ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

TRẦN KIÊN

XÂY DỰNG QUY TRÌNH BẢO ĐẢM AN TOÀN THÔNG TIN THEO CHUẨN ISO27001 CHO CÁC DOANH NGHIỆP VỪA VÀ NHỎ TẠI VIỆT NAM

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Hà Nội - 2017

ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

TRẦN KIÊN

XÂY DỰNG QUY TRÌNH BẢO ĐẢM AN TOÀN THÔNG TIN THEO CHUẨN ISO27001 CHO CÁC DOANH NGHIỆP VỪA VÀ NHỎ TẠI VIỆT NAM

Ngành: Công nghệ thông tin
Chuyên ngành: Quản lý Hệ thống thông tin
Mã số: 6048101

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. BÙI QUANG HƯNG

Hà Nội - 2017

LỜI CAM ĐOAN

Tôi xin cam đoan báo cáo luận văn này được viết bởi tôi dưới sự hướng dẫn của cán bộ hướng dẫn khoa học, thầy giáo, TS. Bùi Quang Hưng. Tất cả các kết quả đạt được trong luận văn là quá trình tìm hiểu, nghiên cứu, khảo sát, xây dựng kết hợp với kinh nghiệm của riêng tôi và sự chỉ dẫn của thầy giáo, TS. Bùi Quang Hưng. Nội dung trình bày trong luận văn là của cá nhân tôi hoặc và được tổng hợp từ nhiều nguồn tài liệu tham khảo khác đều có xuất xứ rõ ràng và được trích dẫn hợp pháp.

Tôi xin hoàn toàn chịu trách nhiệm và chịu mọi hình thức kỷ luật theo quy định cho lời cam đam của mình.

Hà Nội, ngày 21 tháng 8 năm 2017

Người cam đoan

Trần Kiên

LỜI CẢM ƠN

Tôi xin gửi lời cảm ơn chân thành và sâu sắc nhất tới thầy giáo, TS. Bùi Quang Hưng, người đã trực tiếp hướng dẫn nhiệt tình giúp đỡ tôi, chỉ bảo tôi những kinh nghiệm, phương pháp tiếp cận cũng như những tài liệu tham khảo để giúp tôi hoàn thành đề tài này.

Tôi cũng bày tỏ lời cảm ơn chân thành tới các thầy cô giáo đã giảng dậy tôi trong thời gian tôi học tập tại trường như PGS.TS. Hà Quang Thụy, PGS.TS Hoàng Xuân Huấn, PGS.TS Trần Đăng Hưng, PGS.TS Phạm Ngọc Hùng, PGS. TS Nguyễn Ngọc Hóa, TS. Nguyễn Tuệ, TS. Trần Trọng Hiếu, TS. Phan Xuân Hiếu, TS. Đặng Đức Hạnh, TS. Nguyễn Hoài Sơn, cùng các thầy cô giác khác trong khoa.

Tôi xin gửi lời cảm ơn đến bạn bè, đồng nghiệp những người đã dành thời gian nghe những lời chia sẻ, tâm sự của tôi và đưa ra những lời khuyên, lời động viên chân thành và quý báu. Đặc biệt tôi xin gửi lời cảm ơn chân thành nhất đến bạn Lê Hữu Tùng, chuyên gia tư vấn và triển khai đảm bảo an toàn thông tin cho các doanh nghiệp tại Việt Nam, hiện tại đang công tác tại công ty BKAV đã luôn theo sát, chỉ tôi cách tiếp cận vấn đề một cách thực tiễn nhất trong quá trình nghiên cứu luận văn.

Cuối cùng tôi xin gửi những tình cảm chân thành nhất từ trong trái tim đến bố, mẹ, vợ, con trai và đặc biệt là con gái tôi, cháu đã sinh ra vào thời điểm tôi bắt đầu nhận đề tài và bắt tay làm luận văn, một dấu mốc mà tôi khó thể quên trong cuộc đời này.

Hà Nội, ngày 21 tháng 8 năm 2017

Học viên thực hiện luận văn

Trần Kiên

MỤC LỤC

DANH MỤC TỪ VIẾT TẮT

STT	Từ tiếng Việt	Từ tiếng Anh	Từ viết tắt
1	An toàn thông tin	Information Security	ATTT
2	Công nghệ thông tin	Information Technology	CNTT
3	Doanh nghiệp vừa và nhỏ	Small and Medium Enterprise	SME
4	Hệ thống quản lý thông tin	Information Security Management System	ISMS

DANH MỤC BẢNG BIỂU

DANH MỤC HÌNH VẼ

MỞ ĐẦU

Sự phát triển của Internet Việt Nam đã đạt được nhiều thành quả to lớn trong 15 năm qua, với số lượng gần 4,8 triệu thuê bao truy nhập Internet băng rộng cố định, hơn 3,2 triệu hộ gia đình có kết nối Internet, 100% các Bộ ngành, tỉnh thành phố có cổng thông tin điện tử. Hiện tại, theo xu hướng ứng dụng công nghệ thông tin vào cuộc sống ngày càng sâu rộng thì các loại hình tội phạm mạng cũng như các nguy cơ làm mất an toàn thông tin ngày càng đa dạng và khó phòng chống hơn. Hệ thống máy tính của các tổ chức thường xuyên phải đối phó với các cuộc tấn công, xâm nhập trái phép, gây rò rỉ, mất mát thông tin, thậm chí dừng hoạt động, ảnh hưởng tiêu cực đến tiến độ, chất lượng công việc, kéo theo đó là các tổn thất về kinh tế, uy tín của tổ chức và thậm chí là ảnh hưởng tới an ninh quốc gia.

Các sự cố liên quan đến an toàn thông tin (ATTT) tại Việt Nam

Theo báo cáo của nhiều tổ chức quốc tế về an toàn thông tin, Việt Nam là một trong các mục tiêu hàng đầu trong khu vực của các tấn công gián điệp có tổ chức, mà mục tiêu của các cuộc tấn công này là các cơ quan, tổ chức quan trọng thuộc chính phủ và các tổ chức có sở hữu các hạ tầng thông tin trọng yếu.

Theo ghi nhận của trung tâm VNCERT số lượng các loại vụ việc, sự cố mất an toàn thông tin trong những năm qua được phát hiện và xửa lý ngày càng tăng. Trong 3 năm 2013-2015 trung tâm VNCERT ghi nhận 4.954.853 lượt địa chỉ IP của Việt Nam bị các mạng máy tính ma chiếm quyền điều khiển để đánh cắp thông tin hoặc phát tán mã độc, phát tán thư điện tử rác và tấn công mạng, trong đó có tới 12.480 lượt địa chỉ IP tĩnh của các cơ quan nhà nước nằm trong các mạng này. Chỉ tính riêng 6 tháng đầu năm 2016 các sự cố này đã trên 127.000. Trong đó, Phishing: 8.758; Deface: 77.160; Malware: 41.712.[1] Tâm điểm về các sự cố mất an toàn thông tin năm 2016 là vụ tin tặc tấn công vào vào một số màn hình hiển thị thông tin chuyến bay tại khu vực làm thủ tục bay của các sân bay như: Sân bay Tân Sơn Nhất, Sân bay Nội Bài, Sân bay Đà Nẵng, Sân bay Phú Quốc vào chiều 29 tháng 07 năm 2016. Các màn hình của sân bay đã bị chèn những hình ảnh và nội dung câu chữ xúc phạm Việt Nam và Philippines, xuyên

[1] Nguồn: Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam

tạc các nội dung về biển Đông. Hệ thống phát thanh của sân bay cũng phát đi những thông điệp tương tự. Đồng thời website của Việt Nam Airlines cũng bị hack với 411.000 dữ liệu của hành khách đi máy bay đã bị hacker thu thập và phát tán. Vụ việc đã gây thiệt hại làm cho hơn 100 chuyến bay bị ảnh hưởng, trong đó hàng chục chuyến bay bị chậm giờ từ 15 phút cho đến hơn 1 tiếng. Tại sân bay Nội Bài tất cả các màn hình và loa phát thanh tạm thời ngưng hoạt động để ngăn chặn hacker phát thông tin giả mạo. Các hãng hàng không phải sử dụng loa tay để thông báo cho khách.

Bên cạnh những rủi ro về an toàn thông tin (ATTT) do bị tấn công phá hoại có chủ đích, đáng chú ý là nhiều đơn vị không biết những sự cố liên quan đến an toàn thông tin đang nằm trong hệ thống mạng của mình. Các nguyên nhân chủ yếu là: Các quy trình quản lý, vận hành không đảm bảo; việc quản lý quyền truy cập chưa được kiểm tra và xem xét định kỳ; nhận thức của nhân viên trong việc sử dụng và trao đổi thông tin chưa đầy đủ; năng lực của các cán bộ kỹ thuật còn yếu, thiếu cán bộ chuyên môn và thiếu trang bị kỹ thuật tối thiểu… Do đó, ngoài các biện pháp kỹ thuật, tổ chức cần xây dựng và áp dụng các chính sách, quy định, quy trình vận hành phù hợp để giảm thiểu rủi ro.

Giải pháp ISO27001

Giải pháp toàn diện và hiệu quả nhất để giải quyết vấn đề trên là hệ thống của doanh nghiệp cần xây dựng, triển khai quy trình bảo vệ ATTT theo tiêu chuẩn ISO27001. Việc triển khai quy trình đáp ứng tiêu chuẩn ISO27001 sẽ giúp hoạt động đảm bảo ATTT của tổ chức được quản lý chặt chẽ, đạt được một số lợi ích sau:

- Bảo vệ thông tin của tổ chức, khách hàng và đối tác.

- Nhân viên tuân thủ và có thói quen đảm bảo ANTT.

- Hoạt động đảm bảo ANTT luôn được duy trì và cải tiến.

- Hoạt động nghiệp vụ trọng yếu của tổ chức không bị gián đoạn.

- Nâng cao uy tín của tổ chức, tăng sức mạnh cạnh tranh.

Thực trạng triển khai ISO27001 tại Việt Nam

Hiện tại tại Việt Nam việc xây dựng, triển khai quy trình bảo vệ ATTT theo tiêu

chuẩn ISO27001 còn rất hạn chế. Chủ yếu là các doanh nghiệp lớn hoặc doanh nghiệp có vốn đầu tư nước ngoài mới quan tâm đến việc đầu tư, xây dựng và triển khai.

- Tháng 2/2006: Tổng cục Tiêu chuẩn Đo lường Chất lượng Việt Nam đã ban hành tiêu chuẩn TCVN 7562: 2005 – Công nghệ thông tin – Mã thực hành quản lý an toàn thông tin, (tương đương với tiêu chuẩn ISO/IEC 17799: 2000). Tiêu chuẩn này đề ra các hướng dẫn thực hiện hệ thống quản lý an ninh thông tin làm cơ sở cho ISO27001.

- Tháng 1/2007: Công ty CSC Việt Nam (Computer Sciences Corporation) đã trở thành đơn vị đầu tiên có được chứng nhận ISO27001.

- Đến tháng 7/2013 ở Việt Nam có 5 đơn vị (CSC Việt Nam, FPT IS, FPT Soft, GHP FarEast, ISB Corporation Vietnam…) đã đạt chứng nhận ISO27001 và hơn 10 đơn vị (HPT Soft, VietUnion, Quantic…) đang trong quá trình triển khai ứng dụng tiêu chuẩn này.

- Đến hết năm 2012, Việt Nam đã có 249 chứng chỉ ISO27001.

- Năm 2014, Việt Nam được cấp 94 chứng chỉ ISO27001, nhiều hơn so với năm 2013 và 2012 lần lượt là 55 và 50 chứng chỉ.

Cũng qua số liệu này, chúng ta có thể thấy số đơn vị đạt chứng nhận ISO27001 tại Việt Nam khá khiêm tốn so với Nhật Bản (53290 chứng nhận), Trung Quốc (8294 chứng nhận), Malaixia (759 chứng nhận). Một trong những nguyên nhân của tình trạng này là chi phí để đạt chứng nhận ISO27001 khá cao, bao gồm các chi phí về tư vấn, cấp chứng nhận và đặc biệt là chi phí doanh nghiệp phải bỏ ra để thực hiện các biện pháp kiểm soát rủi ro.

Vấn đề của các doanh nghiệp vừa và nhỏ tại Việt Nam trong việc áp dụng và triển khai ISO27001

Các doanh nghiệp ở Việt Nam chủ yếu là các doanh nghiệp có quy mô vừa và nhỏ[2], chiếm 94.8%[3] nên nguồn lực còn hạn chế nên sự quan tâm đến lĩnh vực áp

[2] Ở Việt Nam, theo Điều 3, Nghị định số 56/2009/NĐ-CP ngày 30/6/2009 của Chính phủ, quy định số lượng lao động trung bình hàng năm từ 10 người trở xuống được coi là doanh nghiệp siêu nhỏ, từ 10 đến dưới 200 người lao động được coi là Doanh nghiệp nhỏ và từ 200 đến 300 người lao động thì được coi là Doanh nghiệp vừa.

[3] Nguồn: "Báo cáo tổng quan về tình hình doanh nghiệp" trong báo cáo phục vụ Hội nghị Thủ

các chuẩn quản lý chất lượng quốc tế như ISO27001 còn chưa nhiều. Nguyên nhân của thực trạng này là như sau:

- Nhận thức của toàn tổ chức về việc đảm bảo ANTT, lợi ích triển khai áp dụng Hệ thống quản lý ANTT chưa cao.

- Chi phí để áp dụng khá cao, trong đó đặc biệt là chi phí doanh nghiệp phải bỏ ra để thực hiện các biện pháp kiểm soát rủi ro.

- Khó khăn trong triển khai: phối hợp không tốt giữa các bộ phận, không cam kết nguồn lực tham gia và áp lực về thời gian.

- Sự quan tâm, cam kết thực hiện của lãnh đạo chưa cao.

- Đầu tư (nguồn lực, tài chính) còn bị hạn chế.

Mục tiêu của luận văn

Với mong muốn đóng góp một phần nhỏ công sức cho nền doanh nghiệp nước nhà trong việc đảm bảo an toàn thông tin, nơi mà tỷ lệ doanh nghiệp vừa và nhỏ chiếm đa số, luận văn sẽ tập trung tìm hiểu ISO27001, chọn ra một doanh nghiệp vừa và nhỏ đặc trưng để tiến hành xây dựng quy trình đáp ứng tiêu chuẩn ISO27001 cho doanh nghiệp này với các mục tiêu như chi phí, nhân sự tham gia áp dụng quy trình, thời gian triển khai được giảm thiểu tới mức tối đa. Với tinh thần đó, luận văn được bố cục thành 04 chương chính như sau:

- Mở đầu

Phần này sẽ nêu ra các vấn đề, thực trạng trong việc áp dụng các tiêu chuẩn đảm bảo an toàn thông tin theo chuẩn ISO27001 trong các doanh nghiệp tại Việt Nam, vấn đề gặp phải của các doanh nghiệp vừa và nhỏ khi tiến hành áp dụng tiêu chuẩn này và đưa ra mục tiêu trong việc giải quyết vấn đề của luận văn.

- Chương 1: Giới thiệu ISO27001

Chương này sẽ tập trung giới thiệu khái niệm ISO27001, cấu trúc, nội dung, các điều khoản phải tuân thủ khi áp dụng ISO27001.

- Chương 2: Khảo sát doanh nghiệp SME cụ thể về bảo đảm an toàn thông tin

Chương này sẽ chọn ra một doanh nghiệp SME tiêu biểu trong việc đảm bảo an toàn thông tin, giới thiệu về cơ cấu tổ chức, nhân sự, lĩnh vực hoạt động kinh doanh… cũng như yêu cầu đảm bảo an toàn thông tin của các bên liên quan. Sau đó sẽ tiến hành khảo sát về thực trạng bảo đảm an toàn thông tin của doanh nghiệp SME đã lựa chọn dựa trên việc liệt kê các tài sản của doanh nghiệp, phân tích các rủi ro, các nguy cơ và đưa ra các biện pháp kiểm soát.

- Chương 3: Đề xuất bộ quy trình cho doanh nghiệp SME đã lựa chọn

Sau khi tiến hành khảo sát doanh nghiệp SME đã lựa chọn ở chương 2, chương này sẽ đề xuất xây dựng quy trình, chính sách, biện pháp, thủ tục… để đảm bảo an toàn thông tin, giải quyết các vấn đề liên quan đến an toàn thông tin mà doanh nghiệp trên gặp phải theo chuẩn ISO27001.

- Chương 4: Kết luận

Sau khi đề xuất, xây dựng bộ quy trình ở chương 3, chương này sẽ đánh giá những mặt được và mặt chưa được của bộ quy trình đã xây dựng được. Sau đó sẽ tiến hành đề xuất những hướng phát triển tiếp theo của luận văn, đó là tiếp tục tìm hiểu các doanh nghiệp vừa và nhỏ đặc trưng khác trong việc bảo đảm an toàn thông tin, rút ra những nét đặc trưng để xây dựng một nền tảng quy trình chung, với mục đích đóng góp một phần công sức cho các doanh nghiệp vừa và nhỏ tại Việt Nam trong việc đảm bảo an toàn thông tin, một vấn đề khá nhức nhối hiện nay.

CHƯƠNG 1.

GIỚI THIỆU ISO27001

1.1. Khái niệm

ISO27001 là tiêu chuẩn quốc tế đặc tả cho các hệ thống quản lý ATTT, nó cung cấp một mô hình thống nhất để thiết lập, vận hành, duy trì và cải tiến hệ thống quản lý ATTT. Việc tuân thủ theo ISMS chính là quyết định chiến lược của mỗi tổ chức.

ISO27001 tạo ra một hệ thống theo dõi và duy trì:

- Tính bảo mật thông tin.

- Tính sẵn có (availability) của thông tin.

- Tính tính toàn vẹn (integrity) của thông tin.

Trong đó:

Tính bảo mật thông tin bao gồm:

- Tính bảo mật dữ liệu (Data confidentiality) đảm bảo rằng thông tin hoặc bí mật cá nhân không được cung cấp và tiết lộ cho các cá nhân không có thẩm quyền.

- Tính riêng tư (Privacy) đảm bảo rằng cá nhân kiểm soát và có tác động tới thông tin gì liên quan đến họ được phép thu thập và lưu giữ, và kiểm soát và tác động tới người nào được phép cung cấp thông tin nói trên và cung cấp tới những ai.

Tính toàn vẹn thông tin bao gồm:

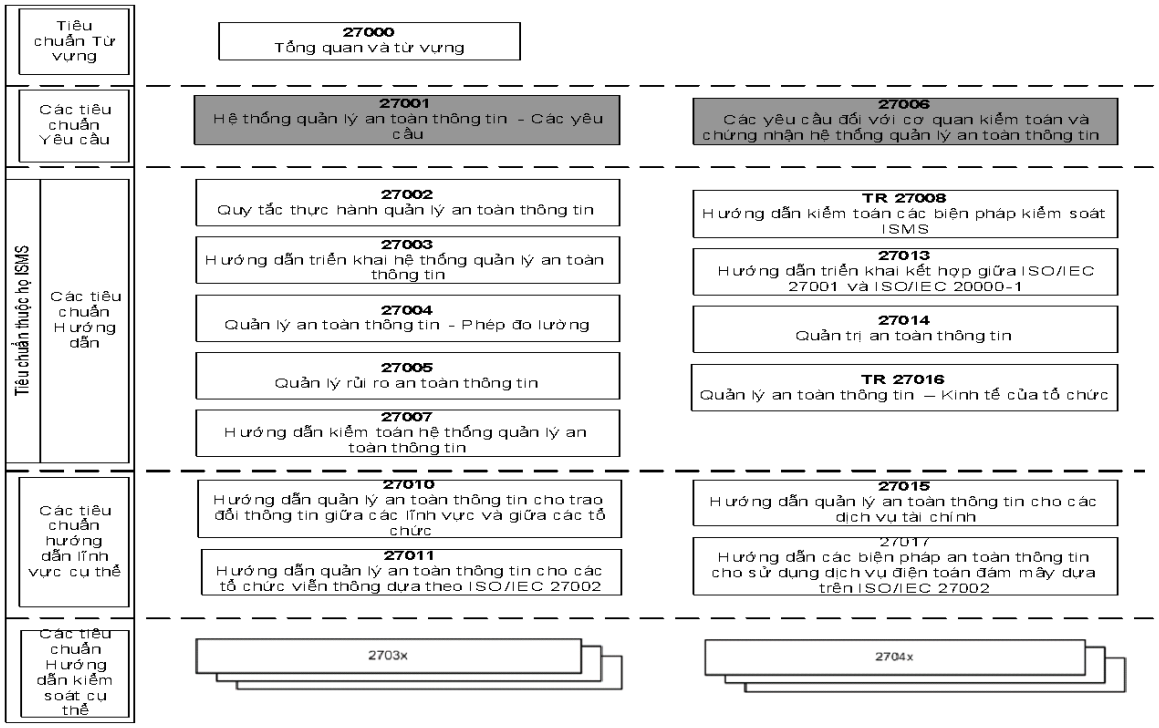
- Tính toàn vẹn dữ liệu (Data integrity) đảm bảo rằng thông tin và chương trình chỉ được thay đổi theo các cách thức quy định và được phép.

