi Tài sản thông tin:
4. Thông tin Mật/ Tuyệt mật khi vận chuyển **bằng đường bưu điện** phải được đặt trong phong bì, đóng dấu niêm phong và ghi rõ loại thông tin bên ngoài. Phong bì chứa thông tin Mật/ Tuyệt mật đã niêm phong phải được bọc trong một phong bì khác và gửi đi bằng dịch vụ gửi bưu phẩm đảm bảo.
5. Nhân viên của Công Ty X **trực tiếp mang, vận chuyển** các thông tin Mật/ Tuyệt mật phải đảm bảo không tiết lộ nội dung cũng như việc đang mang theo các thông tin Mật/ Tuyệt mật cho những người không liên quan; Không để các thông tin Mật/ Tuyệt mật ở những nơi không có sự giám sát.
6. Thông tin Mật/ Tuyệt mật khi truyền **qua các phưong tiện điện tử** phải được mã hóa dữ liệu nhằm đảm bảo chỉ có người nhận biết mật khẩu mới có thể đọc được nội dung tài liệu. Mật khẩu và tài liệu chứa thông tin Mật/ Tuyệt mật không được phép gửi cùng nhau, mà mật khẩu phải được gửi bằng một email theo sau hoặc một phương tiện khác gửi tin một cách bảo mật. Thông tin gửi qua phương tiện trực tuyến phải được bảo vệ khỏi việc gửi đi không đầy đủ, sai đường truyền, thay đổi, tiết lộ, sao chép không đúng quyền hạn.
7. Thông tin Mật/ Tuyệt mật **khi trao đổi qua điện thoại** phải bảo đảm đủ các điều kiện sau:

* Xác nhận chính xác danh tính của người gọi (khách hàng, nhân viên trong Công ty, cơ quan pháp luật).
* Luôn đảm bảo liên hệ đúng người cần gặp ngay cả khi biết trước số máy gọi của khách hàng, nhân viên thuộc phòng ban khác, đối tác bên thứ ba.
* Khi thực hiện cuộc gọi tại những nơi công cộng (sân bay, nhà ga, bến tàu, khách sạn, thang máy) phải đề phòng cuộc gọi có thể bị nghe lén.
* Không cung cấp mật khẩu đăng nhập, mã số PIN.

1. Lưu trữ Tài sản thông tin: Tài sản thông tin của tập đoàn Công Ty X phải được lưu trữ theo phương thức phù hợp với loại và mức độ quan trọng của tài sản.
2. Tài sản thông tin được công bố phải được bảo vệ khỏi các hành động gian lận về điều khoản hợp đồng, tiết lộ hoặc sửa đổi của người không có thẩm quyền.
3. Thành phần lưu trữ tài sản thông tin phục vụ cho giao dịch thương mại điện tử phải được thiết lập sẵn và bảo vệ để ngăn ngừa sự sửa đổi của người không được phép.
4. Tài sản thông tin thuộc loại Mật và Tuyệt mật nhân viên phụ trách liên quan không được phép gửi ra ngoài hay lưu vào các thiết bị lưu trữ cắm ngoài. Trường hợp cần thông tin loại này phải đề xuất và được sự phê duyệt của cấp có thẩm quyền.
5. Các thông tin Mật/ Tuyệt mật dạng giấy tờ phải được lưu trong tủ có khóa bảo vệ hoặc trong khu vực có kiểm soát truy cập vào ra, đảm bảo chỉ có người được phép mới có thể truy cập.
6. Các thông tin Mật/ Tuyệt mật dạng bản mềm phải có kiểm soát truy cập chặt chẽ, và phải có phương pháp mã hóa phù hợp (Như veracrypt, keepass…)
7. Hủy bỏ Tài sản thông tin
8. Thông tin dư thừa, không sử dụng hoặc không cần lưu trữ phải được hủy bỏ. Trước khi hủy bỏ, đơn vị thực hiện hủy phải xin phê duyệt của Lãnh đạo phụ trách trực tiếp, phòng ban liên quan đến thông tin hủy bỏ. Những thông tin này, khi chưa được hủy bỏ, phải lưu ở nơi an toàn đảm bảo tính bảo mật.
9. Tùy thuộc vào loại thông tin mà cách thức hủy bỏ thông tin được thực hiện khác nhau để đảm bảo tính an toàn bảo mật và không thể khôi phục
10. Thông tin bản cứng khi không sử dụng hoặc hết hạn sử dụng cần đảm bảo được xé vụn hoặc tiêu hủy bằng máy hủy giấy trước khi vứt đi. Tuyệt đối không để nguyên trạng tài liệu khi vứt bỏ.
11. Các thông tin Mật/ Tuyệt mật lưu trên các phương tiện lưu trữ (đĩa CD, đĩa cứng hoặc các phương tiện lưu trữ điện từ khác của Công Ty X ) phải được hủy bỏ bằng biện pháp phù hợp (format dữ liệu, nghiền nát, hủy vật lý…) không có khả năng khôi phục trước khi loại bỏ, thanh lý hoặc đưa các phương tiện lưu trữ trên ra ngoài kiểm soát của Công Ty X .

**Điều 7. Quản lý tài sản vật lý**

1. Tất cả các tài sản vật lý của tập đoàn Công Ty X được quản lý, thống kê trên hệ thống quản lý tài sản (BEM) của công ty và thực hiện theo đúng “Quy trình về quản lý thiết bị”
2. Các tài sản vật lý chỉ được mang ra ngoài văn phòng khi được Giám đốc công ty phê duyệt.
3. Loại bỏ tài sản phần cứng thực hiện theo “Quy định về việc xử lý khi loại bỏ và khi bàn giao lại phương tiện lưu trữ”.

**Điều 8. Quản lý Tài sản phần mềm**

1. Tập đoàn Công Ty X chỉ sử dụng các phần mềm do Công Ty X tự phát triển hoặc phần mềm có bản quyền, tuyệt đối không sử dụng các phần mềm không rõ nguồn gốc, phần mềm bị bẻ khóa trên các tài sản phần cứng/thiết bị của Công Ty X .
2. Ban ANM định kỳ thực hiện rà soát, cập nhật các bản vá lỗi về an ninh bảo mật, quét virus định kỳ.
3. Định kỳ rà soát danh sách phần mềm được cài đặt trên hệ thống, gỡ bỏ phần mềm không còn sử dụng, cài đặt thêm phần mềm cần thiết.

**Điều 9. Trách nhiệm của các cá nhân, phòng ban liên quan**

1. Tất cả các nhân viên của tập đoàn Công Ty X đều phải có trách nhiệm bảo vệ tài sản thông tin của Công Ty X, sử dụng đúng quyền truy cập được cấp, tham gia các chương trình đào tạo nhận thức an toàn thông tin. Khi không còn làm việc tại Công Ty X thì phải có trách nhiệm bàn giao tất cả các quyền truy cập, tài sản CNTT và cam kết không tiết lộ, đánh cắp, phá hoại hệ thống thông tin của tập đoàn Công Ty X.
2. Trách nhiệm của nhân viên tuyển dụng:
3. Nhân viên tuyển dụng có trách nhiệm thương thảo với ứng viên và được ghi trong điều khoản của hợp đồng lao động liên quan quy định bảo mật thông tin. Hợp đồng lao động phải bao gồm các điều khoản về cam kết bảo mật thông tin của người được tuyển dụng với Công Ty X trong và sau khi làm việc.
4. Nhân viên tuyển dụng phải kiểm tra lý lịch, thông tin ứng viên, các yếu tố khen thưởng, kỷ luật trước đó để xem xét đánh giá tư cách đạo đức, trình độ chuyên môn của các ứng viên cho phù hợp với yêu cầu của vị trí tuyển dụng.
5. Nhân viên tuyển dụng cần làm rõ trách nhiệm về ATTT cho các vị trí cần tuyển dụng thông qua bản mô tả công việc hoặc yêu cầu tuyển dụng của phòng ban.
6. Trách nhiệm của nhân viên:
7. Tất cả các nhân viên của Công Ty X được đào tạo và cập nhật thông tin về các quy trình, Quy chế ATTT kịp thời. Nội dung đào tạo có thể khác nhau tùy từng đối tượng.
8. Nhân viên phải ký cam kết bảo mật thông tin, quyền sở hữu trí tuệ và không xung đột lợi ích.
9. Chương trình đào tạo định hướng của Công Ty X phải có các nội dung cơ bản về ATTT mà nhân viên phải tuân thủ, giúp nhân viên mới nắm rõ vai trò và trách nhiệm của mình trong việc tuân thủ, đảm bảo ATTT của công ty.
10. Nhân viên khi được bổ nhiệm, miễn nhiệm, bãi nhiệm, luân chuyển, điều động, tạm hoãn, chấm dứt hợp đồng hoặc nghỉ theo chế độ thai sản có trách nhiệm hoàn trà nguyên vẹn các tài sản CNTT thuộc hệ thống Công Ty X
11. Nhân viên đã được điều chỉnh hoặc cắt toàn bộ các quyền truy cập hệ thống thông tin, ứng dụng thì vẫn phài tiếp tục chịu trách nhiệm và nghĩa vụ bảo mật thông tin hệ thống của tập đoàn Công Ty X trong thời gian sau đó.
12. Đối với các nhân viên không có hợp đồng toàn thời gian, trưởng bộ phận quản lý trực tiếp có trách nhiệm phổ biến Quy chế ATTT, giám sát tuân thủ và cùng chịu trách nhiệm về các vấn để ATTT với nhân viên đó.
13. Trách nhiệm của Ban An ninh mạng
14. Tổ chức các chương trình truyền thông nội bộ nhằm nâng cao ý thức, trách nhiệm của toàn bộ nhân viên thuộc hệ thống Công Ty X nói chung về ATTT.
15. Nhận diện và đánh giá rủi ro để đề xuất biện pháp xử lý/khắc phục phù hợp.
16. Đề xuất áp dụng các biện pháp xử lý kỷ luật đối với các nhân viên khi có hành vi vi phạm Quy chế ATTT. Hình thức kỷ luật tùy thuộc vào mức độ nghiêm trọng của hành vi vi phạm và được xử lý theo quy định của công ty và quy định của pháp luật.