- Tính toàn vẹn hệ thống (System integrity) đảm bảo rằng hệ thống triển khai các chức năng định sẵn một cách không suy giảm, độc lập đối với các thao tác trái phép cố ý hoặc vô ý.

Tính sẵn có đảm bảo rằng hệ thống làm việc nhanh và dịch vụ không bị từ chối

đối với người dùng được phép.

1.2. Vị trí của ISO27001 trong họ ISO27000[5]



Hình 1.1 Vị trí ISO27001

1.3. Cấu trúc của ISO27001[4]

Tiêu chuẩn ISO27001 có cấu trúc bao gồm 2 phần là "Điều khoản" và "Biện pháp kiểm soát".

Phần "Điều khoản"

Phần "Điều khoản" bao gồm 7 điều khoản bắt buộc phải thực thi. Mọi vi phạm đối với từng điều khoản đều được coi là không tuân thủ ISO27001.

- 07 điều khoản chính (từ phần 4 đến phần 10 của Tiêu chuẩn): đưa ra yêu cầu bắt buộc về các công việc cần thực hiện trong việc thiết lập, vận hành, duy trì, giám sát và nâng cấp ISMS của các tổ chức. Bất kỳ vi phạm nào của tổ chức so với các quy định nằm trong 07 điều khoản này đều được coi là không tuân thủ theo tiêu chuẩn:

---

[4] Theo http://antoanthongtin.vn

Điều khoản 4 - Phạm vi tổ chức: Đưa ra các yêu cầu cụ thể để tổ chức căn cứ trên quy mô, lĩnh vực hoạt động và các yêu cầu, kỳ vọng của các bên liên quan thiết lập phạm vi Hệ thống quản lý ATTT phù hợp.

Điều khoản 5 - Lãnh đạo: Quy định các vấn đề về trách nhiệm của Ban lãnh đạo mỗi tổ chức trong ISMS, bao gồm các yêu cầu về sự cam kết, quyết tâm của Ban lãnh đạo trong việc xây dựng và duy trì hệ thống; các yêu cầu về việc cung cấp nguồn lực, tài chính để vận hành hệ thống.

Điều khoản 6 - Lập kế hoạch: Tổ chức cần định nghĩa và áp dụng các quy trình đánh giá rủi ro, từ đó đưa ra các quy trình xử lý. Điều khoản này cũng đưa ra các yêu cầu về việc thiết lập mục tiêu ATTT và kế hoạch để đạt được mục tiêu đó.

Điều khoản 7 - Hỗ trợ: yêu cầu đối với việc tổ chức đào tạo, truyền thông, nâng cao nhận thức cho toàn thể cán bộ, nhân viên của tổ chức về lĩnh vực ATTT và ISMS, số hóa thông tin.

Điều khoản 8 - Vận hành hệ thống: Tổ chức cần có kế hoạch vận hành và quản lý để đạt được các mục tiêu đã đề ra. Đồng thời cần định kỳ thực hiện đánh giá rủi ro ATTT và có kế hoạch xử lý.

Điều khoản 9 - Đánh giá hiệu năng hệ thống: Quy định trách nhiệm của Ban lãnh đạo trong việc định kỳ xem xét, đánh giá ISMS của tổ chức. Phần này đưa ra yêu cầu đối với mỗi kỳ xem xét hệ thống, đảm bảo đánh giá được toàn bộ hoạt động của hệ thống, đo lường hiệu quả của các biện pháp thực hiện và có kế hoạch khắc phục, nâng cấp hệ thống cho phù hợp với những thay đổi trong hoạt động của tổ chức.

Điều khoản 10 - Cải tiến hệ thống: Giữ vững nguyên tắc Kế hoạch - Thực hiện - Kiểm tra - Hành động (P-D-C-A), tiêu chuẩn cũng đưa ra các yêu cầu đảm bảo ISMS không ngừng được cải tiến trong quá trình hoạt động. Gồm các quy định trong việc áp dụng các chính sách mới, các hoạt động khắc phục, phòng ngừa các điểm yếu đã xảy ra và tiềm tàng để đảm bảo hiệu quả của ISMS.

Phần "Biện pháp kiểm soát"

Các mục tiêu và biện pháp kiểm soát: đưa ra 14 lĩnh vực kiểm soát với 35 mục tiêu kiểm soát (ứng với 114 biện pháp kiểm soát) nhằm cụ thể hóa các vấn đề mà tổ chức cần xem xét, thực hiện khi xây dựng và duy trì ISMS. Các lĩnh vực

đưa ra xem xét bao gồm từ chính sách của lãnh đạo tổ chức, tới việc đảm bảo ATTT trong quản lý tài sản, nhân sự, các nguyên tắc căn bản để đảm bảo ATTT trong việc vận hành, phát triển, duy trì các hệ thống CNTT…

STT	Các lĩnh vực kiểm soát trong ISO27001
5	**Chính sách ATTT** Mục tiêu: Để cung cấp hướng quản lý và hỗ trợ an ninh thông tin theo những yêu cầu của doanh nghiệp, những điều luật và những quy định liên quan. Các mục tiêu kiểm soát: - Chính sách an ninh thông tin. - Soát xét chính sách an ninh thông tin.
6	**ATTT trong tổ chức** - Tổ chức nội bộ: Thiết lập một hệ thống quản lý để bắt đầu và kiểm soát sự thực hiện và các hoạt động liên quan đến an ninh thông tin trong tổ chức. - Các thiết bị di động và làm việc từ xa: Để đảm bảo an toàn trong việc làm việc từ xa và an toàn trong việc sử dụng thiết bị di động. Các mục tiêu kiểm soát: - Vai trò và trách nhiệm liên quan đến an ninh thông tin. - Sự phân chia trách nhiệm. - Liên lạc với các bên liên quan. - Liên lạc với nhóm có những lợi ích đặc biệt. - An ninh thông tin trong quản lý dự án. - Chính sách thiết bị di động. - Làm việc từ xa.
7	**ATTT nhân sự** - Trước khi làm việc: Để đảm bảo rằng những nhân viên và nhà thầu

	hiểu rõ được trách nhiệm và phù hợp với vai trò họ được đảm nhiệm. - Trong quá trình làm việc: Để đảm bảo rằng những nhân viên và nhà thầu hiểu và thực hiện trách nhiệm của họ liên quan đến an ninh thông tin. - Chấm dứt và thay đổi nhân sự: Để bảo vệ lợi ích của tổ chức khi thay đổi hay chấm dứt hợp đồng nhân viên. Các mục tiêu kiểm soát: - Screening. - Điều khoản và điều kiện làm việc. - Trách nhiệm trong việc quản lý. - Nhận thức, giáo dục và đào tạo an ninh thông tin. - Quy trình kỷ luật. - Chấm dứt hoặc thay đổi trách nhiệm công việc.
8	**Quản lý tài sản** - Trách nhiệm đối với tài sản: Để xác định tài sản của tổ chức và xác định trách nhiệm bảo vệ phù hợp. - Phân loại thông tin: Để đảm bảo rằng thông tin nhận được mức bảo vệ phù hợp phù hợp với tầm quan trọng của nó đối với tổ chức. - Xử lý media: Để tránh việc tiết lộ, chỉnh sửa, xóa hay hủy bỏ thông tin được lưu trữ trên các phương tiện, thiết bị lưu trữ một cách không được phép. Các mục tiêu kiểm soát: - Kiểm kê tài sản. - Quyền sở hữu tài sản. - Chấp nhận sử dụng tài sản.

	- Trả lại tài sản. - Phân loại thông tin. - Đánh nhãn thông tin. - Xử lý tài sản. - Quản lý các phương tiện, thiết bị di dời được. - Tiết lộ thông tin. - Vận chuyển phương tiện, thiết bị vật lý
9	**Kiểm soát truy nhập** - Yêu cầu của doanh nghiệp trong việc kiểm soát truy cập: Để giới hạn truy cập đến thông tin và thiết bị xử lý thông tin. - Quản lý truy cập người dùng: Để đảm bảo truy cập người dùng hợp pháp và ngăn chặn việc truy cập vào hệ thống và dịch vụ một cách bất hợp pháp. - Trách nhiệm người dùng: Để người dùng có trách nhiệm bảo vệ thông tin đã được xác thực của họ. - Kiểm soát truy cập hệ thống và ứng dụng: Để ngăn chặn truy cập trái phép vào hệ thống và ứng dụng. Các mục tiêu kiểm soát: - Chính sách kiểm soát truy cập. - Truy cập đến mạng và các dịch vụ mạng. - Đăng ký và hủy đăng ký người dùng - Truy cập người dùng. - Quản lý quyền truy cập đặc quyền

	- Quản lý thông tin bảo mật của người dùng. - Soát xét quyền truy cập người dùng. - Hủy bỏ hoặc điều chỉnh quyền truy cập. - Sử dụng thông tin bảo mật. - Giới hạn truy cập thông tin. - Quy trình đăng nhập bảo mật. - Hệ thống quản lý mật khẩu. - Sử dụng các chương trình tiện ích. - Kiểm soát truy cập đến mã nguồn chương trình.
10	**Mật mã / Mã hóa** Đảm bảo mã hóa đúng và hiệu quả để đảm bảo tính bí mật, xác thực và/hoặc toàn vẹn của thông tin. Các mục tiêu kiểm soát: - Chính sách về kiểm soát mã hóa. - Quản lý khóa.
11	**ATTT vật lý và nơi làm việc** - Phạm vi an toàn: Để tránh truy cập vật lý, gây thiệt hại và can dự trái phép vào thông tin và thiết bị xử lý thông tin của tổ chức. - Thiết bị: Ngăn chặn sự mất mát, thiệt hại, trộm cắp tài sản à sự gián đoạn hoạt động của tổ chức. Các mục tiêu kiểm soát: - Chu vi an ninh vật lý.

	- Kiểm soát lối vào vật lý. - Bảo vệ tòa nhà, văn phòng và các thiết bị. - Bảo vệ chống lại các mối đe dọa từ bên ngoài và môi trường. - Làm việc trong khu vực an toàn. - Đặt và bảo vệ thiết bị. - Các tiện ích hỗ trợ. - An toàn cáp. - Bảo trì thiết bị. - Hủy bỏ tài sản. - Hủy bỏ hoặc tái sử dụng an toàn thiết bị. - Thiết bị tự động. - Chính sách bàn làm việc và màn hình máy tính sạch.
12	**ATTT trong quá trình vận hành** - Quy trình và trách nhiệm: Để đảm bảo đúng và an toàn các hoạt động trong các thiết bị xử lý thông tin. - Bảo vệ khỏi phần mềm độc hại: Để đảm bảo rằng thông tin và các thiết bị xử lý thông tin được bảo vệ khỏi các phần mềm độc hại. - Sao lưu: Để bảo vệ chống mất mát dữ liệu - Đăng nhập và theo dõi: Log các sự kiện và sinh ra các evidence. - Kiểm soát phần mềm hoạt động: Để đảm bảo tính toàn vẹn của hệ thống hoạt động. - Quản lý lỗ hổng kỹ thuật: Để tránh khai thác lỗ hổng kỹ thuật. - Xem xét đánh giá hệ thống thông tin: Giảm đến mức tối thiểu tác

	động của hoạt động đánh giá trên hệ thống hoạt động. Các mục tiêu kiểm soát: - Quy trình hoạt động phải được tài liệu hóa. - Quản lý thay đổi. - Quản lý khả năng lưu trữ. - Tách biệt việc phát triển, kiểm thử và môi trường hoạt động. - Kiểm soát phần mềm độc hại. - Sao lưu thông tin. - Log sự kiện. - Bảo vệ thông tin log. - Người quản trị và người vận hành log. - Cài đặt phần mềm trên hệ thống hoạt động. - Quản lý lỗ hổng kỹ thuật. - Hạn chế cài đặt phần mềm.
13	**ATTT trong truyền thông** - Quản lý an ninh mạng: Để đảm bảo thông tin trong mạng và thiết bị xử lý hỗ trợ thông tin của nó. - Truyền thông tin: Để duy trì sự an toàn của thông tin được truyền trong một tổ chức và với các thực thể bên ngoài. Các mục tiêu kiểm soát: - Kiểm soát mạng. - An toàn dịch vụ mạng. - Chia mạng.

	- Thủ tục và chính sách truyền thông tin. - Thỏa thuận truyền thông tin. - Tin nhắn điện tử. - Thỏa thuận bí mật và không tiết lộ.
14	**ATTT trong phát triển vòng đời hệ thống** - An ninh trong quy trình phát triển và hỗ trợ: Để đảm bảo rằng an ninh thông tin được thiết kế và thực thi trong vòng đời phát triển hệ thống thông tin. - Test data: Để đảm bảo việc bảo vệ dữ liệu được sử dụng trong kiểm thử. Các mục tiêu kiểm soát: - Phân tích và đặc tả các yêu cầu an ninh thông tin. - Bảo mật các dịch vụ, ứng dụng và mạng công cộng. - Bảo vệ các giao dịch dịch vụ, ứng dụng. - Chính sách phát triển bảo mật. - Thủ tục kiểm soát thay đổi hệ thống. - Soát xét công nghệ của ứng dụng sau khi thay đổi nền tảng hoạt động. - Hạn chế thay đổi gói phần mềm. - Nguyên tắc an toàn hệ thống. - Môi trường phát triển an toàn. - Phát triển thuê ngoài. - Kiểm tra an ninh hệ thống. - Kiểm thử accept hệ thống.

15	**ATTT khi làm việc với nhà cung cấp** - An ninh thông tin trong mối quan hệ với nhà cung cấp: Để đảm bảo việc bảo vệ tài sản của tổ chức được truy cập bởi nhà cung cấp. - Quản lý phân phối dịch vụ nhà cung cấp: Để duy trì một mức độ thỏa thuận an ninh thông tin và cung cấp dịch vụ phù hợp với các thỏa thuận cung cấp. Các mục tiêu kiểm soát: - Chính sách an ninh thông tin trong mối quan hệ với nhà cung cấp. - Đưa an ninh thông tin vào trong thỏa thuận với nhà cung cấp. - Thông tin và chuỗi cung cấp công nghệ truyền thông. - Giám sát và xem xét dịch vụ cung ứng. - Quản lý thay đổi đến nhà cung cấp dịch vụ.
16	**Quản lý sự cố ATTT** Để đảm bảo phương pháp tiếp cận hiệu quả và tính nhất quản để quản lý sự cố an ninh thông tin, bao gồm truyền thông về các sự kiện an ninh thông tin và những yếu điểm. Các mục tiêu kiểm soát: - Thủ tục và trách nhiệm. - Báo cáo sự cố an ninh thông tin. - Báo cáo điểm yếu trong an ninh thông tin. - Đánh giá và quyết định trên sự kiện an ninh thông tin. - Phản hồi từ sự cố an ninh thông tin. - Học từ những sự cố an ninh thông tin. - Tập hợp các evidence.

17	**Đảm bảo tính hoạt động liên tục trong trường hợp thảm họa** - Tính liên tục an ninh thông tin: Tính liên tục an ninh thông tin phải được nhúng vào hệ thống quản lý tính liên tục doanh nghiệp của tổ chức. - Sự dư thừa: Để đảm bảo tính sẵn sàng của thiết bị xử lý thông tin. Các mục tiêu kiểm soát: - Kế hoạch tính liên tục an ninh thông tin. - Triển khai tính liên tục an ninh thông tin. - Kiểm chứng, soát xét và đánh giá tính liên tục an ninh thông tin. - Tính sẵn sàng của các thiết bị xử lý thông tin.
18	**Sự tuân thủ** - Tuân thủ những yêu cầu pháp lý và những yêu cầu có tính hợp đồng: Để tránh vi phạm pháp lý, luật định, quy định hoặc nghĩa vụ hợp đồng liên quan đến an ninh thông tin của bất kỳ yêu cầu an ninh nào. - Review an ninh thông tin: Để đảm bảo rằng an ninh thông tin được thực thi và vận hành tuân theo chính sách và quy trình của tổ chức. Các mục tiêu kiểm soát: - Xác định điều lệ áp dụng và những yêu cầu ràng buộc hợp đồng. - Quyền sở hữu trí tuệ. - Bảo vệ các hồ sơ. - Tính riêng tư và bảo vệ thông tin cá nhân. - Quy định kiểm soát mật mã. - Soát xét một cách độc lập an ninh thông tin. - Sự tuân thủ chính sách và tiêu chuẩn an ninh.

	- Soát xét sự tuân thủ kỹ thuật.

1.4. Các lợi ích mà ISO27001 mang lại[5]

- Sự liên tục trong kinh doanh.

- Đánh giá được mối nguy và triển khai được các phương pháp để giảm bớt ảnh hưởng.

- An ninh được cải thiện.

- Kiểm soát việc truy cập.

- Tiết kiệm chi phí.

- Tạo ra một quá trình quản lý nội bộ.

- Tuyên truyền cam kết của bạn để bảo vệ dữ liệu của khách hàng.

- Chứng minh được rằng bạn tuân thủ các quy định pháp luật.

- Xác định được rằng các lãnh đạo cấp cao thực sự nghiêm túc trong việc bảo mật dữ liệu.

- Đánh giá thường xuyên để duy trì hiệu quả bảo mật.

- Cung cấp chứng nhận độc lập.

[5] Theo http://acsregistrars.vn (Chủ thể trang: Công ty TNHH Chứng nhận ACS Việt Nam. ACS Registrars là một trong những tổ chức chứng nhận hàng đầu của Vương quốc Anh)

CHƯƠNG 2.

KHẢO SÁT DOANH NGHIỆP SME CỤ THỂ VỀ BẢO ĐẢM AN TOÀN THÔNG TIN

Chương này sẽ chọn ra một doanh nghiệp SME tiêu biểu trong việc đảm bảo an toàn thông tin, giới thiệu về cơ cấu tổ chức, nhân sự, lĩnh vực hoạt động kinh doanh… cũng như yêu cầu đảm bảo an toàn thông tin của các bên liên quan. Sau đó sẽ tiến hành khảo sát về thực trạng bảo đảm an toàn thông tin của doanh nghiệp SME đã lựa chọn dựa trên việc liệt kê các tài sản của doanh nghiệp, phân tích các rủi ro, các nguy cơ và đưa ra các biện pháp kiểm soát.

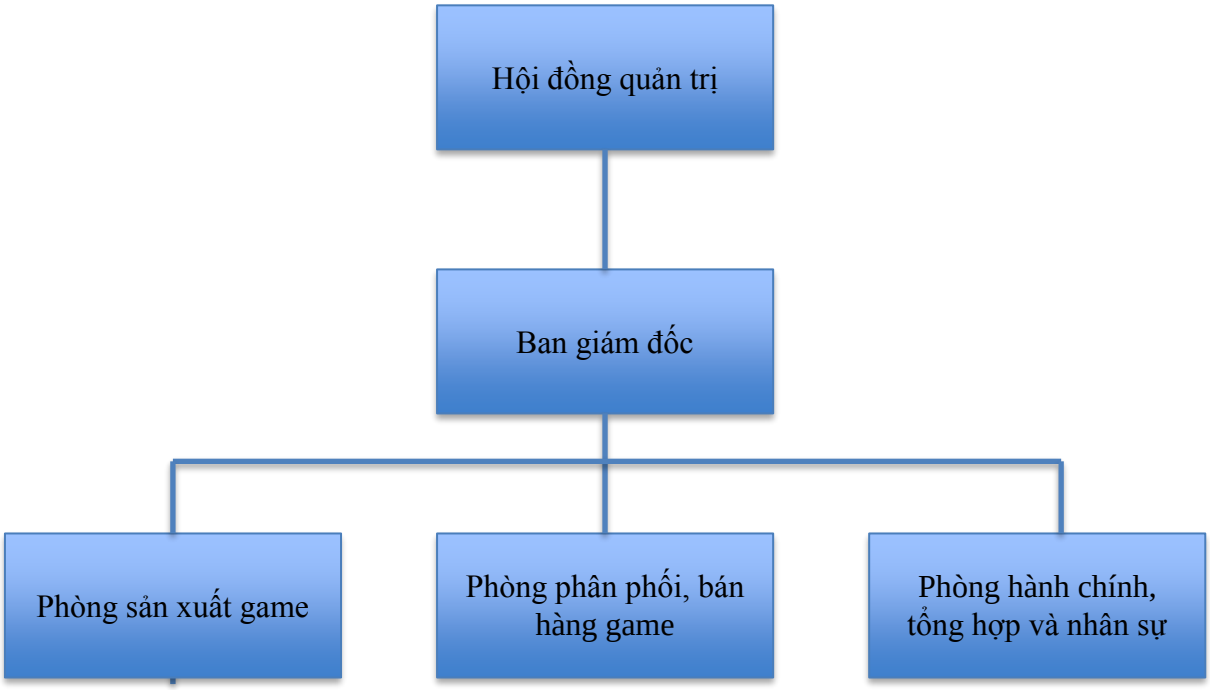
2.1. Giới thiệu công ty SME cụ thể

Tên công ty	Công ty X[6]
Thành lập	Năm 2012
Nhân sự	50 nhân viên
Lĩnh vực hoạt động	Game Studio chuyên sản xuất và phân phối game cho thiết bị di động: iOS, Android, Windows, BlackBerry, Java... Chủ yếu các game được xây dựng trên nền đồ họa 2D, ý tưởng game lấy từ cảm hứng từ những game kinh điển trên hệ máy Nintendo thời xưa.
Sứ mệnh	Công ty X nỗ lực trở thành nhà sản xuất game có uy tín trên toàn quốc, đưa sản phẩm ra quốc tế, sáng tạo các giá trị vì khách hàng, đem lại thành công cho các thành viên, đóng góp cho cộng đồng.
Các sản phẩm, dịch vụ	**1. Kungfu Feet** - Trò chơi bóng đá trên điện thoại di động - Giải nhất cuộc thi Bluebird Award 2015 - Thị trường phát hành: trong nước và quốc tế - Số lượng lượt tải: 100.000 **2. Jewel Pandora** - Trò chơi xếp hình kim cương trên điện thoại di động - Thị trường phát hành: quốc tế - Số lượng lượt tải: 1.000.000

[6] Do vấn đề bảo mật về tên công ty, nên tên công ty được gọi trong luận văn là công ty X

	3. Kingdom Reborn - Magic Rush - Game chiến thuật công thành - Thị trường phát hành: quốc tế - Số lượng lượt tải: 300.000 **4. Penguin Club** - Game thể loại casual - Thị trường phát hành: quốc tế - Số lượng lượt tải: 250.000 **5. Boom Bá Online** - Game đặt bom chiến thuật - Thị trường phát hành: Việt Nam - Tháng 6/2017 chính thức phát hành

2.2. Tổ chức



Hình 2.1 Sơ đồ tổ chức

2.3. Các đối thủ cạnh tranh

- Công ty phát triển game di động Divmob.
- Công ty phát triển game di động Tofu.
- Công ty game MeCorp.
- Công ty cổ phần Egame.
- Công ty Fgame.

2.4. Các đối tác liên quan

- Các đối tác cung cấp dịch vụ kênh thanh toán trong game.
- Các công ty phát hành những sản phẩm game do công ty sản xuất.
- Các cá nhân phát hành những sản phẩm game do công ty sản xuất.

2.5. Mong muốn và yêu cầu của các bên liên quan đối với công ty

- Các công ty phát hành sản phẩm do công ty X sản xuất luôn muốn công ty giữ bí mật về doanh thu phát sinh, cách thức họ phát hành, cụ thể số lượt tải phát sinh từ các nguồn quảng cáo, các sản phẩm game mà họ độc quyền phân phối thì Công ty X không được gửi cho bất kỳ công ty phân phối game nào khác và chi tiết hợp đồng hợp tác giữa Công ty X và họ.

- Các cá nhân phát hành sản phẩm do công ty X sản xuất luôn muốn công ty giữ bí mật về doanh thu phát sinh, cách thức họ phát hành, cụ thể số lượt tải phát sinh từ các nguồn quảng cáo và chi tiết hợp đồng hợp tác giữa Công ty X và họ.

- Các đối tác cung cấp dịch vụ kênh thanh toán trong game muốn công ty giữ bí mật về doanh thu phát sinh khi chạy qua kênh thanh toán của họ, chi tiết log giao dịch của khách hàng và chi tiết hợp đồng hợp tác giữa Công ty X và họ.

Về mặt cơ sở pháp lý:

Vào ngày 19/11/2015, Luật ATTT mạng số 86/2015/QH13 Quốc hội khóa XIII thông qua tại Kỳ hợp thứ 10 và luật này có hiệu lực vào ngày 01/07/2016. Luật ATTT mạng có 8 chương, 54 điều gồm Chương 1 Quy định chung (Điều 1-Điều 8), Chương 2. Đảm bảo ATTT mạng (Mục 1. Bảo vệ thông tin mạng gồm Điều 9-Điều 15, Mục 2. Bảo vệ thông tin cá nhân gồm Điều 16-Điều 20, Mục 3. Bảo vệ hệ thống thông tin gồm Điều 21-Điều 27, Mục 4. Ngăn chặn xung đột thông tin trên mạng gồm Điều 28-Điều 29), Chương 3. Mật mã dân sự (Điều 30-Điều 36), Chương 4. Tiêu chuẩn, quy chuẩn kỹ thuật ATTT mạng (Điều 37-Điều 39), Chương 5. Kinh doanh trong lĩnh vực ATTT mạng (Mục 1. Cấp giấy phép kinh doanh an toán thông tin mạng gồm Điều 40-46, Mục 2. Quản lý nhập khẩu sản phẩm ATTT mạng gồm Điều 47-Điều 48), Chương 6. Phát triển nguồn nhân lực ATTT mạng (Điều 49-Điều 50), Chương 7. Quản lý nhà nước về ATTT mạng (Điều 51-Điều 52), Chương 8. Điều khoản triển khai (Điều 53-Điều 54).

Bên cạnh Luật ATTT mạng, đối với một công ty sản xuất game như Công ty X, sẽ phải tuân thủ những quy định sau trong việc bảo đảm an toàn thông tin:[7]

- Theo Điều 6 Khoản 2 Thông tư 24/2014/TT-BTTTT quy định: Doanh nghiệp

[7] Nguồn: Thông tư 24/2014/TT-BTTT của Bộ Thông tin và Truyền thông ban hành ngày 29 tháng 12 năm 2014 Quy định chi tiết về hoạt động quản lý, cung cấp và sử dụng dịch vụ trò chơi điện tử trên mạng

cung cấp dịch vụ trò chơi điện tử G1 phải lưu giữ các thông tin cá nhân người chơi trong suốt quá trình người chơi sử dụng dịch vụ và trong 06 (sáu) tháng sau khi người chơi ngừng sử dụng dịch vụ.

- Theo Điều 12 Khoản 2 Thông tư 24/2014/TT-BTTTT về Điều kiện về tổ chức, nhân sự cung cấp dịch vụ trò chơi điện tử G1 quy định: Có đội ngũ nhân sự quản trị trò chơi điện tử phù hợp với quy mô hoạt động, bảo đảm tối thiểu 01(một) nhân sự quản trị 2 (hai) máy chủ.

- Theo Điều 12 Khoản 3 Thông tư 24/2014/TT-BTTTT về Điều kiện về tổ chức, nhân sự cung cấp dịch vụ trò chơi điện tử G1 quy định: Có nhân sự tốt nghiệp đại học trở lên chịu trách nhiệm về quản lý hoạt động cung cấp trò chơi điện tử.

- Theo Điều 13 Khoản 4 Thông tư 24/2014/TT-BTTTT về Điều kiện về kỹ thuật cung cấp dịch vụ trò chơi điện tử G1 quy định: Có phương án dự phòng về thiết bị và kết nối, phương án sao lưu dữ liệu để bảo đảm an toàn hệ thống khi có sự cố xảy ra.

- Theo Điều 13 Khoản 5 Thông tư 24/2014/TT-BTTTT về Điều kiện về kỹ thuật cung cấp dịch vụ trò chơi điện tử G1 quy định: Có phương án bảo đảm an toàn, an ninh thông tin và bí mật thông tin cá nhân của người chơi.

2.6. Nhận xét về thực trạng áp dụng tiêu chuẩn an toàn đối với hệ thống thông tin tại Công ty X

Là một công ty chuyên sản xuất và phân phối game, do 5 thành viên sáng lập vào năm 2013, Công ty X đã và đang phấn đấu là công ty có vị thế tại Việt Nam trong lĩnh vực sản xuất game. Khi mà đa số các công ty game lớn ở Việt Nam đang tiến hành kinh doanh dựa trên nhập game nước ngoài rồi phân phối tại thị trường Việt Nam, thì Công ty X đã chọn hướng đi riêng, với tinh thần hướng tới mục tiêu người Việt chơi game do người Việt tự sản xuất. Công ty X có nhiều sản phẩm có chỗ đứng trên thị trường Việt Nam, từng bước đưa sản phẩm ra quốc tế và đặc biệt đã từng đạt giải nhất cuộc thi Blue Bird do VTV3 tổ chức vào năm 2015.

Khởi đầu công ty là một công ty startup, đến nay đã phát triển được với hơn 50 nhân viên. Khi mà quy mô công ty ngày càng lớn mạnh, Công ty X đã bắt đầu nhận thức rõ được các rủi ro và nguy cơ tiềm ẩn từ hệ thống CNTT và luôn xem đây là một khía cạnh quan trọng cần được quan tâm đúng mức. Hiện tại công ty

chưa áp dụng hay thực hiện các tiêu chuẩn đối với hệ thống quản lý an toàn thông tin của mình, mà mọi việc như thiết lập, xây dựng, điều hành hay giám sát hệ thống thông tin đều thực hiện một cách tự phát, bằng kinh nghiệm có được của các thành viên sáng lập.

Luận văn sẽ tiến hành khảo sát hệ thống an toàn thông tin của công ty X, và áp dụng các tiêu chuẩn ISO27001 đối với hệ thống quản lý an toàn thông tin tại công ty X.

2.7. Khảo sát công ty X về đảm bảo an toàn thông tin

Theo định nghĩa của ISO, thông tin là một loại tài sản, cũng như các loại tài sản quan trọng khác của một doanh nghiệp, có giá trị cho một tổ chức và do đó, cần có nhu cầu để bào vệ thích hợp. An toàn thông tin là bảo vệ thông tin trước nguy cơ mất an toàn nhằm đảm bảo tính liên tục trong hoạt động kinh doanh của doanh nghiệp, giảm thiểu sự phá hoại doanh nghiệp và gia tăng tới mức tối đa các cơ hội kinh doanh và đầu tư phát triển.

Thông tin và dữ liệu mà con người hiểu được tồn tại dưới nhiều dạng khác nhau, ví dụ như các số, các ký tự văn bản, âm thanh, hình ảnh, tài liệu, giấy tờ..., được truyền đi qua đường bưu điện, công văn hoặc dùng thư điện tử. Nhưng cho dù thông tin tồn tại dưới dạng nào đi chăng nữa, thông tin được đưa ra với 2 mục đích chính là chia sẻ và lưu trữ, nó luôn luôn cần sự bảo vệ nhằm đảm bảo sự an toàn thích hợp.

An toàn thông tin đạt được bằng cách triển khai tập hợp các kiểm soát phù hợp, bao gồm các biện pháp kỹ thuật, các chính sách, nội quy, quy định của doanh nghiệp và đặc biệt quan trọng nhất là yếu tố con người như: nhận thức, đào tạo và các kỹ năng cần thiết. Các kiểm soát này được xây dựng dựa trên kết quả của quá trình đánh giá rủi ro về an toàn thông tin. Tổ chức sử dụng đánh giá rủi ro để xác định các lỗ hổng, mức độ của các nguy cơ tiềm năng gắn với hệ thống CNTT. Kết quả của quả trình này giúp xác định ra các kiểm soát thích hợp nhằm giảm thiểu hoặc loại trừ rủi ro trong quá trình xử lý rủi ro.

Mục đích của quá trình đánh giá rủi ro nhằm:

- Xác định và nhận biết các rủi ro đối với tài sản CNTT.

- Đánh giá mức độ ảnh hường của rủi ro (nếu xảy ra) đối với tài sản CNTT cũng như đối với hoạt động sản xuất kinh doanh.

- Xác định mức độ rủi ro chấp nhận được.

- Đề xuất các giải pháp xử lý rủi ro.

2.7.1. Phân loại tài sản CNTT

Bất kỳ thông tin nào, khi được lưu trữ hoặc xử lý, trên hệ thống CNTT đều cần phải được bảo vệ nhằm chống sự truy cập trái phép, tiết lộ, sửa đổi và tiêu hủy.

Các thông tin sẽ có mức độ quan trọng khác nhau,do đó cần phân loại thông tin dựa trên mức độ cần thiết (quan trọng), hoặc xác định giá trị của thông tin trong tổ chức để đưa ra cách thức bảo đảm an toàn cho thông tin

a. Phân loại tài sản đặc điểm tài sản:

-Tài sản phần cứng: Các thiết bị thông thường (PC, laptop, các loại máy in, máy fax, các loại máy scanner), máy chủ (các loại máy chủ Small, Medium, Big), các thiết bị mạng thông thường (Switch, Router), Các thiết bị bảo mật (Firewall, Proxy, QoS), các thiết bị lưu trữ (tape, ổ đĩa, CD-ROM3 SAN), hệ thống mạng cáp nội bộ (bên trong các tòa nhà).

Tài sản phần mềm: phần mềm hệ thống (Antivirus, Office), phần mềm cơ sở dữ liệu (MySQL, Oracle), hệ thống phần mềm nghiệp vụ (HOST, E-banking, VCB-salary,...).

-Tài sản văn bản giấy.

-Tài sản thông tin: dữliệu trong các cơ sở dữ liệu, các dữ liệu khác: các file dữ liệu (dạng Word, Excel, PDF, file ảnh) tạo ra bởi các bộ phận trên máy tính cá nhân.

Tài sản dịch vụ: dịch vụ đường truyền Internet.

Tài sản hỗ trợ: UPS, máy phát điện, hệ thống PCCC.

b. Phân loại theo tính bảo mật

Thông tin công cộng: Nếu các thông tin này không có sẵn hoặc bị rò rỉ hay công bố ra bên ngoài tổ chức thì cũng không tạo ra ảnh hưởng gì. Đây thường là các thông tin mang tính truyền thông hoặc quảng bá. Ví dụ như tài liệu tiếp thị, quảng cáo, thông cáo báo chí...

Thông tin nội bộ: là những thông tin dùng cho tất cả mọi người/bộ phận trong phạm vi của doanh nghiệp. Nếu thông tin bị rò rỉ ra ngoài tổ chức sẽ không gây tổn thất nhiều về mặt tài chính hoặc hình ảnh của doanh nghiệp. Tuy nhiên, việc công bố các thông tin này không được khuyến khích.

Thông tin mật: Là những thông tin nếu như bị rò rỉ ra bên ngoài doanh nghiệp, sẽ ảnh hưởng đáng kể về mặt tài chính, pháp lý hoặc hình ảnh của doanh nghiệp.

Việc tiếp cận các thông tin này cần phải được hạn chế và được sự cho phép của người quản lý. Trong trường hợp có nhu cầu cung cấp thông tin cho bên thứ ba cần phải ký các bản cam kết bảo mật thông tin.

Thông tin tuyệt mật: Là những thông tin mà việc tiết lộ hoặc công bố sẽ ảnh hưởng rất lớn về mặt tài chính, pháp lý hoặc hình ảnh của doanh nghiệp. Ví dụ: Các chiến lược, kế hoạch kinh doanh, kế hoạch phát triển sản phẩm có thể được xếp vào nhóm này.

2.7.2. Các bước đánh giá rủi ro tài sản CNTT

Bước 1: Mô tả tài sản và các giá trị tương ứng với tài sản

Bước 2: Xác định các điểm yếu

Các điểm yếu có thể được xác định từ một trong số các nguồn sau:

Phân tích các kiểm soát trong tiêu chuẩn ISO27001.

Phân tích nguyên nhân gây ra sự cố an toàn thông tin xảy ra tại Công ty X và các tổ chức khác.

Khuyến cáo về an toàn thông tin của cơ quan quản lý nhà nước và các tổ chức khác.

Phát hiện của nhân viên tại Công ty X.

Bước 3: Xác định các nguy cơ

Các nguy cơ có thể được xác định từ một trong số các nguồn sau:

Phân tích các kiểm soát trong tiêu chuẩn ISO27001.

Phân tích nguyên nhân gây ra sự cố an toàn thông tin xảy ra tại Công ty X và các tổ chức khác.

Khuyến cáo về an toàn thông tin của cơ quan quản lý nhà nước và các tổ chức khác.

Phát hiện của nhân viên tại Công ty X.

Bước 4: Xác định khả năng xuất hiện của nguy cơ

Bước 5: Xác định giá trị rủi ro

Giá trị rủi ro = Khả năng xuất hiện của nguy cơ * Giá trị tài sản

Bước 6: Đề xuất các kiểm soát và lựa chọn xử lý rủi ro

Trong đó:

- C: tính bảo mật, được xác định bằng

Bảng 2.1 Bảng giá trị tính bảo mật

Giá trị	Mô tả
1	Thông tin công khai
2	Thông tin nhạy cảm, chỉ được sử dụng trong nội bộ
3	Thông tin nhạy cảm, chỉ được sử dụng bởi quản lý cấp cao

- I: tính toàn vẹn, được xác định bằng

Bảng 2.2 Bảng giá trị tính toàn vẹn

Giá trị	Mô tả
1	Thông tin được phép xóa hoặc sửa trong nội bộ
2	Thông tin được phép xóa hoặc sửa phòng chức năng liên quan
3	Thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép

- A: tính sẵn sàng, được xác định bằng

Bảng 2.3 Bảng giá trị tính sẵn sàng

Giá trị	Mô tả
1	Sẵn sàng đáp ứng trong 25% số giờ làm việc
2	Sẵn sàng đáp ứng từ 25% đến 75% số giờ làm việc
3	Sẵn sàng đáp ứng trên 75% số giờ làm việc

- Tỷ lệ xảy ra, được xác định bằng

Bảng 2.4 Bảng giá trị tỷ lệ xảy ra

Giá trị	Mô tả
1	Khả năng xảy ra thấp
2	Khả năng xảy ra trung bình
3	Khả năng xảy ra lớn

- AV: giá trị tài sản, được tính bằng công thức MAX(C, I, A)

- Giá trị rủi ro = AV (Giá trị tài sản) * Tỷ lệ xảy ra

- Với từng nguy cơ, sẽ tiến hành áp dụng biện pháp kiểm soát khi giá trị rủi ro tương ứng có giá trị lớn hơn hoặc bằng 4.