**Điều 10. Quy định đối với đối tác hoặc bên thứ ba**

Hợp tác với đối tác hoặc bên thứ ba phải đảm bảo ATTT và an toàn dữ liệu cho hệ thống của tập đoàn Công Ty X từ khâu ký kết hợp đồng, thực hiện cho đến kết thúc hợp đồng theo trình tự sau:

1. Trước khi ký kết hợp đồng với đối tác hoặc bên thứ ba:
2. Thông qua các biện pháp như phỏng vấn, đánh giá danh tiếng và uy tín, kiểm chứng thông tin, đơn vị đầu mối đánh giá được mức độ cam kết bảo mật thông tin của đối tác hoặc bên thứ ba để đối chiếu tiêu chuẩn về ATTT của Công Ty X.
3. Trao đổi với đối tác hoặc bên thứ ba về tiêu chuẩn ATTT của Công Ty X. Hai bên phải ký cam kết không tiết lộ thông tin (NDA), xác nhận trách nhiệm của đối tác hoặc bên thứ ba trong việc đảm bảo an toàn dữ liệu và hệ thống thông tin của Công Ty X .
4. Trong thời gian thực hiện hợp đồng với đối tác hoặc bên thứ ba:
5. Công Ty X có kế hoạch rà soát định kỳ bởi phòng ban trực tiếp làm việc với đối tác hoặc bên thứ ba nhằm đánh giá mức độ tuân thủ cam kết về ATTT với Công Ty X .
6. Đối tác hoặc bên thứ ba khi làm việc tại Công Ty X phải đảm bảo thực hiện đầy đủ các yêu cầu về cam kết ATTT trong phạm trù công việc liên quan, đồng thời chứng minh được việc đáp ứng đầy đủ các cam kết đã được thống nhất và ký kết trước đó.
7. Trong trường hợp Công Ty X phát hiện các sự cố, dấu hiệu vi phạm ATTT của đối tác hoặc bên thứ ba, phòng ban trực tiếp làm việc với đối tác phải:

* Tạm dừng hoạt động liên quan của đối tác với Công ty
* Ngay lập tức báo cáo lãnh đạo trực tiếp quản lý và phòng ban phụ trách về ATTT của tập đoàn Công Ty X.
* Bộ phận phụ trách ATTT phối hợp với các đơn vị liên quan đánh giá mức độ vi phạm để báo cáo Ban lãnh đạo đơn vị
* Sau khi có kết luận chính thức của Ban An ninh mạng, đơn vị đầu mối có trách nhiệm thông báo chính thức các vi phạm về ATTT cho đối tác hoặc bên thứ ba.
* Đơn vị đầu mối trực tiếp làm việc với đối tác hoặc bên thứ ba và báo cáo cho Lãnh đạo đơn vị kết quả làm việc và đề xuất biện pháp khắc phục hoặc tạm dừng hoặc chấm dứt Hợp đồng.
* Trong trường họp tạm dừng dịch vụ thì quản trị viên có trách nhiệm thu hồi quyền truy cập hệ thống Công Ty X đã cấp cho đổi tác hoặc bên thứ ba.

1. Khi kết thúc hợp đồng với đối tác hoặc bên thứ ba:
2. Trước khi kết thúc hợp đồng với Công Ty X , đối tác hoặc bên thứ ba phải hoàn trả tất cả tài sản và quyền truy cập hệ thống, tòa nhà cho các phòng ban liên quan.
3. Quản trị viên thực hiện vô hiệu hóa, xóa bỏ hay thay đổi ngay các khóa, mật khẩu tạm thời đã được bàn giao cho đối tác hoặc bên thứ ba.

**Điều 11. An ninh thông tin mức vật lý**

1. Quy định truy cập các khu vực vật lý
2. Khu vực vật lý đặt các hệ thống thông tin phải có các biện pháp bảo vệ, kiểm soát truy cập, lưu nhật ký truy cập. Việc truy cập vào khu vực cần phải được cấp có thẩm quyền phê duyệt tùy vào mức độ quan trọng của khu vực. Những khu vực chứa thông tin và phương tiện xử lý thông tin phải được bảo vệ, kiểm soát truy cập vào ra (ví dụ như tường, cửa ra vào có trang bị hệ thống thẻ từ/vân tay, có bảo vệ kiểm soát, có hệ thống mera theo dõi...), có bảo vệ kiểm soát, có hệ thống mera theo dõi...
3. Các khu vực bảo mật là khu vực có yêu cầu cao về an toàn bảo mật như phòng máy chủ, trung tâm dữ liệu, phải có các biện pháp kiểm soát truy cập và ghi nhật ký truy cập, đảm bảo chỉ những người được phép mới có thể ra vào khu vực này, phải có nội quy và hướng dẫn làm việc rõ ràng, phù hợp.
4. Khu vực văn phòng, khu vực làm việc và các thiết bị văn phòng phải được kiểm soát bảo mật vật lý phù hợp.
5. Các khu vực giao/nhận hàng, sảnh lễ tân và một số khu vực công cộng khác phải được kiểm soát chặt chẽ, và tách biệt với các khu vực đặt phương tiện xử lý thông tin để tránh bị truy cập trái phép.
6. Quy định kiểm soát ra vào đối với tất cả nhân viên Công ty và khách
7. Chỉ được quyền ra vào khu vực tương ứng theo phạm vi được cấp phép
8. Thực hiện nguyên tắc quyền hạn tối thiểu: Mỗi cá nhân chỉ được cấp quyền truy cập tối thiểu vào tòa nhà hay hệ thống cơ sở vật chất của Công Ty X , đủ để phục vụ công việc.
9. Các khu vực lưu trữ, xử lý thông tin Mật/ Tuyệt mật như các phòng ban công nghệ, quản lý thẻ bảo mật, trung tâm dữ liệu (Data center) phải được kiểm soát bằng các hệ thống kiểm soát truy cập vật lý.
10. Thẻ truy cập của khách phải được phân biệt với thẻ của nhân viên, được giới hạn khu vực và thời gian truy cập.
11. Các nhân viên, khách khi ra vào tòa nhà của công ty phải đeo thẻ trước ngực (thẻ nhân viên, thẻ khách).
12. Không được phép sử dụng chung, cho mượn, trao đổi thẻ.
13. Thu hồi thẻ và quyền truy cập của cá nhân nghỉ phép dài hạn, chuyển công tác hay thôi việc.
14. Nghiêm cấm việc mang túi xách, điện thoại di động, mera, máy ghi hình vào các khu vực bảo mật. Việc truy cập những khu vực này phải được sự phê duyệt bằng văn bản của Lãnh đạo đơn vị quản lý trực tiếp khu vực bảo mật và phải ghi lại trong nhật ký truy cập.
15. Lãnh đạo các phòng ban quản lý hệ thống truy cập tại các khu vực bảo mật phải xem xét định kỳ về quyền truy cập của các đối tượng được phép, đồng thời kiềm tra nhật ký truy cập khu vực mình phụ trách.
16. Nhân viên công ty cần giám sát không để khách của mình khi ra/vào công ty tự ý kết nối thiết bị vào hệ thống mạng của công ty.
17. Lễ tân kiểm soát thông tin khách, đối tác tới làm việc về tên, số chứng minh thư/ hộ chiếu, thời gian vào/ ra, mục đích, khu vực làm việc. Thông tin này cần được lưu đầy đủ trong nhật ký ra vào của khách và được lưu tối thiểu 03 (ba) tháng.