Bảng 2.5 Bảng giá trị rủi ro

Phân loại tài sản	STT	Tên tài sản	C	I	A	AV	Các điểm yếu, lỗ hổng	Nguy cơ	Tỷ lệ xảy ra	Giá trị rủi ro	Biện pháp kiểm soát
Tài sản thông tin	1	Cơ sở dữ liệu khách hàng, cơ sở dữ liệu người chơi, cơ sở dữ liệu nhân viên	3	3	3	3	Thiếu quy trình kiểm soát phân quyền, truy cập (có nhiều người trong nội bộ cùng có quyền truy cập)	Có thể có nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đối với cơ sở dữ liệu nhưng truy cập trái phép thông tin trên cơ sở dữ liệu	3	9	CÓ
							Thiếu quy trình cho việc backup dữ liệu	Mất dữ liệu do xóa nhầm, do bị virus tấn công, không đảm bảo Khoản 2 Điều 6 Thông tư 24 của Bộ Thông tin và Truyền thông về Quy định chi tiết về hoạt động quản lý, cung cấp và sử dụng dịch vụ trò chơi điện tử trên mạng quy định: thông tin cá nhân người chơi phải được lưu trữ backup 6 tháng sau khi người chơi ngừng sử dụng dịch vụ.	2	6	CÓ
							Thiếu kiểm soát việc sao chép	Rò rỉ thông tin do nhân viên có chức năng, nhiệm vụ và trách nhiệm liên quan lấy dữ liệu từ cơ sở dữ liệu về máy tính và sao chép ra thiết bị lưu trữ cá nhân mang ra khỏi công ty.	2	6	CÓ

Phân loại tài sản	STT	Tên tài sản	C	I	A	AV	Các điểm yếu, lỗ hổng	Nguy cơ	Tỷ lệ xảy ra	Giá trị rủi ro	Biện pháp kiểm soát
							Khi nghỉ việc, người quản lý cũ quên không bàn giao password cá nhân	Những nhân viên đã nghỉ việc vẫn có thể truy cập vào cơ sở dữ liệu khi không còn chức năng, nhiệm vụ và trách nhiệm liên quan nữa.	2	6	CÓ
							Password bảo vệ yếu	Dễ bị hacker tấn công để truy cập cơ sở dữ liệu bất hợp pháp.	2	6	CÓ
							Để chung cơ sở dữ liệu với file mềm cho phép pubic download	Dễ bị hacker tấn công để truy cập cơ sở dữ liệu bất hợp pháp.	1	3	KHÔNG
	2	Văn bản, công văn trao đổi trong nội bộ tổ chức	2	2	1	2	Thiếu quy trình kiểm soát phân quyền, truy cập (có nhiều người trong nội bộ cùng có quyền truy cập)	Có thể bị những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến văn bản, công văn nhưng xem, truy cập thông tin trái phép.	3	6	CÓ
							Thiếu kiểm soát việc sao lưu hay nhân bản tài liệu	Có thể bị những nhân viên có chức năng, nhiệm vụ và trách nhiệm liên quan đến văn bản, công văn nhưng sao chép, nhân bản tài liệu vì mục đích không tốt.	2	4	CÓ
							Bảo vệ vật lý yếu	Bị đột nhập, trộm cắp, phá hoại những văn bản, công văn	2	4	CÓ
							Giấy, dễ bị ảnh hưởng bởi độ ẩm, bụi	Rách, mủn, mờ do môi trường	1	2	KHÔNG

Phân loại tài sản	STT	Tên tài sản	C	I	A	AV	Các điểm yếu, lỗ hổng	Nguy cơ	Tỷ lệ xảy ra	Giá trị rủi ro	Biện pháp kiểm soát
							Thiếu cẩn thận khi hủy bỏ	Rò rỉ thông tin do những cá nhân không có chức năng, nhiệm vụ và trách nhiệm liên quan đến văn bản, công văn truy hồi, lấy lại thông tin vì mục đích không tốt.	1	2	KHÔNG
	3	Văn bản, công văn, hóa đơn, bảng kê khai thuế trao đổi với khách hàng bên ngoài	1	2	1	2	Bảo vệ vật lý yếu	Bị đột nhập, trộm cắp, phá hoại những văn bản, công văn	2	4	CÓ
							Giấy, dễ bị ảnh hưởng bởi độ ẩm, bụi	Rách, mủn, mờ do môi trường	1	2	KHÔNG
	4	Chiến lược phát triển kinh doanh, thông tin đối thủ cạnh tranh, thông tin về lương, thưởng của nhân viên… bằng giấy	3	2	2	3	Thiếu quy trình kiểm soát phân quyền, truy cập (có nhiều người trong nội bộ cùng có quyền truy cập)	Có thể bị những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến chiến lược phát triển kinh doanh, thông tin đối thủ cạnh tranh, thông tin về lương, thưởng của nhân viên… nhưng xem, truy cập thông tin trái phép để cung cấp cho những đối thủ cạnh tranh.	3	9	CÓ
							Thiếu kiểm soát việc sao lưu hay nhân bản tài liệu	Có thể bị những nhân viên có chức năng, nhiệm vụ và trách nhiệm liên quan đến văn bản, công văn nhưng sao chép, nhân bản tài liệu vì mục đích không tốt.	2	6	CÓ

Phân loại tài sản	STT	Tên tài sản	C	I	A	AV	Các điểm yếu, lỗ hổng	Nguy cơ	Tỷ lệ xảy ra	Giá trị rủi ro	Biện pháp kiểm soát
							Bảo vệ vật lý yếu	Bị đột nhập, trộm cắp, phá hoại những chiến lược phát triển kinh doanh, thông tin đối thủ cạnh tranh, thông tin về lương, thưởng của nhân viên…	2	6	CÓ
							Giấy, dễ bị ảnh hưởng bởi độ ẩm, bụi	Rách, mủn, mờ do môi trường.	1	3	KHÔNG
							Thiếu kiểm soát việc người phụ trách trực tiếp đem tài liệu về nhà	Có thể bị rò rỉ thông tin ra ngoài do người phụ trách trực tiếp mang về nhà nhưng kiểm soát tài liệu không tốt.	2	6	CÓ
							Thiếu cẩn thận khi hủy bỏ	Rò rỉ thông tin do những cá nhân không có chức năng, nhiệm vụ và trách nhiệm liên quan đến chiến lược phát triển kinh doanh, thông tin đối thủ cạnh tranh, thông tin về lương, thưởng của nhân viên… truy hồi, lấy lại thông tin vì mục đích không tốt.	1	3	KHÔNG

Phân loại tài sản	STT	Tên tài sản	C	I	A	AV	Các điểm yếu, lỗ hổng	Nguy cơ	Tỷ lệ xảy ra	Giá trị rủi ro	Biện pháp kiểm soát
	5	Chiến lược phát triển kinh doanh, thông tin đối thủ cạnh tranh, thông tin về lương, thưởng của nhân viên… bằng file mềm (Word, Excel)	3	2	2	3	Thiếu quy trình kiểm soát phân quyền, truy cập (có nhiều người trong nội bộ cùng có quyền truy cập)	Có thể bị những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến chiến lược phát triển kinh doanh, thông tin đối thủ cạnh tranh, thông tin về lương, thưởng của nhân viên… nhưng xem, truy cập thông tin trái phép để cung cấp cho những đối thủ cạnh tranh.	3	9	CÓ
							Thiếu quy trình quản lý sự thay đổi	Tính sẵn sàng của thông tin bị ảnh hưởng: có thể những nhân viên khi cần lại lấy nhầm file không phải mới nhất hoặc khi cần lấy những file tại một thời điểm nào đó nhưng lại lấy nhầm file, không đảm bảo được thông tin được lấy được chính xác.	2	6	CÓ
							Thiếu kiểm soát người phụ trách trực tiếp đem tài liệu về nhà	Có thể người phụ trách trực tiếp copy dữ liệu file từ máy tính ra các thiết bị cá nhân rồi mang về nhà gây rò rỉ thông tin ra ngoài do kiểm soát tài liệu không tốt.	2	6	CÓ

Phân loại tài sản	STT	Tên tài sản	C	I	A	AV	Các điểm yếu, lỗ hổng	Nguy cơ	Tỷ lệ xảy ra	Giá trị rủi ro	Biện pháp kiểm soát
	6	File source code do lập trình viên tạo	3	3	3	3	Thiếu quy trình kiểm soát phân quyền, truy cập (có nhiều người trong nội bộ cùng có quyền truy cập)	Có thể bị những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến source code nhưng xem, truy cập thông tin trái phép vì mục đích riêng.	3	9	CÓ
							Thiếu quy trình quản lý sự thay đổI, thiếu việc đánh nhãn để biết được lịch sử của source code, source code nào là mới nhất	Lập trình viên get nhầm source code, phát triển trên bộ source code không phải là mới nhất, gây tổn thất về thời gian, công sức phát triển game của công ty.	3	9	CÓ
	7	File ảnh do designer tạo, file Word, Excel về kế hoạch dự án, tracking tiến độ, file quản lý issues… (những tài liệu liên quan đến dự án sản suất game) do các thành viên dự án phát triển game (thuộc phòng sản xuất game) tạo	2	3	3	3	Thiếu quy trình kiểm soát phân quyền, truy cập (có nhiều người trong nội bộ cùng có quyền truy cập)	Có thể bị những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến file ảnh do designer tạo, file Word, Excel về kế hoạch dự án, tracking tiến độ, file quản lý issues… (những tài liệu liên quan đến dự án sản suất game) do các thành viên dự án phát triển game (thuộc phòng sản xuất game) tạo nhưng xem, truy cập thông tin trái phép.	3	9	CÓ

Phân loại tài sản	STT	Tên tài sản	C	I	A	AV	Các điểm yếu, lỗ hổng	Nguy cơ	Tỷ lệ xảy ra	Giá trị rủi ro	Biện pháp kiểm soát
							Thiếu quy trình quản lý sự thay đổi	Tính sẵn sàng của thông tin bị ảnh hưởng: có thể những nhân viên design, quản lý dự án khi cần lại lấy nhầm file không phải mới nhất hoặc khi cần lấy những file tại một thời điểm nào đó nhưng lại lấy nhầm file, không đảm bảo được thông tin được lấy được chính xác hoặc mất thời gian trong việc tìm kiếm thông tin.	2	6	CÓ
							Thiếu kiểm soát người phụ trách trực tiếp đem tài liệu về nhà	Có thể người phụ trách trực tiếp copy dữ liệu file từ máy tính ra các thiết bị cá nhân rồi mang về nhà để làm thêm nhưng dễ gây rò rỉ thông tin ra ngoài do kiểm soát tài liệu không tốt.	2	6	CÓ

Phân loại tài sản	STT	Tên tài sản	C	I	A	AV	Các điểm yếu, lỗ hổng	Nguy cơ	Tỷ lệ xảy ra	Giá trị rủi ro	Biện pháp kiểm soát
	8	Tài liệu source code, ảnh, các tài liệu liên quan đến dự án sản xuất game… bằng giấy do phòng sản xuất game quản lý	2	3	3	3	Thiếu quy trình kiểm soát phân quyền, truy cập (có nhiều người trong nội bộ cùng có quyền truy cập)	Có thể bị những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến file ảnh do designer tạo, file Word, Excel về kế hoạch dự án, tracking tiến độ, file quản lý issues… (những tài liệu liên quan đến dự án sản suất game) do quản lý dự án (trưởng phòng sản xuất) tạo nhưng xem, truy cập thông tin trái phép.	3	9	CÓ
							Thiếu kiểm soát việc sao lưu hay nhân bản tài liệu	Có thể bị những nhân viên có chức năng, nhiệm vụ và trách nhiệm liên quan đến tài liệu source code, ảnh, các tài liệu liên quan đến dự án sản xuất game… bằng giấy do phòng sản xuất quản lý nhưng sao chép, nhân bản tài liệu vì mục đích không tốt.	2	6	CÓ
							Bảo vệ vật lý yếu	Bị đột nhập, trộm cắp, phá hoại những tài liệu source code, ảnh, các tài liệu liên quan đến dự án sản xuất game… bằng giấy do phòng sản xuất quản lý.	2	6	CÓ
							Giấy, dễ bị ảnh hưởng bởi độ ẩm, bụi	Rách, mủn, mờ do môi trường	1	3	KHÔNG

Phân loại tài sản	STT	Tên tài sản	C	I	A	AV	Các điểm yếu, lỗ hổng	Nguy cơ	Tỷ lệ xảy ra	Giá trị rủi ro	Biện pháp kiểm soát
							Thiếu kiểm soát việc người phụ trách trực tiếp đem tài liệu về nhà	Có thể người phụ trách trực tiếp mang tài liệu source code, ảnh, cái tài liệu liên quan đến dự án sản xuất game… về để làm thêm ở nhà nhưng dễ gây rò rỉ thông tin ra ngoài do kiểm soát tài liệu không tốt.	2	6	CÓ
							Thiếu cẩn thận khi hủy bỏ	Rò rỉ thông tin do những cá nhân không có chức năng, nhiệm vụ và trách nhiệm liên quan đến tài liệu source code, ảnh, tài liệu liên quan đến dự án sản xuất game… truy hồi, lấy lại thông tin vì mục đích không tốt.	1	3	KHÔNG
Tài sản phần cứng	9	Các thiết bị PC của công ty	2	2	3	3	Nhân viên không tắt máy khi rời khỏi máy	Có thể bị những cá nhân khác truy cập trái phép máy tính vì mục đích không tốt.	2	6	CÓ
							Thiếu kiểm soát cài đặt phần mềm vào máy PC của nhân viên	Dễ gây ra nhiễm, tán phát virus trong máy tính, nội bộ mạng của công ty do cài đặt những phần mềm không rõ nguồn gốc trên mạng.	2	6	CÓ

Phân loại tài sản	STT	Tên tài sản	C	I	A	AV	Các điểm yếu, lỗ hổng	Nguy cơ	Tỷ lệ xảy ra	Giá trị rủi ro	Biện pháp kiểm soát
							Thiếu kiểm soát sao chép dữ liệu từ máy tính ra thiết bị lưu trữ ngoài	Dễ gây rò rỉ những thông tin quan trọng, cần bảo mật, quyết định sống còn đến chiến lược phát triển công ty ra ngoài.	2	6	CÓ
							Các mã độc hại có thể lây nhiễm sang các máy tính	Rò rỉ thông tin	1	3	KHÔNG
							Không cập nhật thường xuyên phần mềm chống virus	Dễ bị virus	1	3	KHÔNG
	10	Các thiết bị laptop của nhân viên mang đến công ty	2	2	3	3	Thiếu kiểm soát việc che thiết bị camera trên laptop của nhân viên	Bị phần mềm gián điệp của đối thủ cạnh tranh kích hoạt camera để thu các hình ảnh về công ty, các tài liệu liên quan đến công ty	2	6	CÓ
							Thiếu kiểm soát việc kết nối mạng của máy tính laptop của nhân viên vào mạng của công ty	Dễ bị virus lây nhiễm từ máy tính laptop của nhân viên vào mạng của công ty, gây phá hoại, đánh cắp thông tin trong nội bộ mạng của công ty.	2	6	CÓ
							Các mã độc hại có thể lây nhiễm sang các máy tính	Rò rỉ thông tin	1	3	KHÔNG
							Không cập nhật thường xuyên phần mềm chống virus	Dễ bị virus	1	3	KHÔNG

Phân loại tài sản	STT	Tên tài sản	C	I	A	AV	Các điểm yếu, lỗ hổng	Nguy cơ	Tỷ lệ xảy ra	Giá trị rủi ro	Biện pháp kiểm soát
							Thiếu biện pháp kiểm soát việc mang máy tính cá nhân ra, vào hàng ngày	Dễ lây nhiễm virus, nhân viên mang việc, tài liệu quan trọng về nhà làm rồi kiểm soát không cẩn thận, gây rò rỉ thông tin, ảnh hưởng đến việc kinh doanh của công ty.	2	6	CÓ
	11	Thiết bị wacom dùng cho các designer vẽ	1	2	2	2	Thiếu sự bảo quản cần thiết sau khi dùng xong	Dễ bị đánh cắp, mất tài sản	2	4	CÓ
							Thiếu chính sách sử dụng tài sản	Dễ bị sử dụng không đúng mục đích của những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến thiết bị wacom.	1	2	KHÔNG
	12	Các thiết bị máy in, máy scanner	1	1	1	1	Thiếu chính sách sử dụng tài sản	Dễ bị sử dụng không đúng mục đích của những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến các thiết bị máy in, máy scanner.	1	1	KHÔNG
	13	Thiết bị máy fax	2	1	1	2	Thiếu chính sách sử dụng tài sản	Dễ bị sử dụng không đúng mục đích của những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến thiết bị máy fax.	1	2	KHÔNG

Phân loại tài sản	STT	Tên tài sản	C	I	A	AV	Các điểm yếu, lỗ hổng	Nguy cơ	Tỷ lệ xảy ra	Giá trị rủi ro	Biện pháp kiểm soát
	14	Máy chủ game, máy chủ cơ sở dữ liệu	3	3	3	3	Thuê phần cứng và chỗ đặt tại Viettel, nhà cung cấp dịch vụ Data Center đảm bảo chất lượng nên không có điểm yếu, lỗ hổng	Không có	1	3	KHÔNG
	15	Máy chủ web về công ty, sản phẩm, dịch vụ, trang tải	2	2	3	3	Thuê phần cứng và chỗ đặt tại Viettel, nhà cung cấp dịch vụ Data Center đảm bảo chất lượng nên không có điểm yếu, lỗ hổng	Không có	1	3	KHÔNG
	16	Các thiết bị mạng thông thường (Switch, Router)	2	1	2	2	Thiếu chính sách sử dụng tài sản	Dễ bị sử dụng không đúng mục đích của những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến các thiết bị mạng thông thường (Switch, Router).	1	2	KHÔNG
	17	Thiết bị bảo mật Firewall	2	2	2	2	Thiếu chính sách sử dụng tài sản	Dễ bị sử dụng không đúng mục đích của những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến thiết bị bảo mật Firewall.	1	2	KHÔNG
	18	Các thiết bị lưu trữ (USB, ổ cứng, CD-	2	2	1	2	Thiếu sự bảo vệ vật lý	Có thể bị đột nhập, trộm cắp và phá hoại tài sản	2	4	CÓ

Phân loại tài sản	STT	Tên tài sản	C	I	A	AV	Các điểm yếu, lỗ hổng	Nguy cơ	Tỷ lệ xảy ra	Giá trị rủi ro	Biện pháp kiểm soát
		ROM)					Thiếu chính sách sử dụng tài sản	Dễ bị sử dụng không đúng mục đích của những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến các thiết bị lưu trữ (USB, ổ cứng, CD-ROM).	2	4	CÓ
	19	Các máy điện thoại để test game	2	2	2	2	Thiếu sự bảo vệ vật lý	Có thể bị đột nhập, trộm cắp và phá hoại tài sản	2	4	CÓ
							Thiếu chính sách sử dụng tài sản	Dễ bị sử dụng không đúng mục đích của những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến các máy điện thoại để test game.	2	4	CÓ
							Thiếu kiểm soát cài đặt phần mềm	Có thể các điện thoại test game của công ty bị nhiễm virus do việc cài đặt các phần mềm không rõ nguồn gốc từ trên mạng, gây tán phát virus trong nội bộ mạng của công ty.	1	2	KHÔNG
	20	Hệ thống cửa từ thẻ ra vào	2	2	2	2	Không có phụ tùng thay thế khi hỏng	Có thể hệ thống kiểm soát cửa ra vào công ty bị vô hiệu hóa, gây khó khăn trong việc kiểm soát ra vào của công ty trong một thời gian nhất định.	1	2	KHÔNG

Phân loại tài sản	STT	Tên tài sản	C	I	A	AV	Các điểm yếu, lỗ hổng	Nguy cơ	Tỷ lệ xảy ra	Giá trị rủi ro	Biện pháp kiểm soát
	21	Điện thoại cá nhân của nhân viên mang đến công ty	1	1	2	2	Không được kiểm soát chặt chẽ về việc sử dụng tại công ty	Có thể bị nhân viên sử dụng điện thoại để chụp, quay hình, nghe lén những thông tin quan trọng, quyết định lớn đến chiến lược kinh doanh của công ty, gây rò rỉ, tán phát ra ngoài vì mục đích xấu.	3	6	CÓ
Tài sản phần mềm	21	Phần mềm hệ thống (Antivirus, Office)	2	1	2	2	Phần mềm chưa được cập nhật mới nhất	Có thể phần mềm đang sử dụng vẫn còn những lỗi tiềm ẩn, hoặc phần mềm mới có những chức năng cần thiết đến nhu cầu sử dụng của công ty nhưng công ty không được sử dụng do không sử dụng phần mềm mới nhất.	1	2	KHÔNG
	22	Phần mềm cơ sở dữ liệu (MySQL, Oracle)	2	1	2	2	Phần mềm chưa được cập nhật mới nhất	Có thể phần mềm đang sử dụng vẫn còn những lỗi tiềm ẩn, hoặc phần mềm mới có những chức năng cần thiết đến nhu cầu sử dụng của công ty nhưng công ty không được sử dụng do không sử dụng phần mềm mới nhất.	1	2	KHÔNG
	23	Phần mềm phát triển (Java, Android, Windows Phone)	2	1	2	2	Phần mềm chưa được cập nhật mới nhất	Có thể phần mềm đang sử dụng vẫn còn những lỗi tiềm ẩn, hoặc phần mềm mới có những chức năng cần thiết đến nhu cầu sử	1	2	KHÔNG

Phân loại tài sản	STT	Tên tài sản	C	I	A	AV	Các điểm yếu, lỗ hổng	Nguy cơ	Tỷ lệ xảy ra	Giá trị rủi ro	Biện pháp kiểm soát
								dụng của công ty nhưng công ty không được sử dụng do không sử dụng phần mềm mới nhất, ảnh hưởng đến chất lượng phát triển game của công ty.			
	24	Hệ thống phần mềm nghiệp vụ (Unity, Photoshop)	2	1	2	2	Thiếu kiểm soát việc sao chép	Có thể những phần mềm do công ty mua bản quyền nhưng được sao chép, sử dụng bừa bãi không đúng mục đích.	2	4	CÓ
	25	Phần mềm game do công ty sản xuất: Kungfu Feet, Jewel Pandora, Kingdom Reborn	2	3	3	3	Thiếu kiểm soát việc sao chép	Có thể những phần mềm do công ty phát triển nhưng chưa công bố ra thị trường đã bị tán phát, gây ảnh hưởng đến bí mật kinh doanh của công ty.	2	6	CÓ
Tài sản con người	26	Các thành viên hội đồng quản trị	1	3	2	3	Thiếu kiến thức về an toàn thông tin	Nhận thức về đảm bảo an toàn thông tin trong công ty yếu, khó quản lý nhân viên trong việc đảm bảo an toàn thông tin.	3	9	CÓ
	27	Giám đốc	1	3	2	3	Thiếu kiến thức về an toàn thông tin	Nhận thức về đảm bảo an toàn thông tin trong công ty yếu, khó quản lý nhân viên trong việc đảm bảo an toàn thông tin.	3	9	CÓ

Phân loại tài sản	STT	Tên tài sản	C	I	A	AV	Các điểm yếu, lỗ hổng	Nguy cơ	Tỷ lệ xảy ra	Giá trị rủi ro	Biện pháp kiểm soát
	28	Trưởng các phòng sản xuất, kinh doanh và hành chính nhân sự	1	2	2	2	Thiếu kiến thức về an toàn thông tin	Nhân viên làm việc dễ truy cập trái phép hoặc làm rò rỉ thông tin một cách thiếu ý thức	3	6	CÓ
	29	Nhân viên	1	2	2	2	Thiếu kiến thức về an toàn thông tin	Nhân viên làm việc dễ truy cập trái phép hoặc làm rò rỉ thông tin một cách thiếu ý thức	3	6	CÓ
							Dễ rời bỏ công ty	Sang làm việc cho đối thủ canh tranh	2	4	CÓ
Tài sản hỗ trợ	30	Thiết bị cung cấp khi bị mất điện UPS	1	1	1	1	Không có phụ tùng thay thế khi hỏng	Trong trường hợp thiết bị UPS bị hỏng, ảnh hưởng đến năng suất, chất lượng, kết quả công việc của nhân viên trong công ty.	2	2	KHÔNG
	31	Hệ thống PCCC	1	1	1	1	Không có phụ tùng thay thế khi hỏng	Trong trường hợp hỏa hoạn mà hệ thống PCCC bị hỏng, dễ gây ra những thiệt hại về tài sản.	2	2	KHÔNG

CHƯƠNG 3.

ĐỀ XUẤT BỘ QUY TRÌNH CHO DOANH NGHIỆP SME ĐÃ CHỌN

Sau khi tiến hành khảo sát doanh nghiệp SME đã lựa chọn ở chương 2, chương này sẽ đề xuất xây dựng quy trình, chính sách, biện pháp, thủ tục… để đảm bảo an toàn thông tin, giải quyết các vấn đề liên quan đến an toàn thông tin mà doanh nghiệp trên gặp phải theo chuẩn ISO27001.

3.1. Đưa ra các biện pháp kiểm soát

Bảng 3.1 Các biện pháp kiểm soát đối ứng với các nguy cơ

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
1	Có thể có nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đối với cơ sở dữ liệu nhưng truy cập trái phép thông tin trên cơ sở dữ liệu	**Xây dựng chính sách Kiểm soát truy cập** **1. Đăng ký người sử dụng:** a) sử dụng một tên truy cập cá nhân duy nhất để người sử dụng có thể kết nối và chịu trách nhiệm với các hoạt động của mình; b) kiểm tra mức cho phép truy cập có phù hợp với mục đích doanh nghiệp và có nhất quán với chính sách an ninh của tổ chức; c) đưa cho người sử dụng một bản công bố quyền truy cập của họ; d) yêu cầu người sử dụng ký các bản kê để chỉ ra rằng họ hiểu các điều kiện truy cập; e) duy trì một bản lưu chính thức toàn bộ những người đăng ký sử dụng dịch vụ; f) bỏ quyền truy cập của người sử dụng ngay khi người sử dụng thay đổi công việc hoặc rời tổ chức; g) kiểm tra định kỳ để xóa bỏ các tên truy cập và tài khoản cá nhân không cần thiết; h) đảm bảo rằng các tên truy cập cá nhân dư thừa không được phát hành cho người sử dụng khác. **2. Quản lý đặc quyền:** a) xác định các đặc quyền kết hợp với cơ sở dữ liệu: ai có quyền View, ai có quyền Create, ai có quyền Update, ai có quyền Delete, và các đặc quyền đối với cơ sở dữ liệu được phân phối đối với nhân viên dựa trên vai trò và chức năng của họ; b) một quy trình cấp quyền và một bản lưu toàn bộ các đặc quyền được phân phối được bảo lưu. Các đặc quyền không nên được cho phép cho đến khi quy trình cấp quyền hoàn tất; **3. Quản lý mật khẩu người sử dụng:**	**An ninh cá nhân** **Giáo dục và đào tạo an ninh thông tin** Toàn bộ các nhân viên của công ty được đào tạo thích hợp và các cập nhật thường xuyên về chính sách và thủ tục của tổ chức, được đào tạo việc sử dụng đúng các phương tiện xử lý thông tin trước khi truy cập tới thông tin cơ sở dữ liệu.

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
		a) yêu cầu người sử dụng ký kết một bản cam kết để giữ bí mật các mật khẩu cá nhân (điều này có thể thêm vào trong các điều khoản và điều kiện thuê nhân công); b) đảm bảo rằng lúc đầu họ được cung cấp một mật khẩu tạm thời an toàn mà họ buộc phải thay đổi ngay lập tức; c) yêu cầu đưa các mật khẩu tạm thời cho người sử dụng một cách an toàn. Người sử dụng nên thông báo đã nhận được các mật khẩu. **4. Soát xét các quyền truy cập của người sử dụng** a) quyền truy cập của người sử dụng được soát xét sau mỗi khoảng thời gian đều đặn định kỳ 6 tháng và sau bất kỳ sự thay đổi nào; b) việc cấp đặc quyền truy cập đặc biệt được soát xét sau khoảng thời gian ngắn hơn, định kỳ 3 tháng; c) phân phối đặc quyền được kiểm tra thường sau mỗi khoảng thời gian đều đặn để đảm bảo rằng không có các đặc quyền trái phép.	
2	Mất dữ liệu do xóa nhầm, do bị virus tấn công, không đảm bảo Khoản 2 Điều 6 Thông tư 24 của Bộ Thông tin và Truyền thông về Quy định chi tiết về hoạt động quản lý, cung cấp và sử dụng dịch vụ trò chơi điện tử trên mạng quy định: thông tin cá nhân người chơi phải được lưu trữ backup 6 tháng sau khi người chơi ngừng sử dụng dịch vụ.	**Xây dựng chính sách Quản lý truyền thông và hoạt động** **Sao lưu thông tin** a) Technical leader của công ty là người sẽ tiến hành thực hiện sao lưu, kiểm tra việc thực hiện sao lưu. b) mức thông tin sao lưu nhỏ nhất, sao lưu toàn bộ dữ liệu cơ sở dữ liệu có được, cùng với lưu trữ các bản sao chép dự phòng và các thủ tục lưu trữ được ghi chép lại chính xác và đầy đủ nên được lưu ở một nơi tách biệt, với khoảng cách đủ để thoát khỏi các hư hại do một tai hoạ xảy ra ở vị trí chính. c) nếu có thể, tool thực hiện backup nên được kiểm tra đều đặn để đảm bảo rằng chúng có thể chông cậy được trong lúc khẩn cấp khi cần; d) việc tiến hành sao lưu cơ sở dữ liệu phải đảm bảo ít nhất 6 tháng kể từ khi người chơi ngừng sử dụng dịch vụ và việc sao lưu được tiến hành hàng ngày vào ban đêm (khi hệ thống dịch vụ game ít người chơi truy cập nhất)	**An ninh cá nhân** **Kỹ thuật:** Dùng tool backup tự động (tool mua có bản quyền) **Giáo dục và đào tạo an ninh thông tin** Technical leader được đào tạo thích hợp và cập nhật thường xuyên về chính sách và thủ tục của tổ chức, được đào tạo việc sử dụng các tool backup để thực hiện việc sao lưu cơ sở dữ liệu.
3	Rò rỉ thông tin do nhân viên có chức năng, nhiệm vụ và trách		

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
	nhiệm liên quan lấy dữ liệu từ cơ sở dữ liệu về máy tính và sao chép ra thiết bị lưu trữ cá nhân mang ra khỏi công ty.		
4	Những nhân viên đã nghỉ việc vẫn có thể truy cập vào cơ sở dữ liệu khi không còn chức năng, nhiệm vụ và trách nhiệm liên quan nữa.	Bổ sung vào chính sách Kiểm soát truy cập, mục Đăng ký người sử dụng nội dung: bỏ quyền truy cập của người sử dụng ngay khi người sử dụng thay đổi công việc hoặc rời tổ chức;	
5	Dễ bị hacker tấn công để truy cập cơ sở dữ liệu bất hợp pháp.	Bổ sung vào chính sách Kiểm soát truy cập, mục Sử dụng mật khẩu Tất cả những nhân viên, cá nhân khi được cung cấp mật khẩu để truy cập cơ sở dữ liệu phải: a) giữ bí mật các mật khẩu; b) tránh giữ lại một tờ giấy ghi mật khẩu, trừ phi nó được lưu giữ an toàn; c) thay đổi mật khẩu bất kỳ lúc nào có dấu hiệu hệ thống hoặc mật khẩu có thể bị tổn hại; d) chọn các mật khẩu có chất lượng với độ dài ít nhất 6 ký tự và: 1) dễ nhớ; 2) không dựa trên bất kỳ cái gì mà một ai khác có thể dễ dàng đoán ra hoặc có được các thông tin liên quan đến cá nhân, ví dụ tên, số điện thoại, ngày sinh v..v.; 3) tránh các nhóm ký tự giống nhau liên tiếp hoặc các số hoặc các chữ cái. e) thay đổi các mật khẩu sau mỗi khoảng thời gian đều đặn hoặc theo những lần truy cập (các mật khẩu của cá tài khoản đặc quyền nên được thay đổi thường xuyên hơn các mật khẩu thông thường) và tránh sử dụng lại, quay lại các mật khẩu cũ; f) thay đổi mật khẩu tạm thời vào lần khởi động đầu tiên; g) không tính đến các mật khẩu trong bất kỳ quá trình khởi động tự động hoá nào, ví dụ được lưu trữ trong một phím chức năng hoặc macro; h) không chia sẻ các mật khẩu cá nhân.	Toàn bộ các nhân viên, cá nhân liên quan của công ty được đào tạo thích hợp và các cập nhật thường xuyên về chính sách và thủ tục của tổ chức, được đào tạo việc sử dụng các chính sách, quy trình về việc sử dụng mật khẩu truy cập tới cơ sở dữ liệu.

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
6	Có thể bị những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến văn bản, công văn nhưng xem, truy cập thông tin trái phép.	**Xây dựng chính sách An ninh môi trường và vật lý** **1. Vành đai an ninh vật lý:** a) Vành đai an ninh được thiết lập rõ ràng: văn bản, công văn trao đổi trong nội bộ công ty được lưu trữ trong tủ kính, chống cháy, có khóa và được đặt trong phòng riêng, do người phụ trách của phòng hành chính, nhân sự quản lý, phòng ra vào có cơ chế kiểm soát bằng thẻ từ. **2. Kiểm soát xâm nhập vật lý:** a) các khách đến các khu vực an ninh nên được giám sát hoặc rà soát và ghi lại ngày giờ ra vào của họ. Họ chỉ được cho phép truy cập vì các mục đích cụ thể. b) truy cập tới các công văn, văn bản được kiểm soát và hạn chế chỉ cho các cá nhân được cấp phép. c) các quyền truy cập tới các khu vực an ninh nên được xem xét và cập nhật một cách đều đặn. **3. Kiểm soát chung:** a) KHI THÍCH HỢP, công văn và các văn bản trao đổi trong nội bộ công ty do các cá nhân liên quan lưu nên được lưu trữ trong các tủ có khoá riêng của cá nhân, đặc biệt ngoài giờ làm việc;	**Kỹ thuật:** Lắp đặt thẻ từ đối với phòng lưu trữ công văn, văn bản trao đổi trong công ty. **Con người:** Toàn bộ các nhân viên, cá nhân liên quan của công ty được đào tạo, giải thích về các khu vực an ninh và được chỉ dẫn về các yêu cầu an ninh của khu vực đó.
7	Có thể bị những nhân viên có chức năng, nhiệm vụ và trách nhiệm liên quan đến văn bản, công văn nhưng sao chép, nhân bản tài liệu vì mục đích không tốt.	Bổ sung vào chính sách An ninh môi trường vật lý, mục Kiểm soát chung, nội dung: - các máy photo nên được khóa ngoài giờ làm việc chính thức (hoặc bảo đảm an toàn khỏi việc sử dụng trái phép bằng cách này cách khác); - thông tin nhạy cảm hoặc được phân loại, khi in xong nên được xoá ngay khỏi máy in.	
8	Bị đột nhập, trộm cắp, phá hoại những văn bản, công văn	Các biện pháp kiểm soát về An ninh môi trường và vật lý đã xây dựng ở trên đã giải quyết được nguy cơ này.	
9	Bị đột nhập, trộm cắp, phá hoại những văn bản, công văn	**Bổ sụng vào chính sách An ninh môi trường và vật lý** **1. Vành đai an ninh vật lý:** a) Vành đai an ninh được thiết lập rõ ràng: Văn bản, công văn, hóa đơn, bảng	**Kỹ thuật:** Lắp đặt thẻ từ đối với phòng lưu trữ văn bản, công văn, hóa đơn,

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
		kê khai thuế trao đổi với khách hàng bên ngoài được lưu trữ trong tủ kính, chống cháy, có khóa và được đặt trong phòng riêng, do người phụ trách của phòng hành chính, nhân sự quản lý, phòng ra vào có cơ chế kiểm soát bằng thẻ từ. **2. Kiểm soát xâm nhập vật lý:** a) các khách đến các khu vực an ninh nên được giám sát hoặc rà soát và ghi lại ngày giờ ra vào của họ. Họ chỉ được cho phép truy cập vì các mục đích cụ thể. b) truy cập tới các công văn, văn bản được kiểm soát và hạn chế chỉ cho các cá nhân được cấp phép. c) các quyền truy cập tới các khu vực an ninh nên được xem xét và cập nhật một cách đều đặn. **3. Kiểm soát chung:** a) KHI THÍCH HỢP, Văn bản, công văn, hóa đơn, bảng kê khai thuế trao đổi với khách hàng bên ngoài do các cá nhân liên quan lưu nên được lưu trữ trong các tủ có khoá riêng của cá nhân, đặc biệt ngoài giờ làm việc;	bảng kê khai thuế trao đổi với khách hàng bên ngoài.
10	Có thể bị những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến chiến lược phát triển kinh doanh, thông tin đối thủ cạnh tranh, thông tin về lương, thưởng của nhân viên… nhưng xem, truy cập thông tin trái phép để cung cấp cho những đối thủ cạnh tranh.	**Bổ sung vào chính sách An ninh môi trường và vật lý** **1. Vành đai an ninh vật lý:** a) Vành đai an ninh được thiết lập rõ ràng: Chiến lược phát triển kinh doanh, thông tin đối thủ cạnh tranh, thông tin về lương, thưởng của nhân viên… được lưu trữ trong tủ kính, chống cháy, có khóa và được đặt trong phòng riêng, do người phụ trách của phòng hành chính, tổng hợp và nhân sự quản lý. Phòng ra vào có cơ chế kiểm soát bằng thẻ từ. **2. Kiểm soát xâm nhập vật lý:** a) các khách đến các khu vực an ninh nên được giám sát hoặc rà soát và ghi lại ngày giờ ra vào của họ. Họ chỉ được cho phép truy cập vì các mục đích cụ thể. b) truy cập tới các công văn, văn bản được kiểm soát và hạn chế chỉ cho các cá nhân được cấp phép. c) các quyền truy cập tới các khu vực an ninh nên được xem xét và cập nhật một cách đều đặn. **3. Kiểm soát chung:** a) KHI THÍCH HỢP, chiến lược phát triển kinh doanh, thông tin đối thủ cạnh	**Kỹ thuật:** Lắp đặt thẻ từ đối với phòng lưu trữ tài liệu chiến lược phát triển kinh doanh, thông tin đối thủ cạnh tranh, thông tin về lương, thưởng của nhân viên… **Con người:** Toàn bộ các nhân viên, cá nhân liên quan của công ty được đào tạo, giải thích về các khu vực an ninh và được chỉ dẫn về các yêu cầu an ninh của khu vực đó.