**Điều 12. Quy định sử dụng Tài sản vật lý**

1. Các thiết bị CNTT phải được đánh giá ATTT, bố trí vị trí lắp đặt đảm bảo an toàn trước khi đưa vào sử dụng. Với các thiết bị quan trọng phải có thiết bị dự phòng. Các thiết bị lưu dữ liệu cần phải xóa vĩnh viễn các thông tin trước khi hủy bỏ hoặc tái sử dụng cho việc khác.
2. Quy định về bố trí lắp đặt thiết bị CNTT:
3. Các thiết bị và hệ thống công nghệ của hệ thống của tập đoàn Công Ty X phải được lắp đặt tại các khu vực ít người qua lại, an toàn, tránh các nguy cơ có thể xảy ra như hỏa hoạn, lũ lụt, động đất, ô nhiễm khói bụi, nhiễu sóng điện từ trường, nhiễm xạ và được áp dụng các biện pháp kiểm soát truy cập để ngăn ngừa các truy cập trái phép.
4. Các phương tiện xử lý thông tin liên quan tới các dữ liệu Mật/ Tuyệt Mật cần được đặt tại các vị trí hạn chế tầm quan sát từ bên ngoài, tránh tiết lộ thông tin.
5. Tại các trung tâm dữ liệu, phòng máy chủ cần phải đảm bảo có giám sát và trang bị thiết bị cảnh báo các điều kiện môi trường bên trong (nhiệt độ, độ ẩm), lắp đặt các hệ thống chống sét cho khu vực, tòa nhà đặt thiết bị.
6. Quy định về dự phòng thiết bị:
7. Các thiết bị, hệ thống công nghệ quan trọng của hệ thống của tập đoàn Công Ty X phải được trang bị thiết bị dự phòng (thiết bị dự trữ sằn sàng hoạt động trong trường hợp thiết bị chính có sự cố) nhằm đảm bảo sự liên tục của hoạt động trong trường hợp xảy ra sự cố như mất điện.
8. Các thiết bị dự phòng phải được kiểm tra định kỳ hàng tuần/tháng/năm nhằm đảm bảo sự sẵn sàng và giảm thiểu các nguy cơ gây hỏng thiết bị.
9. Phải có quy trình vận hành các thiết bị dự phòng, khuyến khích cấu hình hoạt động ở chế độ dự phòng nóng (thiết bị dự phòng tự động thay thế thiết bị chính khi xảy ra sự cố đối với thiết bị chính)
10. Quy định an toàn dây cáp:
11. Các đường dây cáp điện, cáp mạng kết nối các thiết bị, hệ thống công nghệ phải được bảo vệ theo phương thức phù hợp (đặt ngầm hoặc bọc ngoài) nhằm đề phòng nguy cơ hỏng, mất kết nối hoặc truy cập trái phép.
12. Việc thiết kế đi cáp trong các tủ rack phải đảm bảo mỹ quan, thuận tiện trong việc tháo lắp thiết bị. Các dây cáp điện và viễn thông phải được bó gọn gàng, vừa đảm bảo tính mỹ quan, vừa đảm bảo an toàn và tính sẵn sàng cho các thiết bị.
13. Cáp điện và cáp mạng phải được đặt tách biệt để chống nhiễu điện từ.
14. Việc đánh mã dây cáp phải có quy định theo tiêu chuẩn nhằm giảm thiểu các lỗi đấu sai đường cáp mạng khi sửa chữa lắp đặt.
15. Quy định sửa chữa, bảo trì thiết bị:
16. Hệ thống công nghệ của tập đoàn Công Ty X phải được bảo trì tối thiều một năm một lần hoặc theo yêu cầu tiêu chuẩn của nhà cung cấp thiết bị/dịch vụ.
17. Chỉ những đối tác đã được phê duyệt mới được phép sửa chữa, bảo trì các thiết bị, hệ thống của Công Ty X.
18. Các thông tin về sửa chữa, bảo trì thiết bị, hệ thống công nghệ của Công Ty X phải được ghi nhận lại thành văn bản cụ thể.
19. Các thông tin Mật/ Tuyệt mật trong thiết bị phải được xóa sạch, hủy bỏ hoặc mã hóa bằng phương thức an toàn trước khi tiến hành bảo trì. Trong trường hợp nếu không thể xóa/hủy bỏ các dữ liệu này cần yêu cầu nhà cung cấp ký cam kết bảo mật không được tiết lộ và bảo vệ dữ liệu của hệ thống Công Ty X .
20. Nhân viên quản trị hệ thống hoặc đối tác phải đăng xuất (log off) khỏi máy tính, máy chủ khi làm việc xong.

**Điều 13. Quy định vận hành hệ thống**

1. Vận hành hệ thống CNTT phải được thực hiện theo qui trình để đảm bảo ATTT, tính sẵn sàng cho hệ thống. Các thay đổi phải được đánh giá ảnh hưởng đến các hệ thống liên quan và được phê duyệt trước khi thực hiện. Các sự kiện, log của tất cả các hệ thống phải được ghi nhận, quản lý giám sát chặt chẽ. Dữ liệu của hệ thống trong tập đoàn Công Ty X phải được sao lưu định kỳ. Năng lực của hệ thống phải được theo dõi, báo cáo định kỳ đảm bảo tính sẵn sàng cho các hệ thống.
2. Quy trình hóa các thủ tục vận hành:

Ban ISO có trách nhiệm:

1. Ban hành các quy trình vận hành hệ thống thông tin và triển khai các quy trình đến toàn bộ đối tượng tham gia vận hành và giám sát tuân thủ.
2. Tổ chức rà soát, cập nhật, bổ sung các quy trình vận hành tối thiểu mỗi năm một lần.
3. Quản lý sự thay đổi
4. Ban An ninh mạng phải xây dựng quy trình quản lý thay đồi công nghệ nhằm kiểm soát chặt chẽ những thay đổi cấu hình, nâng cấp hệ thống, ứng dụng.
5. Mọi thay đổi phải được đánh giá ảnh hưởng đến hệ thống có liên quan và được phê duyệt bởi các cấp có thẩm quyền trước khi thực hiện. Trước khi thực hiện phải có thông báo chi tiết các thay đổi cho các cá nhân và các phòng ban liên quan.
6. Tất cả mọi sự thay đổi đều phải được ghi lại chi tiết bằng các công cụ để phục vụ công tác kiểm tra hoặc kiểm toán hoạt động của hệ thống.
7. Phải tách biệt việc phát triển hệ thống với việc vận hành hệ thống. Mọi sự thay đổi lên hệ thống thật phải được thực hiện bởi nhân viên vận hành hệ thống. Nhân viên và chuyên gia phát triển phần mềm không được trực tiếp vận hành, nâng cấp và sửa chữa trên hệ thống thật.
8. Nhật ký và giám sát hệ thống
9. Tất cả các sự kiện liên quan đến ATTT đều phải được ghi lại trong nhật ký hoặc hệ thống ghi nhật ký (log). Nhật ký đánh giá cần bao gồm: ID người dùng; thời gian đãng nhập và thoát ra; những truy cập thành công và bị từ chối; dữ liệu truy cập thành công và bị từ chối; những lần truy cập các nguồn tài nguyên; các thay đổi về cấu hình hệ thống; sao lưu dữ liệu; sử dụng tài khoản đặc quyền; file được truy cập và loại truy cập; địa chỉ và giao thức mạng; các cảnh báo.
10. Nhật ký phải được thu thập ở dạng gốc, dung lượng bộ nhớ dành cho việc lưu trữ nhật ký phải được giám sát và đảm bảo phù hợp với yêu cầu thời gian theo quy định.
11. Khối Công nghệ phải giám sát hoạt động của Nhân viên quản trị vận hành hệ thống và người dùng hàng ngày, bao gồm:

* Truy cập được phép: ID người dùng, các sự kiện, thời gian của các sự kiện, các file được truy cập, các chương trình/ tiện ích được sử dụng.
* Các hoạt động được ưu tiên: Sử dụng tài khoản ưu tiên, khởi động/ dừng hệ thống, cắm/tháo thiết bị.
* Các nỗ lực truy cập trái phép: Các hành động bị lỗi hoặc bị từ chối của người dùng, liên quan đến dữ liệu và các nguồn tài nguyên, các vi phạm chính sách truy cập, các cảnh báo từ hệ thống phát hiện xâm nhập.
* Các cảnh báo hoặc lỗi hệ thống.
* Những thay đổi các cài đặt và biện pháp quản lý an toàn hệ thống.
* Nhật ký của người quản trị vận hành: Thời gian xảy ra sự kiện, thông tin sự kiện hoặc sự cố, tài khoản quản trị vận hành, các hoạt động phải thực hiện