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
		tranh, thông tin về lương, thưởng của nhân viên… do các cá nhân liên quan lưu nên được lưu trữ trong các tủ có khoá riêng của cá nhân, đặc biệt ngoài giờ làm việc;	
11	Có thể bị những nhân viên có chức năng, nhiệm vụ và trách nhiệm liên quan đến văn bản, công văn nhưng sao chép, nhân bản tài liệu vì mục đích không tốt.	Các biện pháp kiểm soát về An ninh môi trường và vật lý đã xây dựng ở trên đã giải quyết được nguy cơ này.	
12	Bị đột nhập, trộm cắp, phá hoại những chiến lược phát triển kinh doanh, thông tin đối thủ cạnh tranh, thông tin về lương, thưởng của nhân viên…	Các biện pháp kiểm soát về An ninh môi trường và vật lý đã xây dựng ở trên đã giải quyết được nguy cơ này.	
13	Có thể bị rò rỉ thông tin ra ngoài do người phụ trách trực tiếp mang về nhà nhưng kiểm soát tài liệu không tốt.	**Bổ sung vào phần Quản lý truyền thông và hoạt động, phần Kiểm soát chung nội dung:** a) những tài liệu, thiết bị, tài sản của công ty đều không được phép mang về nhà (điều này có thể thêm vào trong các điều khoản và điều kiện thuê nhân công).	
14	Có thể bị những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến chiến lược phát triển kinh doanh, thông tin đối thủ cạnh tranh, thông tin về lương, thưởng của nhân viên… nhưng xem, truy cập thông tin trái phép để cung cấp cho những đối thủ cạnh tranh.	**Xây dựng chính sách Sử dụng mạng máy tính nội bộ trong công ty** a) Chiến lược phát triển kinh doanh, thông tin đối thủ cạnh tranh, thông tin về lương, thưởng của nhân viên… bằng file mềm (Word, Excel) được lưu trữ trên một server nội bộ riêng của công ty. b) Trên máy server của mạng nội bộ công ty có các dạng thư mục dùng chung: - Thư mục tên các phòng: Phòng sản xuất, Phòng kinh doanh, Phòng hành chính tổng hợp + Dữ liệu trong thư mục do lãnh đạo, nhân viên các Phòng lưu trữ dùng để báo cáo lãnh đạo công ty, xử lý công tác nghiệp vụ.	Toàn bộ các nhân viên, cá nhân liên quan của công ty được đào tạo, giải thích về quy chế, chính sách sử dụng mạng máy tính nội bộ trong công ty và hướng dẫn thi hành.

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
		+ Loại dữ liệu lưu trữ là văn bản mềm, hình ảnh, video… phục vụ cho công việc. + Phân quyền truy cập được quy định cụ thể trong bảng phân quyền. (Sheet bảng phân quyền) - Thư mục Public + Thư mục dùng để chia sẻ, trao đổi dữ liệu giữa các phòng ban, cá nhân trong công ty. + Loại dữ liệu lưu trữ là văn bản mềm, hình ảnh, video… phục vụ cho công việc. + Thời gian lưu trữ: dữ liệu tại thư mục này chỉ được lưu trữ tạm thời và sẽ bị xóa sau một khoảng thời gian nhất định tùy thuộc vào dung lượng nhớ. + Phân quyền truy cập được quy định cụ thể trong bảng phân quyền. (Sheet bảng phân quyền) - Thư mục Nghiệp vụ + Thư mục này lưu trữ các phần mềm ứng dụng, dữ liệu của các nghiệp vụ (như kế toán, lương, văn thư…) + Thời gian lưu trữ: lâu dài + Phân quyền truy cập được quy định cụ thể trong bảng phân quyền. (Sheet bảng phân quyền)	
15	Tính sẵn sàng của thông tin bị ảnh hưởng: có thể những nhân viên khi cần lại lấy nhầm file không phải mới nhất hoặc khi cần lấy những file tại một thời điểm nào đó nhưng lại lấy nhầm file, không đảm bảo được thông tin được lấy được chính xác.	Các biện pháp kiểm soát về Sử dụng mạng máy tính nội bộ trong công ty ở trên đã giải quyết được nguy cơ này.	
16	Có thể người phụ trách trực	**Bổ sung vào phần An ninh môi trường và vật lý, phần An ninh cho các**	

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
	tiếp copy dữ liệu file từ máy tính ra các thiết bị cá nhân rồi mang về nhà gây rò rỉ thông tin ra ngoài do kiểm soát tài liệu không tốt.	**thiết bị ngoại vi** a) Nghiêm cấm việc sử dụng USB, thẻ nhớ trong nội bộ công ty, có thể niêm phong các ổ USB, thẻ nhớ. b) Nghiêm cấm việc cài đặt các phần mềm cho phép gửi file peer-to-peer, ngăn chặn các trang web cho phép upload, gửi file.	
17	Có thể bị những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến source code nhưng xem, truy cập thông tin trái phép vì mục đích riêng.	**Bổ sung vào chính sách Sử dụng mạng máy tính nội bộ trong công ty:** - Tạo thư mục Project, trong đó có chứa các thư mục con như Project 1, Project 2… + Sử dụng tool quản lý source code SVN, tài liệu do các thành viên trong cùng dự án tạo ra. + Nhân viên kỹ thuật sẽ setup server SVN và tạo tài khoản cho từng thành viên trong dự án. + Đầu ngày, developer sẽ get source code mới nhất về, merge source code của những developer khác với source code dưới máy local của mình. + Khi developer đang update file nào thì get lock file, để thông báo và ngăn không cho developer khác cũng update vào file này. + Cuối ngày, trước khi đi về, developer commit source code sau khi mình đã tạo mới, update lên server, đồng thời unlock file. + Mỗi thời điểm như release version mới, các milestone quan trọng… project leader của dự án sẽ tiến hành baseline source code, đánh tag để source code có thể lấy lại tại từng thời điểm theo sự kiện thời gian về sau. + Thời gian lưu trữ: lâu dài + Phân quyền truy cập được quy định cụ thể trong bảng phân quyền. (Sheet bảng phân quyền)	
18	Lập trình viên get nhầm source code, phát triển trên bộ source code không phải là mới nhất, gây tổn thất về thời gian, công sức phát triển game của công ty.	Các biện pháp kiểm soát về Sử dụng mạng máy tính nội bộ trong công ty xây dựng ở trên đã giải quyết được nguy cơ này.	

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
19	Có thể bị những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến file ảnh do designer tạo, file Word, Excel về kế hoạch dự án, tracking tiến độ, file quản lý issues… (những tài liệu liên quan đến dự án sản suất game) do các thành viên dự án phát triển game (thuộc phòng sản xuất game) tạo nhưng xem, truy cập thông tin trái phép.	**Bổ sung vào chính sách Sử dụng mạng máy tính nội bộ trong công ty:** - Tạo thư mục Project, trong đó có chứa các thư mục con như Project 1, Project 2…, trong các thư mục đó, tạo thư mục con Document để lưu trữ những tài liệu + Sử dụng tool quản lý SVN để quản lý những tài liệu do các thành viên trong cùng dự án tạo ra. + Nhân viên kỹ thuật sẽ setup server SVN và tạo tài khoản cho từng thành viên trong dự án. + Đầu ngày, các member trong đội dự án sẽ tài liệu mới nhất về máy local của mình. + Khi một member trong đội dự án đang update file nào thì get lock file, để thông báo và ngăn không cho các member trong đội dự án khác cũng update vào file này. + Cuối ngày, trước khi đi về, các member trong đội dự án commit source code sau khi mình đã tạo mới, update lên server, đồng thời unlock file. + Mỗi thời điểm như project leader của dự án sẽ tiến hành baseline tài liệu, đánh tag để các tài liệu có thể lấy lại tại từng thời điểm theo sự kiện thời gian về sau. + Thời gian lưu trữ: lâu dài + Phân quyền truy cập được quy định cụ thể trong bảng phân quyền. (Sheet bảng phân quyền)	
20	Tính sẵn sàng của thông tin bị ảnh hưởng: có thể những nhân viên design, quản lý dự án khi cần lại lấy nhầm file không phải mới nhất hoặc khi cần lấy những file tại một thời điểm nào đó nhưng lại lấy nhầm file, không đảm bảo được thông tin được lấy được chính xác hoặc mất thời gian trong việc tìm kiếm thông tin.	Các biện pháp kiểm soát về Sử dụng mạng máy tính nội bộ trong công ty xây dựng ở trên đã giải quyết được nguy cơ này.	

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
21	Có thể người phụ trách trực tiếp copy dữ liệu file từ máy tính ra các thiết bị cá nhân rồi mang về nhà để làm thêm nhưng dễ gây rò rỉ thông tin ra ngoài do kiểm soát tài liệu không tốt.	Các biện pháp kiểm soát về An ninh môi trường và vật lý xây dựng ở trên đã giải quyết được nguy cơ này.	
22	Có thể bị những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến file ảnh do designer tạo, file Word, Excel về kế hoạch dự án, tracking tiến độ, file quản lý issues… (những tài liệu liên quan đến dự án sản suất game) do quản lý dự án (trưởng phòng sản xuất) tạo nhưng xem, truy cập thông tin trái phép.	**Bổ sung vào chính sách An ninh môi trường và vật lý** **1. Vành đai an ninh vật lý:** a) Vành đai an ninh được thiết lập rõ ràng: Tài liệu source code, ảnh, các tài liệu liên quan đến dự án sản xuất game bằng giấy… được lưu trữ trong tủ kính, chống cháy, có khóa và được đặt trong phòng riêng, do người phụ trách của phòng sản xuất game quản lý, phòng ra vào có cơ chế kiểm soát bằng thẻ từ. **2. Kiểm soát xâm nhập vật lý:** a) các khách đến các khu vực an ninh nên được giám sát hoặc rà soát và ghi lại ngày giờ ra vào của họ. Họ chỉ được cho phép truy cập vì các mục đích cụ thể. b) truy cập tới các công văn, văn bản được kiểm soát và hạn chế chỉ cho các cá nhân được cấp phép. c) các quyền truy cập tới các khu vực an ninh nên được xem xét và cập nhật một cách đều đặn. **3. Kiểm soát chung:** a) KHI THÍCH HỢP, Tài liệu source code, ảnh, các tài liệu liên quan đến dự án sản xuất game bằng giấy… do các cá nhân liên quan lưu nên được lưu trữ trong các tủ có khoá riêng của cá nhân, đặc biệt ngoài giờ làm việc;	
23	Có thể bị những nhân viên có chức năng, nhiệm vụ và trách nhiệm liên quan đến tài liệu source code, ảnh, các tài liệu liên quan đến dự án sản xuất	**Bổ sung vào chính sách An ninh môi trường vật lý, mục Kiểm soát chung, nội dung:** a) các máy photo nên được khóa ngoài giờ làm việc chính thức (hoặc bảo đảm an toàn khỏi việc sử dụng trái phép bằng cách này cách khác); b) thông tin nhạy cảm hoặc được phân loại, khi in xong nên được xoá ngay	

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
	game… bằng giấy do phòng sản xuất quản lý nhưng sao chép, nhân bản tài liệu vì mục đích không tốt.	khỏi máy in.	
24	Bị đột nhập, trộm cắp, phá hoại những tài liệu source code, ảnh, các tài liệu liên quan đến dự án sản xuất game… bằng giấy do phòng sản xuất quản lý.	Các biện pháp kiểm soát về An ninh môi trường và vật lý xây dựng ở trên đã giải quyết được nguy cơ này.	
25	Có thể người phụ trách trực tiếp mang tài liệu source code, ảnh, cái tài liệu liên quan đến dự án sản xuất game… về để làm thêm ở nhà nhưng dễ gây rò rỉ thông tin ra ngoài do kiểm soát tài liệu không tốt.	**Bổ sung vào chính sách Quản lý truyền thông và hoạt động, nội dung:** - những tài liệu, thiết bị, tài sản của công ty đều không được phép mang về nhà (điều này có thể thêm vào trong các điều khoản và điều kiện thuê nhân công).	
26	Có thể bị những cá nhân khác truy cập trái phép máy tính vì mục đích không tốt.	**Bổ sung vào chính sách An ninh môi trường và vật lý, phần Kiểm soát chung:** - Chính sách màn hình "sạch": máy tính cá nhân và cổng in và các cổng khác của máy tính nên được đóng khi không dùng và nên được bảo vệ bằng các khóa mật mã, mật khẩu hoặc các kiểm soát khác khi không sử dụng.	
27	Dễ gây ra nhiễm, tán phát virus trong máy tính, nội bộ mạng của công ty do cài đặt những phần mềm không rõ nguồn gốc trên mạng.	**Bổ sung vào phần Quản lý truyền thông và hoạt động, phần Bảo vệ chống lại phần mềm cố ý gây hại:** a) một chính sách chính thức đòi hỏi tuân theo giấy phép phần mềm và ngăn cấm việc sử dụng trái phép phần mềm; - xuất bản một chính sách tuân thủ bản quyền phần mềm xác định việc sử dụng pháp lý các sản phẩm phần mềm và thông tin; - việc duy trì nhận thức về bản quyền phần mềm và các chính sách giành được và đưa ra thông báo về mục đích thự hiện hoạt động	

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
		- kỷ luật đối với các nhân viên vi phạm; b) một chính sách chính thức để bảo vệ chống lại cá rủi ro liên quan đến việc sử dụng các tệp và phần mềm từ cả các mạng bên ngoài hoặc trên bất kỳ phương tiện truyền thông khác, cho biết các biện pháp bảo vệ được sử dụng - chỉ mua các chương trình có nguồn đáng tin; - mua các chương trình có mã nguồn mà có thể được xác minh; - sử dụng các sản phẩm đã được đánh giá; c) việc lắp đặt và nâng cấp thông thường phần mềm chống virút và sửa chữa để quét máy vi tính d) chỉ đạo việc soát xét thông thường phần mềm và nội dụng dữ liệu của các hệ thống hỗ trợ các quá trình kinh doanh quyết định. Sự hiện diện của bất kỳ tệp không được chấp nhận hoặc các sửa đổi trái phép nên được điều tra một cách chính thức; e) kiểm tra virút bất kỳ tệp nào trên phương tiện truyền thông điện tử có nguồn gốc không rõ ràng hoặc trái phép hoặc các tệp nhận được từ các mạng không đáng tin trước khi sử dụng ; f) kiểm tra các phần mềm gây hại trên bất kỳ tệp gửi kèm thư điện tử hoặc các phần tải trên mạng trước khi sử dụng. Việc kiểm tra này nên được tiến hành ở nhiều vị trí khác nhau, ví dụ như các máy chủ thư điện tử, máy tính bàn hoặc ở các cổng mạng của tổ chức; g) các thủ tục quản lý và các trách nhiệm giải quyết vấn đề bảo vệ chống virút trên các hệ thống, đào tạo việc sử dụng, báo cáo và khắc phục sự tấn công của virút (xem 6.3 và 8.1.3); h) các kế hoạch liên tục trong kinh doanh phù hợp với việc khắc phục sự tấn công của virút, bao gồm toàn bộ dữ liệu cần thiết và phần mềm sao lưu và các sắp xếp khôi phục (xem mục 11); i) các thủ tục thẩm tra toàn bộ thông tin liên quan đến phần mềm có hại và đảm bảo rằng bản tin cảnh báo chính xác và đầy đủ thông tin. Các nhà quản lý nên đảm bảo rằng các nguồn đủ tiêu chuẩn, ví dụ các báo chí danh tiếng, các địa chỉ mạng hoặc các nhà cung cấp phần mềm diệt virút đáng tin, được sử dụng để phân biệt các trò lừa và virút thực. Nhân viên nên nhận thức được vấn đề về các trò lừa bịp và phải làm gì khi nhận được chúng.	

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
28	Dễ gây rò rỉ những thông tin quan trọng, cần bảo mật, quyết định sống còn đến chiến lược phát triển công ty ra ngoài.	Các biện pháp kiểm soát về An ninh môi trường và vật lý xây dựng ở trên đã giải quyết được nguy cơ này.	
29	Bị phần mềm gián điệp của đối thủ cạnh tranh kích hoạt camera để thu các hình ảnh về công ty, các tài liệu liên quan đến công ty	**Bổ sung vào chính sách An ninh môi trường và vật lý, phần An ninh thiết bị:** - Tất cả các máy tính có gắn camera khi sử dụng trong quá trình làm việc tại công ty phải gián giấy che.	
30	Dễ bị virus lây nhiễm từ máy tính laptop của nhân viên vào mạng của công ty, gây phá hoại, đánh cắp thông tin trong nội bộ mạng của công ty.	**Bổ sung vào chính sách Kiểm soát truy cập, phần Kiểm soát truy cập mạng:** Xây dựng Chính sách về sử dụng các dịch vụ mạng: a) các mạng và dịch vụ mạng được phép mới được truy cập; b) các thủ tục cấp phép để xác định rõ người được phép truy cập các mạng và dịch vụ mạng đó; c) các kiểm soát và thủ tục quản lý để bảo vệ truy cập tới các kết nối mạng và dịch vụ mạng.	
31	Dễ lây nhiễm virus, nhân viên mang việc, tài liệu quan trọng về nhà làm rồi kiểm soát không cẩn thận, gây rò rỉ thông tin, ảnh hưởng đến việc kinh doanh của công ty.	**Bổ sung vào chính sách An ninh môi trường và vật lý, phần An ninh thiết bị:** - Tất cả các nhân viên mang máy tính cá nhân ra, vào công ty phải được nhân viên kỹ thuật kiểm tra, được sự đồng ý của lãnh đạo	
32	Dễ bị đánh cắp, mất tài sản	**Bổ sung vào chính sách An ninh môi trường và vật lý, phần Vành đai an ninh vật lý:** - Vành đai an ninh được thiết lập rõ ràng: Thiết bị Wacom được lưu trữ trong tủ kính, chống cháy, có khóa và được đặt trong phòng riêng, do người phụ trách của phòng sản xuất game quản lý. Phòng ra vào có cơ chế kiểm soát bằng thẻ từ.	

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
33	Có thể bị đột nhập, trộm cắp và phá hoại tài sản	**Bổ sung vào chính sách An ninh môi trường và vật lý, phần Vành đai an ninh vật lý:** - Vành đai an ninh được thiết lập rõ ràng: Các thiết bị lưu trữ (USB, ổ cứng, CD-ROM) được lưu trữ trong tủ kính, chống cháy, có khóa và được đặt trong phòng riêng, do người phụ trách của phòng sản xuất game quản lý. Phòng ra vào có cơ chế kiểm soát bằng thẻ từ.	
34	Dễ bị sử dụng không đúng mục đích của những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến các thiết bị lưu trữ (USB, ổ cứng, CD-ROM).	**Bổ sung vào chính sách An ninh môi trường và vật lý, phần Kiểm soát chung:** - Các thiết bị lưu trữ (USB, ổ cứng, CD-ROM) khi sử dụng phải được log lại bằng văn bản, sử dụng xong phải trả lại, có ký nhận và phải được sự cho phép của lãnh đạo.	
35	Có thể bị đột nhập, trộm cắp và phá hoại tài sản	**Bổ sung vào chính sách An ninh môi trường và vật lý, phần Vành đai an ninh vật lý:** - Vành đai an ninh được thiết lập rõ ràng: Các máy điện thoại để test game được lưu trữ trong tủ kính, chống cháy, có khóa và được đặt trong phòng riêng, do người phụ trách của phòng sản xuất game quản lý. Phòng ra vào có cơ chế kiểm soát bằng thẻ từ.	
36	Dễ bị sử dụng không đúng mục đích của những nhân viên không có chức năng, nhiệm vụ và trách nhiệm liên quan đến các máy điện thoại để test game.	**Bổ sung vào chính sách An ninh môi trường và vật lý, phần Kiểm soát chung:** - Các máy điện thoại để test game khi sử dụng phải được log lại bằng văn bản, sử dụng xong phải trả lại, có ký nhận và phải được sự cho phép của lãnh đạo.	
37	Có thể bị nhân viên sử dụng điện thoại để chụp, quay hình, nghe lén những thông tin quan trọng, quyết định lớn đến chiến lược kinh doanh của công ty, gây rò rỉ, tán phát ra	**Bổ sung vào chính sách An ninh môi trường và vật lý, phần Kiểm soát chung:** - Nghiêm cấm việc sử dụng các chức năng liên quan đến ghi âm, ghi hình trong công ty.	

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
	ngoài vì mục đích xấu.		
38	Có thể những phần mềm do công ty mua bản quyền nhưng được sao chép, sử dụng bừa bãi không đúng mục đích.	**Bổ sung chính sách Sử dụng mạng máy tính nội bộ trong công ty** Trên máy server của mạng nội bộ công ty có các dạng thư mục dùng chung: - Thư mục Software + Thư mục này lưu trữ các phần mềm, chương trình dùng để cài đặt, bảo dưỡng máy vi tính và các thiết bị khác... + Dữ liệu lưu trữ đa dạng: .exe, .msi... + Thời gian lưu trữ không hạn chế. + Phân quyền truy cập được quy định cụ thể trong bảng phân quyền. (Sheet bảng phân quyền) + Đối các phần mềm do công ty mua bản quyền, active online key, định kỳ check với bên bán phần mềm để check việc ai active, máy tính có IMEI nào active, địa chỉ IP là bao nhiêu...	
39	Có thể những phần mềm do công ty phát triển nhưng chưa công bố ra thị trường đã bị tán phát, gây ảnh hưởng đến bí mật kinh doanh của công ty.	**Bổ sung vào chính sách An ninh môi trường và vật lý, phần An ninh cho các thiết bị ngoại vi** - Nghiêm cấm việc sử dụng USB, thẻ nhớ trong nội bộ công ty, có thể niêm phong các ổ USB, thẻ nhớ. - Nghiêm cấm việc cài đặt các phần mềm cho phép gửi file peer-to-peer, ngăn chặn các trang web cho phép upload, gửi file.	
40	Nhận thức về đảm bảo an toàn thông tin trong công ty yếu, khó quản lý nhân viên trong việc đảm bảo an toàn thông tin.	**Xây dựng chính sách An ninh cá nhân, phần Đào tạo người sử dụng** 1. Giáo dục và đào tạo an ninh thông tin Toàn bộ các nhân viên của tổ chức được đào tạo thích hợp và các cập nhật thường xuyên về chính sách và thủ tục của tổ chức. Điều này bao gồm các yêu cầu an ninh, trách nhiệm pháp lý và các kiểm soát kinh doanh, cũng như đào tạo việc sử dụng đúng các phương tiện xử lý thông tin trước khi truy cập tới thông tin hoặc các dịch vụ được cho phép ví dụ thủ tục đăng nhập, sử dụng các gói phần mềm.	
41	Nhận thức về đảm bảo an toàn thông tin trong công ty yếu, khó quản lý nhân viên trong việc đảm bảo an toàn thông	**Bổ sung chính sách An ninh cá nhân** 1. An ninh theo định nghĩa và nguồn công việc 1.1 An ninh theo các trách nhiệm công việc Các vai trò và trách nhiệm an ninh, khi được đặt trong chính sách an ninh thông tin của tổ chức nên được tài liệu hóa một cách thích hợp. Chúng nên	

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
	tin.	gồm mọi trách nhiệm chung đối với việc thực hiện hoặc duy trì chính sách an ninh cũng như mọi trách nhiệm đặc biệt đối với việc bảo vệ các tài sản cụ thể hoặc đối với việc thi hành các quy trình hoặc các hoạt động an ninh cụ thể. 1.2 Chính sách và kiểm tra nhân sự Các kiểm soát bao gồm: a) tính sẵn có của các giấy tờ dẫn chứng về các đặc điểm, ví dụ về công việc và cá nhân; b) kiểm tra (đầy đủ và chính xác) hồ sơ của ứng viên; c) xác nhận bằng cấp được yêu cầu và phẩm chất nghề nghiệp; d) kiểm tra nhận dạng (hộ chiếu hoặc giấy tờ tương tự). 1.3 Thỏa thuận về tính bảo mật Các thỏa thuận về tính bảo mật hoặc không làm lộ được sử dụng để đưa ra lưu ý rằng thông tin là bảo mật hoặc bí mật. Các nhân viên nên ký kết một thỏa thuận như một phần của các điều khoản và điều kiện tuyển dụng ban đầu của họ. Nên yêu cầu những người sử dụng không chủ định, nhân viên và bên thứ ba, chưa có hợp đồng bao gồm thỏa thuận về tính bảo mật, ký kết một thỏa thuận về tính bảo mật trước khi được phép truy cập tới các phương tiện xử lý thông tin. Các thỏa thuận về tính bảo mật nên được soát xét khi có các thay đổi về thời hạn công việc hoặc hợp đồng, cụ thể là khi những người lao động rời tổ chức hoặc các hợp đồng đã hết hạn. 2. Đào tạo người sử dụng 2.1 Giáo dục và đào tạo an ninh thông tin Toàn bộ các nhân viên của tổ chức được đào tạo thích hợp và các cập nhật thường xuyên về chính sách và thủ tục của tổ chức. Điều này bao gồm các yêu cầu an ninh, trách nhiệm pháp lý và các kiểm soát kinh doanh, cũng như đào tạo việc sử dụng đúng các phương tiện xử lý thông tin trước khi truy cập tới thông tin hoặc các dịch vụ được cho phép ví dụ thủ tục đăng nhập, sử dụng các gói phần mềm.	
42	Nhân viên làm việc dễ truy cập	Các biện pháp kiểm soát về An ninh cá nhân xây dựng ở trên đã giải quyết	

STT	Nguy cơ	Chính sách, quy trình	Con người, kỹ thuật
	trái phép hoặc làm rò rỉ thông tin một cách thiếu ý thức	được nguy cơ này.	
43	Nhân viên làm việc dễ truy cập trái phép hoặc làm rò rỉ thông tin một cách thiếu ý thức	Các biện pháp kiểm soát về An ninh cá nhân xây dựng ở trên đã giải quyết được nguy cơ này.	
44	Sang làm việc cho đối thủ canh tranh	**Bổ sung chính sách An ninh cá nhân, phần Chính sách và kiểm tra nhân sự** - Đảm bảo quyền lợi, đưa ra những mục tiêu thăng tiến, phát triển rõ ràng của nhân viên, lương thưởng ở mỗi cấp.	

Từ Bảng các biện pháp kiểm soát đối ứng với các nguy cơ ở trên, tiến hành phân tích, phân tách và rút gọn, lược đồ hóa, thu được bộ chính sách, quy trình và quy định như sau:

1. 01 chính sách về các lĩnh vực:

- Kiểm soát truy cập

- Quản lý truyền thông và hoạt động

- An ninh môi trường và vật lý

- An ninh cá nhân

- Đào tạo nhân viên

2. 04 quy trình:

- Quy trình đo lường của hệ thống quản lý an toàn thông tin

- Quy trình về quản lý source code, các bản mềm tài liệu

- Quy trình về giáo dục nhận thức, đào tạo về an toàn thông tin

- Quy trình hành động phòng ngừa đối với hệ thống quản lý an toàn thông tin

3. 02 quy định:

- 01 quy định chung đối với nhân viên

- 01 quy định những việc phải làm và những việc không được làm đối với nhân viên mới.

3.2. Quy trình đo lường của hệ thống quản lý an toàn thông tin

3.2.1. Mục tiêu

- Cung cấp thông tin, dữ liệu để hệ thống quản lý an toàn thông tin phù hợp hơn với chiến lược kinh doanh và là cơ sở để báo cáo cho các bên có liên quan bên trong và bên ngoài tổ chức.

- Hiệu quả của quy trình và kiểm soát CNTT được ghi nhận và các tiêu chí được đáp ứng.

- Các xu hướng không còn phù hợp được phát hiện kịp thời và được xử lý.

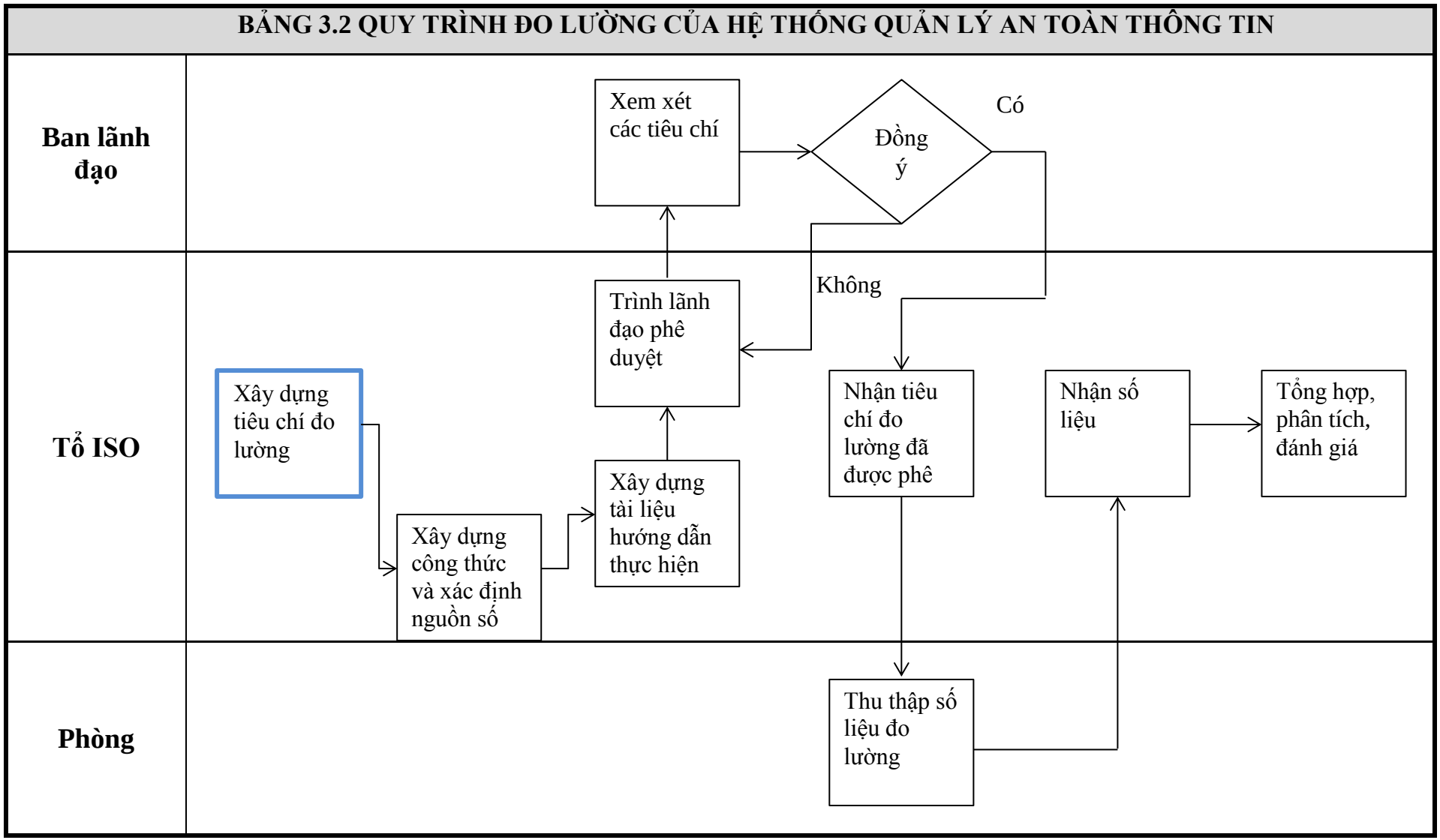
- Giúp giải trình các chi phí liên quan đến ISMS và thực hiện các biện pháp kiểm soát CNTT.

- Thực hiện giám sát việc triển khai ISMS trong tổ chức.

- Cung cấp thông tin, dữ liệu để tiến hành cải tiến, thiết kế lại các quy trình ISMS và thiết kế lại các biện pháp kiểm soát.

3.2.2. Quy trình

BẢNG 3.2 QUY TRÌNH ĐO LƯỜNG CỦA HỆ THỐNG QUẢN LÝ AN TOÀN THÔNG TIN



3.2.3. Các tiêu chí, phương thức đo lường

BẢNG 3.3 CÁC TIÊU CHÍ, PHƯƠNG THỨC ĐO LƯỜNG

STT	Đo lường	Phương pháp / nguồn	Mục tiêu
1	% các quyết định liên quan đến chiến lược kinh doanh được hỗ trợ bởi CNTT và các vấn đề an toàn thông tin.	Soát xét các quyết định chiến lược kinh doanh và đảm bảo rằng những quyết định đó đã được đánh giá rủi ro liên quan đến CNTT và các vấn đề an toàn thông tin. Tương tự như vậy, tất cả các quyết định chiến lược an toàn thông tin quan trọng cần được xem xét và phê duyệt bởi quản lý cấp cao để đảm bảo sự liên kết chúng với các chiến lược kinh doanh.	Tất cả các quyết định kinh doanh cần được hỗ trợ bởi các chiến lược CNTT và đặc biệt là vấn đề bảo mật thông tin. Nếu không có liên quan giữa 2 mặt này, cần phải có sự phê duyệt bằng văn bản.
2	% thay đổi đối với chiến lược an toàn thông tin đã được quản lý phê duyệt.	Soát xét các chiến lược bảo mật thông tin hiện tại và đảm bảo rằng ban lãnh đạo đã chính thức phê duyệt.	Tất cả các quyết định chiến lược về an toàn thông tin cần được quản lý phê duyệt.
3	% quy trình kinh doanh của công ty được bao gồm trong quy trình quản lý rủi ro.	Phỏng vấn, kiểm tra, đo đạc thực tế	Dựa vào mức độ phát triển và thời gian công ty đã tồn tại và phát triển, mục tiêu 50% các quy trình kinh doanh đã được bao gồm trong quy trình quản lý rủi ro.
4	Số biện pháp kiểm soát rủi ro đã được phê duyệt và đã được thực hiện so với các rủi ro đã được đánh giá.	Tương quan với các báo cáo đánh giá rủi ro trước đó.	Cần đảm bảo rằng tất cả các biện pháp kiểm soát rủi ro đã được phê duyệt phải được thực hiện chứ không phải để quên ở đó và chờ cho những lần sau giải quyết.
5	% ngân sách CNTT được sử dụng cho quy trình quản lý rủi ro.	Tương quan tổng số giờ làm việc dành cho quá trình đánh giá rủi ro với tổng ngân sách cho CNTT.	Mục tiêu để theo dõi chi tiêu cho quy trình quản lý rủi ro CNTT.
6	Số lượng các rủi ro mới được xác định so với những đánh giá rủi ro trước đó.	So sánh tổng số rủi ro đã được xác định so với số rủi ro đã được đánh giá trước	Cần giảm rủi ro để đảm bảo rằng các rủi ro đã được đánh giá trước đó không tái

STT	Đo lường	Phương pháp / nguồn	Mục tiêu
		đó.	diễn.
7	Số lượng các sự cố phát sinh do không tuân thủ và chi phí phát sinh hàng năm cho việc khắc phục các sự cố này.	Rà soát các sự cố đã báo cáo vào cuối năm kèm theo các chi phí để giải quyết các sự cố này.	Không có những sự cố nào lớn xảy ra ảnh hưởng đến các chi phí về tài chính và hình ảnh công ty.
8	Khoảng thời gian giữa việc xác định sự không tuân thủ và việc thực hiện các hành động khắc phục.	Tương quan thời gian giữa việc báo cáo các vấn đề không tuân thủ với thời gian thực hiện.	Tùy thuộc vào sự phức tạp, vấn đề cần được giải quyết trong vòng 2 ngày làm việc.
9	Tổng chi phí do mất uy tín, tiền phạt, mất khách hàng… do việc không tuân thủ.	Soát xét tổng chi phí phát sinh do vấn đề không tuân thủ.	Ghi lại tổng chi phí phát sinh và so sánh với năm ngoái. Mục tiêu là giảm chứ không tăng.
10	% chênh lệch khi so sánh giữa chiến dịch nâng cao nhận thức cho nhân viên với kết quả thực tế của các chiến dịch đã thực hiện.	So sánh các kết quả từ chương trình nhận thức / đào tạo với kết quả kiểm tra thực tế của nhân viên.	Mục tiêu là đảm bảo tối thiểu 80% hoàn thành các bài kiểm tra của chiến dịch. Kiểm tra thực tế các khu vực làm việc cho thấy phải có sự giảm đáng kể các việc như: màn hình được lock trước khi rời khỏi chỗ ngồi, thiết bị USB không được sử dụng…
11	Các kế hoạch, chiến lược nhận thức, các buổi học, các khóa học... có phù hợp với những rủi ro an toàn thông tin mà tổ chức đang gặp phải hay quan tâm hay không?	Các chương trình nâng cao nhận thức, đào tạo phải phù hợp với nguy cơ rủi ro thực tế đang hiện hữu trong công ty, những cảnh báo bên ngoài…	Cần phải có liên kết rõ ràng về nội dung chương trình đào tạo, nâng cao nhận thức với tình hình rủi ro thực tế đang tồn tại.
12	% nhân viên trong công ty đã truy cập trang intranet đăng nội dung nhận thức liên quan đến an toàn thông tin.	Ghi lại tổng truy cập, account truy cập hàng tháng của trang intranet liên quan đến bảo mật thông tin.	Tổng số account truy cập không được dưới 70% trên tổng số nhân viên trong công ty.
13	% nhân viên ghi nhớ nội dung mà công ty đã đào tạo, truyền tải liên quan đến an toàn thông tin.	So sánh kết quả của bài kiểm tra được thực hiện trong thời gian ngắn đối với nhân viên với bài kiểm tra đã được thực hiện cách đó 2 đến 6 tháng.	Đạt được 60% nhân viên nhớ được chủ đề, nội dung của bài kiểm tra trước đó.

STT	Đo lường	Phương pháp / nguồn	Mục tiêu
14	Số lượng các thống nhất về các hành động sẽ thực hiện so với kế hoạch hành động được đưa ra.	So sánh số lượng các hành động đã được thống nhất với các hành động được lên kế hoạch.	Tỷ lệ đạt 100%.
15	Tổng số nguồn lực bao gồm thời gian, tiền và nhân lực để thực hiện các hành động đã được thống nhất.	So sánh tổng số nguồn lực để giải quyết các hành động đã được thống nhất và so sánh với tổng số nguồn lực đã chi tiêu vào năm trước.	Trừ khi có những thay đổi lớn liên quan đến cơ sở hạ tầng, chi phí ngân sách nguồn lực chỉ nên chiếm tối đa 10% ngân sách CNTT.

3.3. Quy trình về quản lý source code, các bản mềm tài liệu

3.3.1. Mục tiêu:

Đối với công ty sản xuất game như Công ty X, source code và các tài liệu bản mềm khác như chiến lược phát triển kinh doanh, thông tin đối thủ cạnh tranh, thông tin về lương, thưởng của nhân viên, kế hoạch phát triển dự án, tài liệu quản lý tiến độ, issues, hướng dẫn sử dụng phần mềm, các phần mềm hỗ trợ… là những tài sản có ý nghĩa vô cùng quan trọng trong sự tồn tại và phát triển của công ty. Quy trình này được xây dựng có những mục tiêu sau:

- Đảm bảo source code và các tài liệu liên quan khác không bị mất, phá hủy vì bất kỳ lý do nào.

- Đảm bảo source code và các tài liệu liên quan luôn ở trạng thái sẵn sàng khi sử dụng. Đâu là bản mới nhất, đâu là bản version của bản alpha test, version bản 1.0, version bản 2.0 của một game cụ thể… đều có thể lấy ra một cách nhanh nhất có thể.

- Đảm bảo phân rõ vai trò và quyền cụ thể của các thành viên đối với source code và tài liệu liên quan trong quá trình phát triển dự án.