1. Các lỗi được thông báo bởi người dùng hoặc các chương trình hệ thống liên quan đến các hệ thống thông tin phải được ghi nhận, xem xét và có các biện pháp xử lý lỗi.
2. Các chức năng ghi nhật ký và thông tin nhật ký phải được bảo vệ, không được truy cập trái phép, giả mạo, xóa hay sửa đổi nhật ký hệ thống.
3. Thời gian trên toàn hệ thống phải được đồng bộ với nhau và với nguồn thời gian chuẩn.
4. Sao lưu và phục hồi dữ liệu
5. Ban ANM có trách nhiệm xây dựng và ban hành Quy trình sao lưu và phục hồi dữ liệu.
6. Dữ liệu của Công ty phải được sao lưu định kỳ với tần suất, phương pháp sao lưu phụ thuộc vào từng hệ thống.
7. Các dữ liệu, thiết bị sao lưu phải được lưu trữ an toàn và được kiểm tra định kỳ đề đảm bảo luôn sẵn sàng khi cần sử dụng.
8. Định kỳ hai (02) tháng một lần thử nghiệm khôi phục dữ liệu sao lưu từ phương tiện lưu trữ nhằm đảm bảo dữ liệu sao lưu luôn sẵn sàng khi cần.
9. Các bản sao lưu của dữ liệu Mật/ Tuyệt mật phải được mã hóa.
10. Bảo mật máy chủ
11. Ban ANM chịu trách nhiệm xây dựng yêu cầu tham số cấu hình cho máy chủ nhằm đảo bảo các yêu cầu về ATTT.
12. Máy chủ trước khi đưa vào sừ dụng phải được cài đặt theo đúng yêu cầu tài liệu đưa ra và kiểm tra ATTT bởi đơn vị phụ trách về ATTT của hệ thống Công Ty X .
13. Quản lý bản vá lỗi hệ thống
14. Các hệ thống công nghệ, ứng dụng của Công Ty X phải được cập nhật các bản vá lỗi kịp thời.
15. Các bản vá lỗi bảo mật phải được áp dụng ngay sau khi được kiểm thử thành công, trong trường hợp áp dụng này làm ảnh hưởng các hoạt động cùa Công ty mà không thề thực hiện phải có các biện pháp giám sát phù hợp, giảm thiểu rủi ro.
16. Việc vá lỗi các hệ thống phải được ghi nhận chính xác, và phải được rà soát định kỳ.
17. Quản lý cấu hình tài sản vật lý
18. Ban ANM phải xây dựng các tiêu chuẩn tài sàn vật lý và định kỳ hàng năm tiến hành rà soát cập nhật tiêu chuẩn này.
19. Trước khi tiến hành đưa một hệ thống mới vào sử dụng, phải xây dựng cấu hình hệ thống chuẩn nhằm đáp ứng được yêu cầu về tải của hệ thống đối với hoạt động nghiệp vụ kinh doanh của đơn vị. Cấu hình này phải được lưu trữ và cập nhật mỗi khi có sự thay đổi.
20. Phải xây dựng các tiêu chuẩn cấu hình cho các thành phần trong hệ thống và áp dụng các tiêu chuẩn này cho các hệ thống trước khi đưa vào sử dụng. Cụ thể như sau:

* Các tham số cấu hình mặc định không sử dụng phải được tắt (disable) hoặc gỡ bỏ (remove).
* Phải thay đổi các thông tin mặc định của hãng trước khi đưa vào vận hành, bao gồm nhưng không giới hạn: mật khẩu, khóa mặc định, tên tài khoản.
* Khi có nhu cầu sử dụng, tùy vào chức năng của từng hệ thống, nhân viên quản trị hệ thống liệt kê các thành phần cần sử dụng và xin phê duyệt của cấp có thẩm quyền.
* Không sử dụng các thành phần chưa đáp ứng các yêu cầu ATTT, trong trường hợp phải kích hoạt các thành phần này đề phục vụ nghiệp vụ kinh doanh hoặc do hạn chế kỹ thuật của hệ thống phải có các biện pháp bổ trợ để nâng o mức độ bảo mật và phải được phê duyệt của cấp có thẩm quyền.
* Cấu hình các tham số trên các hệ thống phải được sao lưu định kỳ, mã hóa và lưu trữ ở nơi an toàn để khôi phục trạng thái của hệ thống khi cần thiết.

**Điều 14. Quy định quản lý truy cập**

1. Tất cả các truy cập vào hệ thống của Công Ty X phải được quản lý chặt chẽ, thực hiện theo quy trình để đảm bảo ATTT cho hệ thống. Quyền truy cập vào hệ thống phải được bộ phận phụ trách ATTT thẩm định và được phê duyệt của các cấp có thẩm quyền.
2. Quản lý phân quyền:
3. Mỗi người dùng trong hệ thống Công Ty X được cấp quyền truy cập và chỉ sử dụng đúng quyền đã được phê duyệt theo chức năng, nhiệm vụ được giao. Các trường hợp vi phạm sử dụng không đúng quyền được phê duyệt phải được xử lý theo quy định.
4. Ban ANM có trách nhiệm xây dựng và ban hành quy trình cho việc đăng ký, cấp phát, hủy bỏ và thu hồi quyền truy cập trên tất cả các hệ thống và dịch vụ thông tin.
5. Phải giới hạn và kiểm soát việc cấp phát và sử dụng các đặc quyền bằng văn bản hoặc các biện pháp kỹ thuật (nếu có) đối với mỗi hệ thống. Cụ thể như sau:

* Đảm bảo tính duy nhất.
* Phân quyền theo đúng chức năng, nhiệm vụ.
* Mọi truy cập của người dùng vào hệ thống của Công Ty X phải được phân quyền và quản lý.
* Mọi truy cập đến các hệ thống đều phải xác thực, tùy vào mức độ quan trọng để sử dụng biện pháp xác thực username/password. Việc sử dụng biện pháp xác thực phải được lãnh đạo đơn vị phụ trách về ATTT phê duyệt.
* Các hệ thống kiểm soát truy cập phải được thiết lập mặc định chặn tất cả, chỉ cho phép truy cập đủ để thực hiện công việc.

1. Quyền truy cập tới các thành phần hệ thống của người dùng phải được rà soát, phân loại, giới hạn dựa trên mục đích công việc của các đối tượng đó. Định kỳ 06 (sáu) tháng, đơn vị phụ trách về ATTT chịu trách nhiệm phối hợp với các phòng ban liên quan rà soát đối chiếu lại danh sách tài khoản và quyền truy cập của người dùng và 03 (ba) tháng đối với tài khoản đặc quyền đảm bảo phù hợp với tình hình thực tế.
2. Quá trình đăng nhập của người dùng vào hệ thống Công Ty X phải đáp ứng các yêu cầu bảo mật như sau:

* Tự ngắt kết nối của các phiên truy cập và yêu cầu người dùng xác thực lại sau tối đa 15 phút không sử dụng và có thể được thiết lập khác tùy vào yêu cầu, mức độ quan trọng của các hệ thống, ứng dụng cụ thể.
* Hệ thống hiển thị cảnh báo chỉ những người dùng được cấp phép mới được truy cập.
* Không hiển thị mật khẩu lúc đăng nhập dưới dạng văn bản gốc (clear-text).
* Mật khẩu truyền giữa các hệ thống phải được mã hóa theo qui định mã hóa mật khẩu của Công Ty X .
* Tại một thời điểm chỉ cho phép một phiên đăng nhập trên một tài khoản.
* Thời gian truy cập trong ngày phải được giới hạn tùy theo mục đích công việc của người dùng.

1. Quy định về tài khoản và mật khẩu:
2. Người dùng các hệ thống của Công Ty X phải tuân thủ các quy tắc về sử dụng và quản lý tài khoản, cụ thể như sau:

* Người dùng phải chịu trách nhiệm bảo mật tài khoản, mật khẩu, không lưu trữ trên thiết bị cá nhân, file máy tính, ghi ra giấy.... Người dùng phải thay đồi mật khẩu truy cập hệ thống tối đa sau 60 ngày. Sau 60 ngày, nếu người dùng không thay đổi mật khẩu theo quy định mật khẩu sẽ bị vô hiệu hóa hoặc bị xóa bỏ.
* Mật khẩu người dùng, mật khẩu tài khoản truy cập hệ thống phải là mật khẩu mạnh, đáp ứng yêu cầu: Chiều dài tối thiểu 08 (tám) ký tự, có đủ 03 (ba) trong 04 (bốn) yếu tố bảo mật mật khẩu (chữ thường, chữ hoa, chữ số và ký tự đặc biệt). Các trường hợp khác cần phải có sự phê duyệt cùa cấp có thẩm quyền.
* Mật khẩu quản trị hệ thống (vận hành dịch vụ) phải đáp ứng yêu cầu: Chiều dài tối thiếu 12 (mười hai) ký tự, có đầy đủ 04 (bốn) yếu tố bảo mật mật khẩu (chữ thường, chữ hoa, chữ số và ký tự đặc biệt). KHÔNG được dùng bất cứ ký tự nào thông dụng như: admin, password hay tên người dùng.
* Người dùng phải đổi mật khẩu ngay trong lần truy cập đầu tiên hoặc ngay khi nghi ngờ mật khẩu có khả năng bị lộ.
* Mật khẩu mới không được trùng với 03 (ba) mật khẩu đã được sử dụng gần nhất trước đó.
* Mật khẩu mặc định của nhà cung cấp phải được thay đổi ngay trong quá trình cài đặt.
* Không sử dụng cùng một mật khẩu cho nhiều tài khoản khác nhau (tài khoản đăng nhập máy tính, tài khoản truy cập ứng dụng.).
* Nghiêm cấm chia sẻ mật khẩu hoặc các yếu tố xác thực khác (token) với các cá nhân khác. Nhân viên quản trị phải kiểm tra, xác minh danh tính người sử dụng trước khi cung cấp, đổi mật khẩu hoặc giải khóa tài khoản. Ngay sau khi nhận được mật khẩu mới từ ban ANM người dùng phải tiến hành đổi mật khẩu.

1. Tài khoản quản trị, dịch vụ và vận hành không được dùng chung với tài khoản người dùng.
2. Mật khẩu của tài khoản quản trị o nhất của hệ thống phải được quản lý, theo dõi bảo đảm việc sử dụng, lưu trữ mật khẩu này được an toàn, cấp phát và quản lý mật khẩu đặc quyền các hệ thống của Công Ty X bằng các biện pháp:

* Chỉ có 02 người có trách nhiệm quản trị hệ thống được biết;
* Phải có hệ thống lưu nhật ký để biết được ai là người sử dụng tài khoản quản trị o nhất đăng nhập vào hệ thống tại một thời điểm xác định.

1. Quy định về truy cập hệ thống mạng

Tất cả các truy cập vào hệ thống mạng của Công Ty X đều phải được sự đồng ý và phê duyệt của các cấp có thẩm quyền, cụ thể như sau:

1. Không được phép kết nối trực tiếp giữa các vùng mạng bên ngoài và các vùng mạng nội bộ của hệ thống Công Ty X , mà phải thực hiện qua vùng mạng trung gian.
2. Hệ thống mạng phải được phân chia thành các phân vùng khác nhau dựa trên mức độ rủi ro. Truy cập giữa các vùng mạng phải được kiểm soát bằng thiết bị tường lửa, tùy thuộc vào mức độ quan trọng sẽ áp dụng thêm các biện pháp bảo mật cần thiết khác.
3. Các thiết bị đầu cuối phải tuân thủ quy định ATTT cho thiết bị đầu cuối của Công Ty X mới được phép truy cập vào hệ thống mạng nội bộ của Công Ty X .
4. Phải cách ly các hệ thống quan trọng với môi trường bình thường.
5. Kiểm soát truy cập từ xa:
6. Truy cập từ xa của người dùng, đối tác kết nối đến hệ thống mạng của Công Ty X phải được sự đồng ý và phê duyệt của cấp có thẩm quyền. Truy cập từ xa vào hệ thống mạng nội bộ của Công Ty X phải được thực hiện trên kênh mã hóa và sử dụng các biện pháp xác thực mạnh.
7. Các thiết bị đầu cuối truy cập từ xa phải đảm bảo ATTT mới được phép truy cập từ xa vào hệ thống mạng của Công Ty X .
8. Kiểm soát truy cập vận hành và quản trị hệ thống:
9. Nhân viên quản trị và vận hành hệ thống phải sử dụng máy tính độc lập riêng biệt chỉ kết nối duy nhất tới các hệ thống cần vận hành và quản trị.
10. Yêu cầu khi đăng nhập thực hiện việc vận hành, quản trị viên hệ thống phải xác thực bằng mật khẩu theo quy định, khuyến khích dùng các phương pháp xác thực mạnh 2 yếu tố để chứng minh danh tính. Xác thực 2 yếu tố là sự kết hợp những thông tin mà người dùng biết (số PIN, mật khẩu) cùng với những gì mà người dùng có (Smartrd, USB, Token, Grid rd...).
11. Khu vực đặt các máy để truy cập quản trị, vận hành hệ thống phải được cách ly, kiểm soát truy cập chặt chẽ. Cán bộ truy cập vào khu vực này phải được phê duyệt và phải xác thực bằng thẻ từ và vân tay. Mọi hành động thực hiện trên máy chủ quản trị cần được ghi hình và lưu trữ làm bằng chứng.

**Điều 15. Quy định quản lý mã hóa**

1. Các thông tin Mật/Tuyệt mật phải được áp dụng các biện pháp mã hóa phù hợp khi được lưu trữ trên các hệ thống, truyền nhận dưới dạng điện từ hay sao chép sang phương tiện lưu trữ cầm tay. Các khóa mà hóa phải được áp dụng các biện pháp bảo vệ để đảm bảo tính duy nhất và bí mật.
2. Lãnh đạo ban ANM chịu trách nhiệm phê duyệt lựa chọn phương pháp mã hóa đáp ứng các yêu cầu trên, dựa trên nghiên cứu, đánh giá các chuẩn mã hóa quốc gia, quốc tế.
3. Các thuật toán mã hóa sử dụng phải đảm bảo là các thuật toán mạnh (chưa bị tấn công khai thác) và đáp ứng các yêu cầu của cơ quan Nhà nước hoặc các tiêu chuẩn quốc tế, cụ thể là: AES 256, RSA. SHA-1, SHA-2, SHA-3 hoặc các thuật toán có độ bảo mật o hơn.
4. Việc quản lý khóa mã hóa phải đảm bảo các yêu cầu sau:
5. Các khóa sử dụng để mã hóa dữ liệu khi được khởi tạo phải đảm bảo tính duy nhất và độ mạnh, phải được bảo vệ để không bị mất, thay đổi, hoặc phá hoại trái phép. Thiết bị sinh và chứa khóa mà hóa phải được bảo vệ an toàn cả về mặt vật lý.
6. Khóa sử dung để mã hóa nếu được lưu giữ trên hệ thống phải được lưu trữ dưới định dạng mã hóa. Mật khẩu dùng để mã hóa khóa mã hóa (mật khẩu mã hóa) phải được bảo vệ khỏi bị tiết lộ và sử dụng sai mục đích.
7. Dữ liệu mã hóa, khóa sử dụng để mã hóa và mật khẩu mã hóa phải được lưu trữ tại những vị trí tách biệt.
8. Xây dựng các quy trình thực hiện, trong đó đảm bảo bao gồm các nội dung: khởi tạo khóa, phân phối khóa, lưu giữ, tần suất thay đổi, hủy bỏ các khóa cũ, ngăn ngừa truy cập và thay đổi khóa, thay thế các khóa bị lộ hoặc nghi ngờ bị xâm phạm, thu hồi các khóa cũ hoặc hết giá trị sử dụng.

**Điều 16. Quy định xây dụng, phát triển và duy trì hệ thống**

1. Các hệ thống mới khi xây dựng và phát triển hoặc thuê của nhà cung cấp bên ngoài đều phải đáp ứng các yêu cầu ATTT, phải được đánh giá kiểm thử về ATTT và được phê duyệt các cấp có thẩm quyền trước khi đưa vào sử dụng.
2. Khối Công nghệ có trách nhiệm xây dựng và ban hành quy trình đánh giá ATTT đối với một hệ thống trước khi đưa vào sừ dụng, đánh giá trong quá trình sử dụng, và theo dõi đến khi hệ thống hết thời hạn sử dụng.
3. Yêu cầu bảo mật đối với các hệ thống Công Ty X :
4. Khi xây dựng hệ thống mới hoặc nâng cấp hệ thống thông tin hiện tại phải đáp ứng những yêu cầu ATTT, và có sự xác nhận của Ban ANM trước khi đưa vào sử dụng.
5. Các yêu cầu về ATTT và các biện pháp kiểm soát phải được đưa vào và thực hiện ngay từ giai đoạn đầu triển khai của dự án công nghệ.
6. Việc đưa các công nghệ mới vào sử dụng phải được tài liệu hóa bằng quy định/quy trình chấp nhận sử dụng.
7. Khi xây dựng mới hay nâng cấp một hệ thống thông tin, các tài liệu yêu cầu của hệ thống phải đặc tả rõ các yêu cầu về việc kiểm soát an toàn thông tin.
8. Trong quá trình xây dựng, phát triển hệ thống CNTT và phần mềm: cần xây dựng các quy trình và phải tuân thủ chặt chẽ các quy trình này để đảm bảo chất lượng cũng như kiểm soát các vấn đề an toàn thông tin.
9. Khi thuê các đối tác bên ngoài phát triển phần mềm phải đảm bảo đối tác áp dụng các tiêu chuẩn, quy trình về chất luợng cũng như an toàn thông tin đáp ứng yêu cầu của Công Ty X .
10. Kiểm soát nhập liệu và xử lý dữ liệu:
11. Dữ liệu nhập vào các hệ thống ứng dụng phải tuân theo các tiêu chuẩn chung, kiểm tra độc lập bởi người thứ hai nhằm đảm bảo các dữ liệu này chính xác và phù hợp (validated). Các nội dung, dữ liệu này cần có biện pháp rà soát, đảm bảo tính toàn vẹn và chính xác.
12. Phải có các biện pháp kiểm soát phù hợp cả bên trong các ứng dụng để phát hiện những sai lệch thông tin do lỗi của quá trình xử lý thông tin hoặc do hoạt động phá hoại hoặc các hoạt động gian lận có chủ ý.
13. Kiểm tra tính hợp lệ dữ liệu đầu ra: Dữ liệu kết xuất từ một ứng dụng phải được kiểm tra tính hợp lệ để đảm bảo quá trình xử lý thông tin chính xác và thích hợp.
14. Việc kiểm tra tính hợp lệ của thông tin phải được tiến hành, kết hợp trong nhiều ứng dụng/module khác nhau nhằm phát hiện các thông tin sai lệch do các lỗi trong quá trình xử lý hoặc các hành vi có chủ ý.
15. Phải thực hiện đánh giá rủi ro đối với việc xử lý thông tin và dữ liệu trong các ứng dụng nhằm đảm bảo tính xác thực và toàn vẹn của thông tin.
16. Toàn vẹn dữ liệu
17. Phải xác định và thực hiện các biện pháp kiểm soát thích hợp để đảm bảo tính xác thực và toàn vẹn của thông điệp trong ứng dụng.
18. Việc rà quét điểm yếu kỹ thuật, kiểm thử và kiểm tra ATTT trong hệ thống phải được thực hiện định kỳ hoặc sau khi có những thay đổi trên hệ thống nhằm phát hiện và xử lý các điểm yếu nếu tồn tại.
19. Dựa trên đánh giá rủi ro của các điểm yếu, phải thực hiện phân loại mức độ và xác định thời gian xử lý, phản ứng với các mức độ đó.
20. Việc thực hiện vá các điểm yếu phải tuân thủ các chỉ dẫn về quản lý bản vá.
21. Quy định ATTT trong các quá trình phát triển và hỗ trợ hệ thống:
22. Quy trình kiểm soát thay đổi: Phải có quy trình kiểm soát thay đổi để quản lý việc thực hiện thay đổi trên các hệ thống và phần mềm ứng dụng.
23. Rà soát các ứng dụng sau khi thay đổi hệ điều hành: Khi thay đổi hệ điều hành, cần phải rà soát và kiểm tra lại hoạt động của tất cà các ứng dụng nghiệp vụ để đảm bảo không ảnh hưởng tới hoạt động và tính bảo mật.
24. Hạn chế các thay đổi tới các gói phần mềm: Phải hạn chế việc thay đổi các gói phần mềm cài đặt, chỉ cho phép các thay đổi cần thiết và phải đảm bảo tất cả những thay đổi đều được kiểm soát chặt chè.
25. Kiểm soát truy cập tới mã nguồn chương trình: Phải thực hiện phân quyền đề thực hiện đúng việc truy cập và n thiệp vào mã nguồn của ứng dụng.
26. Thuê dịch vụ ngoài (outsourcing) phát triển phần mềm: Phải theo dõi và giám sát chặt chẽ việc phát triển tất cả các phần mềm mà CÔNG TY X thuê tổ chức bên ngoài thực hiện.
27. Phát triển, kiểm thử và vận hành.
28. Các môi trường phát triển, kiểm thử và môi trường thật (môi trường vận hành) phải được tách biệt nhằm giảm thiểu rủi ro từ truy cập hay thay đổi trái phép.
29. Môi trường kiểm thử phải được xây dựng đảm bảo mô phỏng môi trường vận hành đầy đủ nhất có thề.
30. Không được phép sao chép các dữ liệu Mật/Tuyệt Mật vào môi trường kiểm thử (test). Các dữ liệu Mật/Tuyệt Mật trên môi trường vận hành (Production/Live) phải được mã hóa (masking) trước khi đưa vào môi trường kiểm thử để thực hiện kiểm thử.
31. Bảo vệ dữ liệu kiểm thử: Dữ liệu dùng cho hoạt động kiểm thử phải được lựa chọn phù hợp, được bảo vệ và kiểm soát chặt chẽ, đảm bảo không bị rò rỉ thông tin.
32. Tất cả tài khoản và dữ liệu kiểm thử phải được gỡ bỏ khỏi môi trường phát triển, kiểm thử trước khi đưa vào môi trường vận hành.
33. Phân tách rõ trách nhiệm/quyền hạn của cán bộ kiểm thử/phát triển và cán bộ vận hành. Đảm bảo các cán bộ phát triển/kiểm thử không được phép truy nhập môi trường vận hành và ngược lại, các cán bộ vận hành không được phép truy nhập môi trường phát triển/kiểm thử.
34. Các môi trường phát triển/kiểm thử được lấy từ môi trường vận hành (Production) phải được đơn vị phụ trách ATTT đánh giá và phê duyệt trước khi đưa vào môi trường phát triển/ kiểm thừ.

**Điều 17. Kế hoạch dự phòng đảm bảo hoạt động liên tục**

1. Kế hoạch liên tục kinh doanh (BCP) phải được xây dựng, đào tạo, Công Ty X trong trường hợp xảy ra thảm họa.
2. Công tác đảm bảo hoạt động liên tục (BCP) phải bao gồm tất cả các hoạt động của các hệ thống CNTT quan trọng và hoạt động của bộ phận nghiệp vụ tối thiểu cần có để duy trì hoạt động bình thường của hệ thống.
3. Kế hoạch đảm bảo tính liên tục kinh doanh (BCP) cần được định kỳ diễn tập hàng năm để đảm bảo sẽ triền khai thành công trong tình huống khẩn cấp. Kế hoạch đảm bảo tính liên tục kinh doanh phải được định kỳ xem xét, cập nhật cho phù hợp với những thay đổi của hệ thống.
4. Tất cả các nhân viên phải được đào tạo về kế hoạch đảm bảo liên tục kinh doanh và vai trò, trách nhiệm của họ trong kế hoạch.
5. Xây dựng các quy trình, quy định, hướng dẫn đảm bảo hoạt động liên tục kinh doanh cho các nghiệp vụ liên quan của Công Ty X .
6. Công tác dự phòng thảm họa phải đáp ứng những yêu cầu sau:
7. Phải xây dựng hệ thống dự phòng cho các hệ thống CNTT trọng yếu của Công ty  
   cách hệ thống chính tối thiểu 30 km tính theo đường thẳng nối giữa hai hệ thống.
8. Trong trường hợp có sự cố/thảm họa thì toàn bộ các hoạt động công nghệ bị ảnh hưởng phải được chuyển sang hệ thống dự phòng một cách nhanh nhất (đặc biệt ưu tiên đổi với các ứng dụng cốt lõi).
9. Kịch bản chuyển đổi dịch vụ công nghệ từ hệ thống chính sang hệ thống dự phòng phải được diễn tập định kỳ. Tần suất thực hiện diễn tập do cấp có thẩm quyền quy định cụ thể đối với từng hệ thống đề đảm bảo tính sẵn sàng.

**Điều 18. Quản lý sự cố ATTT**

1. Các sự cố ATTT phải được thông báo và phát hiện kịp thời để đưa ra các biện pháp khắc phục, hạn chế các ảnh hưởng đến hoạt động của hệ thống thông tin. Đối với các sự cố ảnh hưởng lớn phải thành lập nhóm phản ứng sự cố để theo dõi, xử lý và báo cáo kịp thời trong quá trình xử lý sự cố.
2. Tất cả cán bộ nhân viên có trách nhiệm thông báo cho đơn vị phụ trách ATTT ngay khi phát hiện các sự cố an ninh thông tin liên quan đến hệ thống thông tin của Công Ty X .
3. Đơn vị phụ trách ATTT có trách nhiệm ghi nhận và kiểm chứng lại các sự kiện được thông báo, đánh giá mức độ ảnh hường và phối hợp với các bộ phận chủ quản hệ thống đưa ra các biện pháp khắc phục kịp thời. Phải thiết lập trách nhiệm và quy trình quản lý để đảm bảo các sự cố ATTT được khắc phục nhanh chóng, hiệu quả.
4. Khi xảy ra các sự cố an ninh thông tin nghiêm trọng, liên quan tới pháp luật, các bằng chứng vi phạm cần được thu thập, lưu giữ và cung cấp cho các bộ phận xử lý liên quan.
5. Tùy theo mức độ sự cố, phải thành lập nhóm phản ứng sự cố thực hiện các nhiệm vụ như sau:

* Kịp thời xử lý các sự cố an ninh thông tin.
* Tiếp tục theo dõi, giám sát hệ thống sau khi xử lý sự cố cho đến khi khẳng định sự cố đã được giải quyết triệt để.
* Xác định và áp dụng biện pháp phòng ngừa hiệu quả nhất đối với mỗi sự cố an toàn thông tin.
* Nhóm ứng cứu sự cố có trách nhiệm báo cáo về việc xử lý và phòng ngừa sự cố tới các cấp lãnh đạo tùy theo mức độ nghiêm trọng của sự cố.

1. Sau khi khắc phục sự cố, các điểm yếu ATTT liên quan đến sự cố phải được xem xét, phân tích để có các hành động khắc phục kịp thời và rút ra bài học kinh nghiệm.
2. Việc theo dõi, quản lý và xử lý các sự cố an ninh thông tin cần được xây dựng thành cơ sở dữ liệu. Cơ sở dữ liệu này phải được tra cứu và cập nhật mỗi khi xảy ra sự cố an ninh thông tin tham chiếu quy trình xử lý sự cố của trung tâm giám sát.

**Điều 19. Quy định đối với nhân sự tham gia hệ thống**

1. Tất cả các nhân sự tham gia hệ thống Công Ty X phải có trách nhiệm tuân thủ theo cam kết với Quy chế ATTT nhằm đảm bảo việc sử dụng và bảo vệ hệ thống Công Ty X tại Công ty một cách hiệu quả và đúng mục đích. Tất cả các người dùng cần nhận thức rằng, mọi sự vi phạm quy định này có thể gây tác hại nghiệm trọng cho hoạt động của công ty, đồng thời người dùng phải chịu trách nhiệm với mọi hậu quả do việc vi phạm Quy chế ATTT gây ra.
2. Quy định tài khoản cá nhân và mật khẩu
3. Mỗi nhân viên của Công Ty X được tạo một tài khoản (account) với mật khẩu riêng và duy nhất.
4. Mỗi nhân viên có trách nhiệm bảo quản tài khoản và mật khẩu của mình, thay đổi mật khẩu định kỳ theo yêu cầu về bảo mật. Tuyệt đối không trao đổi, sử dụng chung tài khoản và mật khẩu.
5. Khi có yêu cầu khởi tạo/sửa/xóa tài khoản máy tính và tài khoản email cho các nhân viên mới, bộ phận HR tạo yêu cầu gửi đến khối Công nghệ.
6. Để tránh nhiễm và lây lan Virus và Spyware, người dùng sẽ không được cấp tài khoản administrator của máy tính để bàn cá nhân. Trừ một số trường hợp đặc biệt được sự phê duyệt của cấp có thẩm quyền.
7. Quy định “Clear Desk” và “Clear Screen”
8. Quy định “Clear Desk”:

* Thông tin Mật/ Tuyệt mật lưu trữ dưới dạng văn bản hay trong các thiết bị lưu trữ di động đều phải được cất giữ trong tủ có khóa vật lý, phòng tránh truy cập trái phép. Không đặt các thông tin Mật/ Tuyệt mặt trên mặt bàn.
* Cuối giờ làm việc, cán bộ nhân viên phải cất tài liệu được phân loại từ nội bộ trở lên vào ngăn kéo, tủ và khóa lại.
* Tất cả các tài liệu Mật/Tuyệt Mật khi được in, copy hoặc truyền nhận fax phải được kiếm soát, thu hồi ngay sau khi thực hiện xong.

1. Quy định “Clear Screen”:

* Các máy tính của Công Ty X phải được áp dụng chế độ tự động khóa màn hình, người dùng phải khóa máy ngay trước khi rời khỏi bàn làm việc và tắt máy khi không còn làm việc nữa.
* Không lưu các file văn bản có thông tin Mật/ Tuyệt mật (dạng word, excel ...) trên màn hình desktop.
* Nhân viên Công Ty X phải thoát khỏi phiên đăng nhập (log off) ngay sau khi sừ dụng xong máy tính dùng chung (máy được sử dụng cho việc in ấn, sn, chia sẻ dữ liệu chung...).
* Xóa sạch nội dung trên bảng phòng họp khi cuộc họp kết thúc và rời khỏi phòng họp. Việc sử dụng các phương tiện công nghệ dùng để sao chép dữ liệu như máy photocopy, máy quét snners, máy in, mera phải được kiểm soát chặt chẽ.

1. Quy định sử dụng thiết bị phần cứng
2. Sử dụng thiết bị đúng mục đích và yêu cầu công việc. Không lạm dụng các thiết bị công ty cấp phát vào công việc riêng tư. Tuân thủ tất cả các chính sách kiểm soát An ninh của công ty được cài đặt trên các thiết bị được cấp phát.
3. Việc cài đặt, cấu hình, thay đổi sẽ được thực hiện bởi Ban ANM. Người dùng không tự ý cài đặt, cấu hình lại hay thay đổi các thiết bị.
4. Máy laptop do công ty cấp được quản lý như máy để bàn (PCs) của công ty. Quyền Administrator trên các thiết bị này đều được thu hồi và tất cả các phần mềm ứng dụng sẽ do ban ANM cài đặt và cấu hình.
5. Người dùng không được phép kết nối thiết bị/máy tính của cá nhân vào mạng của Công Ty X , trừ kết nối wifi để truy cập trực tiếp ra Internet.
6. Các thiết bị sao lưu như USB, MP3 player không được phép kết nối vào các thiết bị của công ty khi chưa đăng ký và được phê duyệt cho phép sử dụng.
7. Tất cả user có trách nhiệm bảo quản và vệ sinh máy tính, các thiết bị IT mà mình sử dụng. Các trưởng bộ phận có trách nhiệm nhắc nhở nhân viên trong bộ phận mình bảo quản tốt các thiết bị thuộc bộ phận mình. Người dùng có trách nhiệm thanh toán chi phí sửa chữa (nếu có) đối với các trường hợp hỏng hóc thiết bị do công ty cấp gây ra do lỗi sử dụng của người sử dụng đó.
8. Mọi sự cố phần cứng (cũng như phần mềm) cần được thông báo ngay cho Ban công nghệ.
9. Yêu cầu khi sử dụng máy tính Laptop:

* Tuân thủ các quy định quản lý và sử dụng máy tính cá nhân.
* Chỉ được sử dụng laptop là tài sản của Công Ty X hoặc của cá nhân khi được lãnh đạo phê duyệt cho công việc.
* Nghiêm cấm việc kết nối laptop không phải là tài sản của Công ty vào hệ thống mạng của Công Ty X .
* Nghiêm cấm kết nối với hệ thống mạng không dây khi đang kết nối vào hệ thống mạng LAN của Công Ty X .
* Nghiêm cấm sử dụng wifi, các thiết bị thu phát không dây có khả năng truyền dữ liệu kết nối vào mạng nội bộ của Công Ty X .
* Khi Laptop bị mất cắp hoặc hư hỏng không thể phục hồi lại trạng thái hoạt động bình thường phải thông báo ngay cho Ban công nghệ để có biện pháp kiểm soát phù hợp.

1. Quy định sử dụng mạng nội bộ

Khi sử dụng mạng nội bộ người dùng (User) phải tuân thủ các quy định sau:

1. Phải đăng xuất (log-out) hay khoá màn hình (lock screen) máy tính của mình khi rời khỏi máy.
2. Phải tắt máy tính của mình hoàn toàn (shutdown) trước khi ra về.
3. Về quản lý file, mỗi bộ phận có một folder/directory riêng với quyền truy cập phù hợp trên file server hoặc Microsoft Sharepoint Online. Dưới folder này, có một thư mục dùng chung cho bộ phận (thư mục common), người dùng thuộc bộ phận nên tự tạo các thư mục con theo mục đích của bộ phận trong thư mục common.
4. Chỉ sử dụng các thư mục trên server để lưu trữ thông tin dùng cho công việc chung.
5. Thường xuyên tổ chức lại các thư mục thuộc bộ phận của mình cho gọn gàng; Xoá file cũ hay không còn sử dụng.
6. Không được phép truy cập hay sử dụng account của người dùng khác. Không truy cập vào các thư mục, hay hệ thống mạng không thuộc thẩm quyền.
7. Quy định sử dụng Email
8. Người dùng không được phép sử dụng hệ thống Email tại Công Ty X cho các mục đích sau:

* Gửi/nhận các tài liệu, file bất hợp pháp, có nội dung chính trị, tôn giáo hoặc nội dụng không phù hợp thuần phong mỹ tục.
* Cung cấp các tài liệu, tin tức nội bộ của công ty ra ngoài khi không được phép của trường bộ phận.
* Nội dung Email là tài sản thuộc sở hữu của Công ty. Nghiêm cấm hành động xóa hết hòm thư.

1. Gửi danh sách địa chỉ thư (contact list group) của Công ty ra ngoài.
2. Sử dụng Email cho các mục đích cá nhân riêng tư.
3. Công ty được quyền kiểm tra và kiểm soát nội dung Email của tất cả các nhân viên trong công ty khi cần thiết.
4. Người dùng nên hạn chế việc gửi email tới danh bạ email chung (gửi cho tất cả mọi người) khi không cần thiết.
5. Không được gửi email với file đính kèm (Attachment) có kích thước lớn hơn 25MB.
6. Thường xuyên xoá các Email không cần thiết và backup email của mình, nhằm giảm kích thước lưu trữ trên server.
7. Không được mở các file đính kèm lạ, không rõ nguồn gốc hoặc những file đính kèm dưới dạng file có đuôi .exe,.pif. Trong những trường hợp nhận được email như vậy phải thông báo với Ban ANM để có biện pháp xử lý kịp thời.
8. Chịu trách nhiệm đảm bảo an toàn, an ninh thông tin khi sử dụng thư điện tử, không sử dụng thư điện tử để phát tán virus, spam, spyware, phishing....
9. Không được sử dụng các hộp thư điện tử cá nhân trên Internet hoặc của tổ chức khác cho mục đích công việc của Công Ty X .
10. Không được dùng thư điện từ Công Ty X để đăng ký, truy cập vào các diễn đàn, trang mạng, tồ chức ngoài internet.
11. Quy định sử dụng Internet
12. Hệ thống Internet phải được thiết lập mặc định chặn tất cả (deny-all), chỉ cho phép truy cập đủ để thực hiện công việc.
13. Nhân viên được phân quyền truy cập sử dụng Internet theo đúng đối tượng, yêu cầu và phạm vi công việc.
14. Nghiêm cấm những hành vi sừ dụng Internet sai mục đích gây nguy hại cho ATTT cùa hệ thống mạng Công Ty X bao gồm:

* Truy cập vào những trang web hoặc gửi các thông tin hình ảnh qua Internet có nội dung không phục vụ mục đích công việc.
* Thực hiện những hành động gây cản trở, phá hoại hoạt động của mạng Internet, thông qua Internet làm ảnh hưởng đến các hệ thống thông tin khác, hoặc xâm phạm đến quyền lợi, danh dự cá nhân khác.
* Sử dụng các công cụ phần mềm và các biện pháp kỹ thuật dưới mọi hình thức nhằm chiếm dụng băng thông đường truyền gây tắc nghẽn mạng.
* Cung cấp hoặc tìm cách sao chụp thông tin của Công Ty X cho bên thứ ba thông qua Internet khi chưa được sự phê duyệt của các cấp lãnh đạo có thẩm quyền.
* Thực hiện xâm nhập trái phép, tấn công vào các hệ thống, website trên Internet.
* Tải về các phần mềm độc hại, file định dạng lạ, chương trình không có bản quyền, virus ... làm ảnh hưởng tới an ninh hệ thống mạng cũng như rủi ro rò rỉ, mất mát thông tin Công Ty X .

1. Tất cả các website, trang thông tin điện từ cùa Công Ty X phải có tên miền thống nhất dưới dạng https://\*. Công Ty X.vn. Website, trang thông tin điện tử của Công Ty X phải cài đặt chứng chỉ số được chứng thực bởi bên thứ ba, được đánh giá ATTT, đáp ứng các tiêu chuẩn ATTT.
2. Phòng chống mã độc (virus, malware, spam, botnet...)
3. Ban ANM có trách nhiệm thiết lập các hệ thống công nghệ bảo mật nhằm ngăn chặn các nguy cơ lây lan và nhiễm các loại mã độc. Các hệ thống tối thiếu cần có như: Hệ thống phòng chống Virus, hệ thống tường lửa, hệ thống lọc virus và spam cho email.
4. Thiết bị khi phát hiện nhiễm virus, mã độc cần được cách ly hoàn toàn khỏi hệ thống Công Ty X .
5. Tất cả các máy tính cá nhân, máy chủ hệ thống phải được cài đặt chương trình bảo mật cho thiết bị đầu cuối và được thiết lập các quy tắc sau:

* Việc cập nhật mẫu nhận dạng virus (signature) mới phải được thực hiện qua một máy chủ tập trung sau đó phân phối cho các máy chủ, máy trạm còn lại trong hệ thống.
* Lưu nhật ký (log) virus để phục vụ quá trình điều tra và nghiên cứu
* Các nhân viên không được mở các thư điện tử lạ, các tệp tin đính kèm hoặc các liên kết trong thư lạ để tránh virus, mã độc.

1. Quy định sao lưu dữ liệu cá nhân
2. Ban công nghệ chịu trách nhiệm xây dựng và cung cấp hệ thống sao lưu dữ liệu cho các máy chủ trong công ty. Mọi dữ liệu lưu trữ trên các máy chủ của công ty đều được sao lưu định kỳ theo kế hoạch.
3. Người dùng tránh lưu trữ các dữ liệu, thông tin liên quan tới công việc trên ổ cứng của các máy tính. Các dữ liệu lưu trên các ổ cứng của các máy tính có thể dễ dàng bị mất khi có sự cố và không thể khôi phục.
4. Người dùng nên lưu trữ các dữ liệu và thông tin quan trọng lên các ổ đĩa và thư mục trên server theo quy định và phân quyền.
5. Quy định về chụp hình, ghi âm
6. Nghiêm cấm việc chụp ảnh, ghi hình, ghi âm đối với tất cả các đối tượng bao gồm nhân viên, khách hàng, đối tác và cá nhân khác khi không có sự cho phép của cấp có thẩm quyền của Công Ty X .
7. Các bản ghi hình ảnh, âm thanh nếu được phép thực hiện phải qua kiểm duyệt bởi cấp có thẩm quyền trước khi đưa ra ngoài.
8. Quy định sử dụng phần mềm ứng dụng
9. Tất cả các phần mềm và phần mềm ứng dụng, dữ liệu và phần mềm đang phát triển tại Công Ty X là tài sản cùa Công Ty X . Tất cả các người dùng, bao gồm cả các nhân viên quản trị vận hành CNTT và nhân viên phát triển phần mềm, không được phép sao chép và mang ra khỏi công ty dưới mọi hình thức.
10. Khi có nhu cầu bổ sung, nâng cấp phần mềm, cần thông qua Ban ANM để kiểm soát các rủi ro về ATTT trước khi tiến hành mua sắm.
11. Người dùng không được phép cài đặt bất cứ phần mềm nào (bao gồm cả các phần mềm, chương trình download từ Internet) nếu chưa được phép của quản trị hệ thống Công Ty X . Việc cài đặt các phần mềm không có bản quyền do người dùng tự thực hiện sẽ được xem như một vi phạm nghiêm trọng các quy định của Công Ty X .
12. Các sự cố với phần mềm phải được thông báo ngay cho ban ANM.

**Điều 20. Quy định tuân thủ**

1. Tài liệu ATTT của tập đoàn Công Ty X phải đảm bảo phù hợp và tuân thủ theo các yêu cầu pháp lý của Nhà nước Việt Nam cũng như tuân thủ theo các yêu cầu tiêu chuẩn kỹ thuật ngành.
2. Bộ phận phụ trách An ninh thông tin cần thường xuyên cập nhật các văn bản hướng dẫn của Ban lãnh đạo công ty, và các cơ quan liên quan khác để cập nhật thay đổi, nhận biết và đề xuất những biện pháp xử lý rủi ro
3. Tuân thủ pháp lý và tiêu chuẩn ngành:

* Các văn bản khác có liên quan.

1. Tất cả các nhân viên và khách hàng cần hiểu biết rằng, các chứng cứ về sự cố an ninh thông tin đều được lưu trữ và có thể bị xử lý bởi các cơ quan thực thi pháp luật theo lệnh của tòa án.
2. Kiểm tra, kiểm soát
3. Công tác kiểm tra, kiểm soát tài sản của hệ thống Công Ty X thực hiện định kỳ hoặc theo chỉ đạo của Giám đốc. Tổ/ban kiểm tra phải có ít nhất 01 (một) nhân viên CNTT tham gia.
4. Việc kiểm tra, kiểm soát thực hiện thông qua các phương tiện, công cụ và quy trình nhằm bảo đảm quá trình đánh giá chính xác và không ảnh hưởng đến vận hành hệ thống.
5. Toàn bộ thông tin, dữ liệu, kết quả sau quá trình kiểm tra, đánh giá cần được đảm bảo an toàn, bí mật trong nội bộ nhóm đánh giá và các cán bộ liên quan.

**CHƯƠNG II. TỔ CHỨC THỰC HIỆN**

**Điều 21. Đào tạo và truyền thông**

1. Ban ANM có trách nhiệm phổ biến các nội dung Quy chế ATTT sau khi được phê duyệt và ký ban hành tới các đối tượng áp dụng.
2. Các Phòng/Ban liên quan có trách nhiệm phối hợp với Ban ANM tổ chức các khóa đào tạo về ATTT hàng năm.
3. Kết quả của các buổi đào tạo phải đảm bảo đánh giá trên các tiêu chí: Năng lực, kiến thức, yêu cầu của bộ phận..

**Điều 22. Điều khoản chung**

1. Cán bộ nhân viên và các cá nhân, tố chức có liên quan có trách nhiệm tuân thủ thực hiện theo Quy chế ATTT, bất kỳ hành vi vi phạm nào theo Quy chế ATTT sẽ bị áp dụng các hình thức kỷ luật theo quy định của công ty. Trường hợp gây thiệt hại thì sẽ phải bồi thường theo quy định của Công ty và/hoặc của pháp luật.
2. Những vấn đề khác không được đề cập đến trong Quy chế này được thực hiện theo các quy định có liên quan của pháp luật và quy định nội bộ của Công ty. Trong quá trình thực hiện có bất kỳ nội dung nào của quy chế này trái với quy định của pháp luật mới được ban hành hoặc Điều lệ, Nghị quyết cùa Hội đồng quản trị thì nội dung đó đương nhiên hết hiệu lực thi hành.
3. Việc sửa đồi, bổ sung, thay thế tài liệu này do Ban ANM thực hiện trên cơ sở thu thập ý kiến các bên liên quan và thực tế hoạt động, trình Giám đốc phê duyệt.
4. Quy chế ATTT này có hiệu lực kể từ ngày ……/…./2021.
5. https://isocert.org.vn/bo-tai-lieu-iso-27001