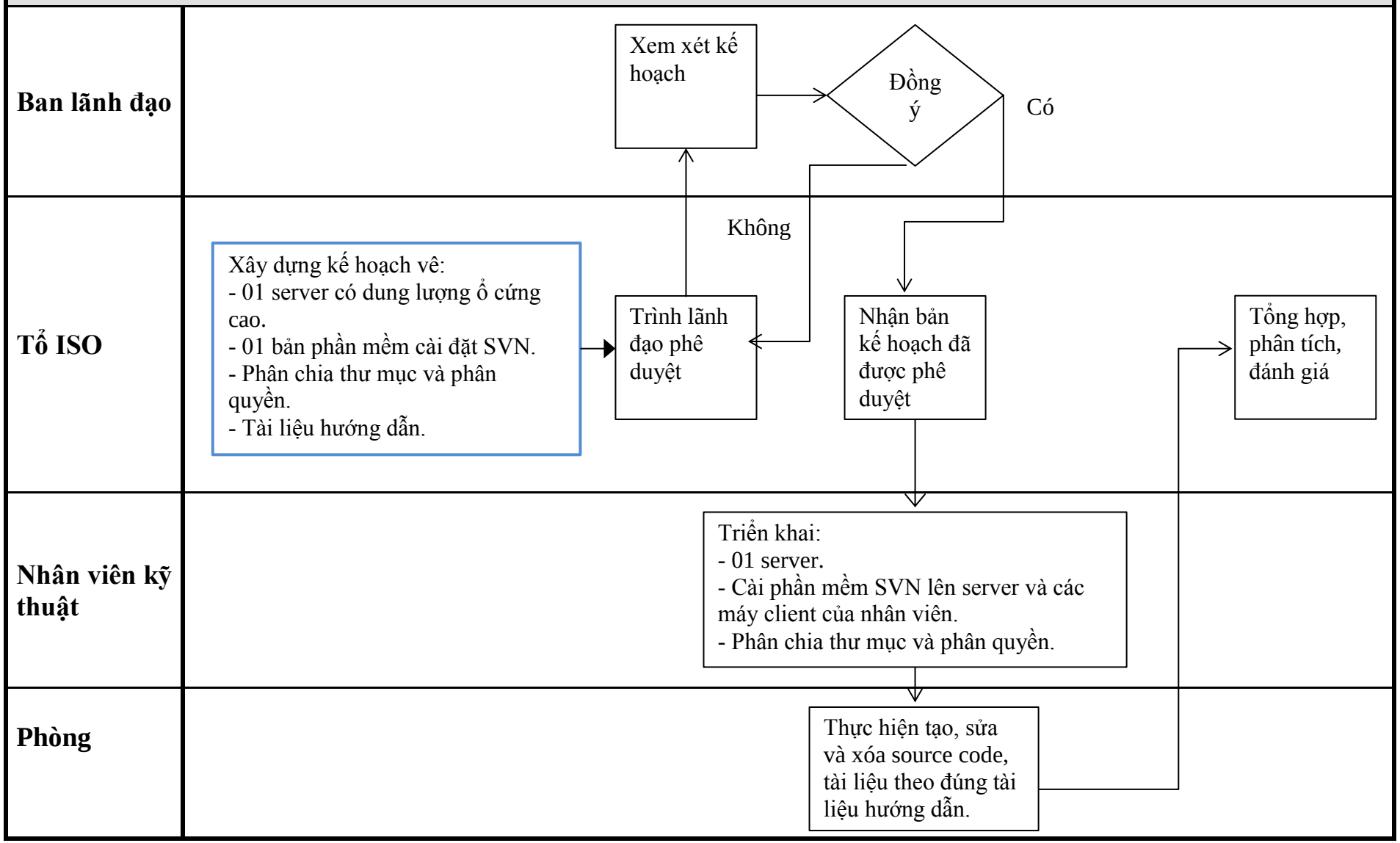
- Đảm bảo tính thông suốt trong quá trình sử dụng, chia sẻ thông tin giữa các phòng, ban.

3.3.2. Kỹ thuật:

- Sử dụng Subversion source control (SVN) để quản lý source code và các tài liệu bản mềm khác.

- Yêu cầu 1 server có dung lượng ổ cứng lớn để lưu trữ những source code và các tài liệu bản mềm này.

BẢNG 3.4 QUY TRÌNH QUẢN LÝ SOURCE CODE, CÁC BẢN MỀM TÀI LIỆU



STT	Tên thư mục	Mục đích	Thông tin lưu trữ	Thời gian lưu trữ	Phân quyền		
					Ban lãnh đạo	Các phòng ban nghiệp vụ	Nhân viên quản lý kỹ thuật
1	Thư mục tên các phòng: Phòng Sản xuất Game, Phòng Kinh doanh, Phòng Hành chính tổng hợp và nhân sự	Dữ liệu trong thư mục do lãnh đạo, nhân viên các Phòng lưu trữ dùng để báo cáo lãnh đạo công ty, xử lý công tác nghiệp vụ.	Loại dữ liệu lưu trữ là văn bản mềm, hình ảnh, video… phục vụ cho công việc.	Lâu dài	Truy cập tất cả.	- Toàn quyền trong thư mục của đơn vị mình. - Không được truy cập vào thư mục Ban khác.	- Có quyền truy cập tất cả các thư mục để quản lý. - Không được xóa, sửa
2	Public	Thư mục dùng để chia sẻ, trao đổi dữ liệu giữa các phòng ban, cá nhân trong công ty.	Loại dữ liệu lưu trữ là văn bản mềm, hình ảnh, video… phục vụ cho công việc.	Dữ liệu tại thư mục này chỉ được lưu trữ tạm thời và sẽ bị xóa sau một khoảng thời gian nhất định tùy thuộc vào dung lượng nhớ.	Truy cập tất cả.	- Được xem, sao chép, thêm. - Được xóa, sửa các file do mình đưa lên.	Có toàn quyền truy cập để quản lý.
3	Nghiệp vụ		Thư mục này lưu trữ các phần mềm ứng dụng, dữ liệu của các nghiệp vụ (như kế toán, lương, văn thư…)	Lâu dài	Truy cập tất cả.	- Theo phân quyền cụ thể của các ứng dụng.	- Có quyền truy cập tất cả để quản lý - Không được xóa, sửa.
4	Project	Lưu trữ source code, tài liệu liên quan trong quá trình phát triển, sản xuất các dự án game	Source code và các tài liệu liên quan	Lâu dài	Truy cập tất cả.	- Chỉ phòng Phát triển mới được phép truy nhập.	- Có quyền truy cập tất cả để quản lý - Không được xóa, sửa.

5	Software	Thư mục này lưu trữ các phần mềm, chương trình dùng để cài đặt, bảo dưỡng máy vi tính và các thiết bị khác…	Các bản cài đặt phần mêm, các file có đuôi dạng như: *.exe, *.msi…	Lâu dài	Truy cập tất cả.	- Được xem, sao chép, thực thi. - Không được thêm, xóa, sửa.	Có toàn quyền truy cập để quản lý.

3.3.4. Các bước thực hiện tạo, sửa và xóa source code, tài liệu liên quan

+ Sử dụng tool quản lý source code SVN, tài liệu do các thành viên trong cùng dự án tạo ra.

+ Nhân viên kỹ thuật sẽ setup server SVN và tạo tài khoản cho từng thành viên trong dự án.

+ Đầu ngày, developer sẽ get source code mới nhất về, merge source code của những developer khác với source code dưới máy local của mình.

+ Khi developer đang update file nào thì get lock file, để thông báo và ngăn không cho developer khác cũng update vào file này.

+ Cuối ngày, trước khi đi về, developer commit source code sau khi mình đã tạo mới, update lên server, đồng thời unlock file.

+ Mỗi thời điểm như release version mới, các milestone quan trọng… project leader của dự án sẽ tiến hành baseline source code, đánh tag để source code có thể lấy lại tại từng thời điểm theo sự kiện thời gian về sau.

+ Sau khi mỗi dự án kết thúc, thì tiến hành nén thư mục dự án, tiến hành sao lưu, bảo quản.

3.4. Quy trình về giáo dục nhận thức, đào tạo về an toàn thông tin

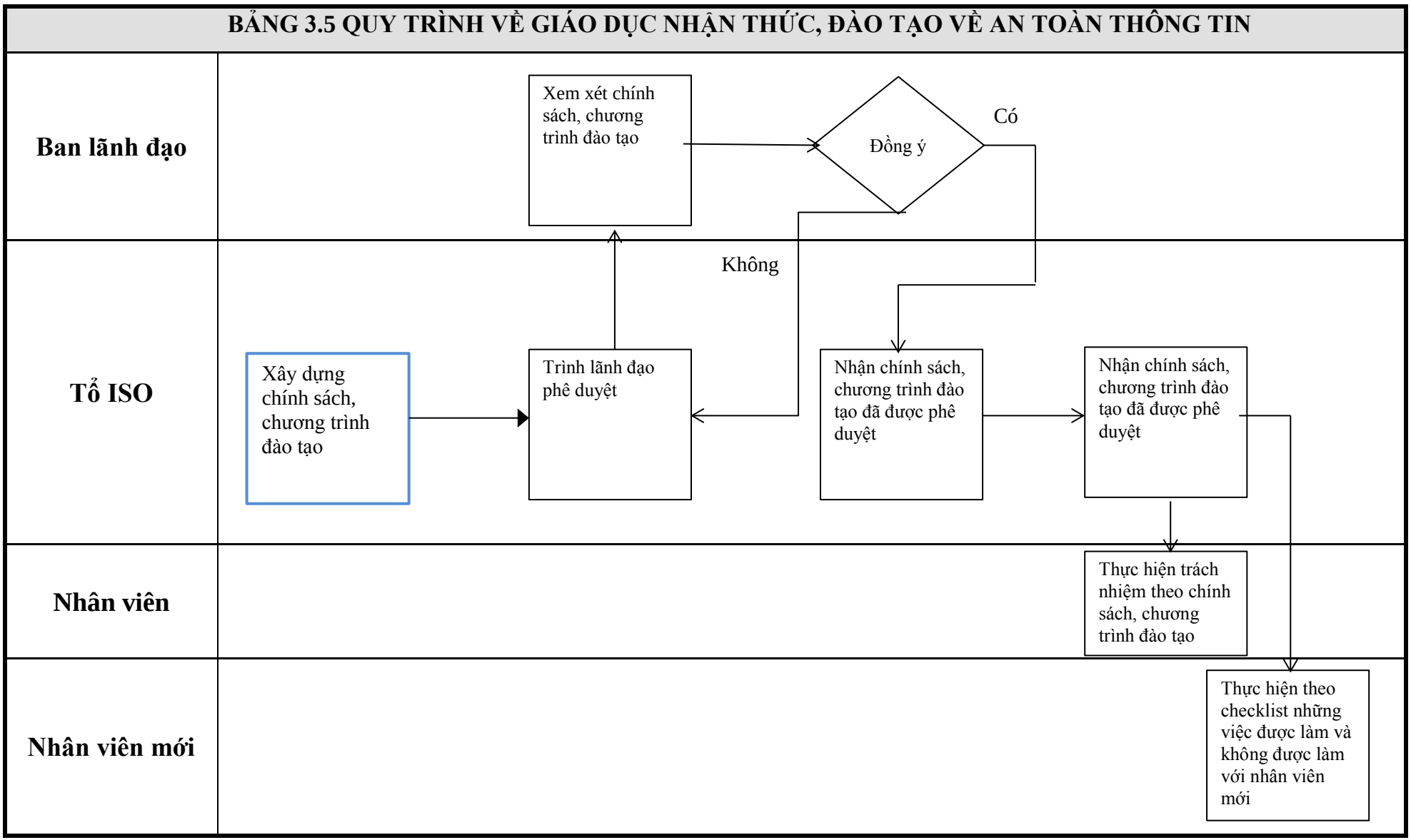
3.4.1. Mục tiêu

- Giúp nhân viên có nhận thức cần thiết để đảm bào an toàn thông tin cho cá nhân và cho tổ chức.

- Giúp nhân viên hiểu rõ tầm quan trọng của an toàn thông tin.

- Giúp nhân viên hiểu được tác hại cũng như những hậu quả đối với việc mất an toàn thông tin có thể gây ra.

BẢNG 3.5 QUY TRÌNH VỀ GIÁO DỤC NHẬN THỨC, ĐÀO TẠO VỀ AN TOÀN THÔNG TIN



Một số chú ý:

- Định kỳ hàng tháng, quý, tổ ISO phải tiến hành báo cáo kết quả giáo dục nhận thức, đào tạo về an toàn thông tin đối với nhân viên trong tổ chức cho ban lãnh đạo.

- Việc xây dựng chương trình đào tạo về cơ bản phải đáp ứng được các tiêu chí:

+ Đối với những vấn đề mới về an toàn thông tin mà doanh nghiệp không có kinh nghiệm thì tiến hành thuê, mời những doanh nghiệp, tổ chức có uy tín về vấn đề về tổ chức khóa học, trực tiếp giảng dậy cho cán bộ nhân viên.

+ Trước khi kết thúc khóa học đều có những bài kiểm tra, phỏng vấn, thu hoạch để kiểm tra kiến thức.

+ Sau mỗi khóa học đều có chữ ký của các nhân viên tham gia khóa học để tăng vai trò, trách nhiệm thực hiện của nhân viên đối với những kiến thức mình được đào tạo.

3.4.3. Chính sách về đào tạo an toàn thông tin

a) Toàn bộ các nhân viên của tổ chức được đào tạo thích hợp và các cập nhật thường xuyên về chính sách và thủ tục của tổ chức. Điều này bao gồm các yêu cầu an toàn, trách nhiệm pháp lý và các kiểm soát kinh doanh, cũng như đào tạo việc sử dụng đúng các phương tiện xử lý thông tin trước khi truy cập tới thông tin hoặc các dịch vụ được cho phép ví dụ thủ tục đăng nhập, sử dụng các gói phần mềm.

b) Toàn bộ các nhân viên của công ty được đào tạo thích hợp và các cập nhật thường xuyên về chính sách và thủ tục của tổ chức, được đào tạo việc sử dụng đúng các phương tiện xử lý thông tin trước khi truy cập tới thông tin cơ sở dữ liệu.

c) Technical leader được đào tạo thích hợp và cập nhật thường xuyên về chính sách và thủ tục của tổ chức, được đào tạo việc sử dụng các tool backup để thực hiện việc sao lưu cơ sở dữ liệu.

d) Toàn bộ các nhân viên, cá nhân liên quan của công ty được đào tạo thích hợp và các cập nhật thường xuyên về chính sách và thủ tục của tổ chức, được đào tạo việc sử dụng các chính sách, quy trình về việc sử dụng mật khẩu truy cập tới cơ sở dữ liệu.

e) Toàn bộ các nhân viên, cá nhân liên quan của công ty được đào tạo, giải thích về các khu vực an ninh và được chỉ dẫn về các yêu cầu an ninh của khu vực đó.

f) Toàn bộ các nhân viên, cá nhân liên quan của công ty được đào tạo, giải thích về quy chế, chính sách sử dụng mạng máy tính nội bộ trong công ty và hướng dẫn thi hành.

Nội dụng cần truyền đạt tới nhân viên:

- Giữ cho máy tính PC “sạch”: đưa ra các nội quy, quy tắc về những phần mềm gì nhân viên được cài đặt lên máy PC của mình. Và đảm bảo rằng họ hiểu những nội quy, quy tắc đó.

- Tuân thủ những quy định liên quan đến mật khẩu: tạo mật khẩu dài và mạnh, có sự kết hợp giữa ký tự viết hoa và ký tự viết thường, số và các ký tự đặc biệt, bên cạnh việc thay đổi thường xuyên mật khẩu, giữ bí mật các mật khẩu này.

- Nhân viên được giáo dục là không được mở những link, tweet, post, message,

file attach hay quảng cáo online lạ, ngay cả khi họ hiểu được nguồn của những link này.

- Sao lưu công việc: nhân viên cũng được đào tạo về phương pháp sao lưu kết quả công việc của mình, sao lưu những gì, sao lưu ra đâu và thời gian sau lưu.

3.4.4. Các quy định đối với nhân viên phải thực thi

Phân loại, xử lý và sử dụng thông tin

Tất cả thông tin phải được gián nhãn dựa trên tính nhậy cảm của thông tin và ai là đối tượng sử dụng thông tin. Thông tin cần phải được đánh nhãn "Mật", "Tuyệt mật", "Tối mật", "Chỉ lưu hành nội bộ" hay "Công khai". Các tài liệu được đánh nhãn "Mật", "Tuyệt mật" hay "Tối mật" phải được cất vào trong tủ và khóa sau khi kết thúc công việc trong ngày. Thông tin điện tử ("Mật", "Tuyệt mật" hay "Tối mật") phải được mã hóa và có mật khẩu bảo vệ. Khi thông tin không còn cần thiết nữa, các tài liệu cần được hủy bỏ bằng máy hủy bỏ và các tài liệu điện tử cần được chia nhỏ và hủy.

Truy cập hệ thống

Nhân viện không được phép chia sẻ UserID và mật khẩu được cấp cho mình, và nhân viên phải có trách nhiệm giữ an toàn về thông tin account và mật khẩu này. Nhân viên cần được chỉ cách đặt mật khẩu và làm thế nào để đặt được mật khẩu mạnh.

Virus

Tất cả máy tính phải được cài đặt phần mềm chống virus và nhân viên sử dụng máy tính của mình phải có trách nhiệm quét máy tính của mình một cách thường xuyên. Tất cả phần mềm và file trước khi copy vào máy tính phải được tiến hành quét, và nhân viên phải tiến hành quét những dữ liệu và phần mềm mới trước khi họ mở và chạy chương trình. Nhân viên phải được giáo dục về tầm quan trọng của việc quét virus, về cách virus phá hủy ổ cứng và làm cho mạng của công ty bị hỏng như thế nào.

Sao lưu

Nhân viên được giáo dục họ phải có trách nhiệm đối với việc sao lưu thông tin trong máy tính cá nhân của họ và việc sao lưu được tiến hành ít nhất 1 tuần 1

lần.

Bản quyền phần mềm

Nhân viên được giáo dục về việc không được cài đặt các phần mềm mà không có bản quyền hay vi phạm pháp luật.

Sử dụng Internet

Nhân viên được giáo dục khi sử dụng Internet: không được truy cập vào những trang không thích hợp, những trang khiêu dâm và trang game, không được tải phần mềm và công cụ hack.

Sử dụng email

Nhân viên được phép sử dụng email để liên lạc cá nhân nhưng không được phép sử dụng hệ thống email cho những lý do sau:

- Gửi, trao đổi những thông tin, tài liệu liên quan đến tôn giáo, chính trị.

- Sử dụng email công ty vào những công việc kinh doanh cá nhân.

Bảo vệ máy tính xách tay

Tất cả các máy tính xách tay phải được bảo vệ sau giờ làm việc trong tủ.

Bảo vệ mạng nội bộ

Tất cả máy tính cá nhân phải để chế độ màn hình có mật khẩu bảo vệ.

Trao đổi thông tin với các bên thứ ba

Thông tin bí mật không nên được tiết lộ cho bên thứ ba trừ khi có một thỏa thuận tiết lộ được ký kết cung cấp thông tin với bên thứ ba và được sự đồng ý của lãnh đạo công ty. Trách nhiệm của tất cả nhân viên là bảo vệ thông tin của công ty.

3.4.5 Các quy định đối với nhân viên mới

Đây là một checklist mà bất cứ một nhân viên khi gia nhập công ty đều được thông báo và hướng dẫn tuân thủ.

Không được làm

- Không chia sẻ mật khẩu với bất kỳ ai, kể cả nhân viên trong công ty.

- Không viết mật khẩu ra giấy, bảng.

- Không sử dụng mật khẩu dễ nhớ như các sự kiện, ngày sinh, tên con cái…

- Không truy cập những trang web khiêu dâm, những trang hacker.

- Không download và cài đặt những phần mềm vi phạm pháp luật và không có bản quyền từ Internet.

Phải làm

- Thay đổi mật khẩu thường xuyên.

- Sử dụng kết hợp giữa ký tự, ký tự đặc biệt và số cho việc đặt mật khẩu.

- Sử dụng mật khẩu khó đoán, chiều dài ít nhất 6 ký tự.

- Bật chế độ màn hình chờ có mật khẩu hay lock máy tính.

- Tiến hành quét virus máy tính một cách thường xuyên.

- Tiến hành kiểm tra phần mềm virus đã được cập nhật hay chưa khi bạn nhận được email thông báo update từ màn hình Desktop.

- Tiến hành sao lưu dữ liệu ít nhất 1 tuần 1 lần.

- Tiến hành lock tất cả tài liệu, file và đĩa có đánh nhãn là “Mật”, “Tuyệt mật” hoặc “Tối mật” sau khi kết thúc công việc trong ngày.

3.5. Quy trình hành động phòng ngừa đối với hệ thống quản lý an toàn thông tin

3.5.1. Mục tiêu

- Sự không phù hợp là sự không đáp ứng bất cứ yêu cầu nào theo quy định đã đề ra.

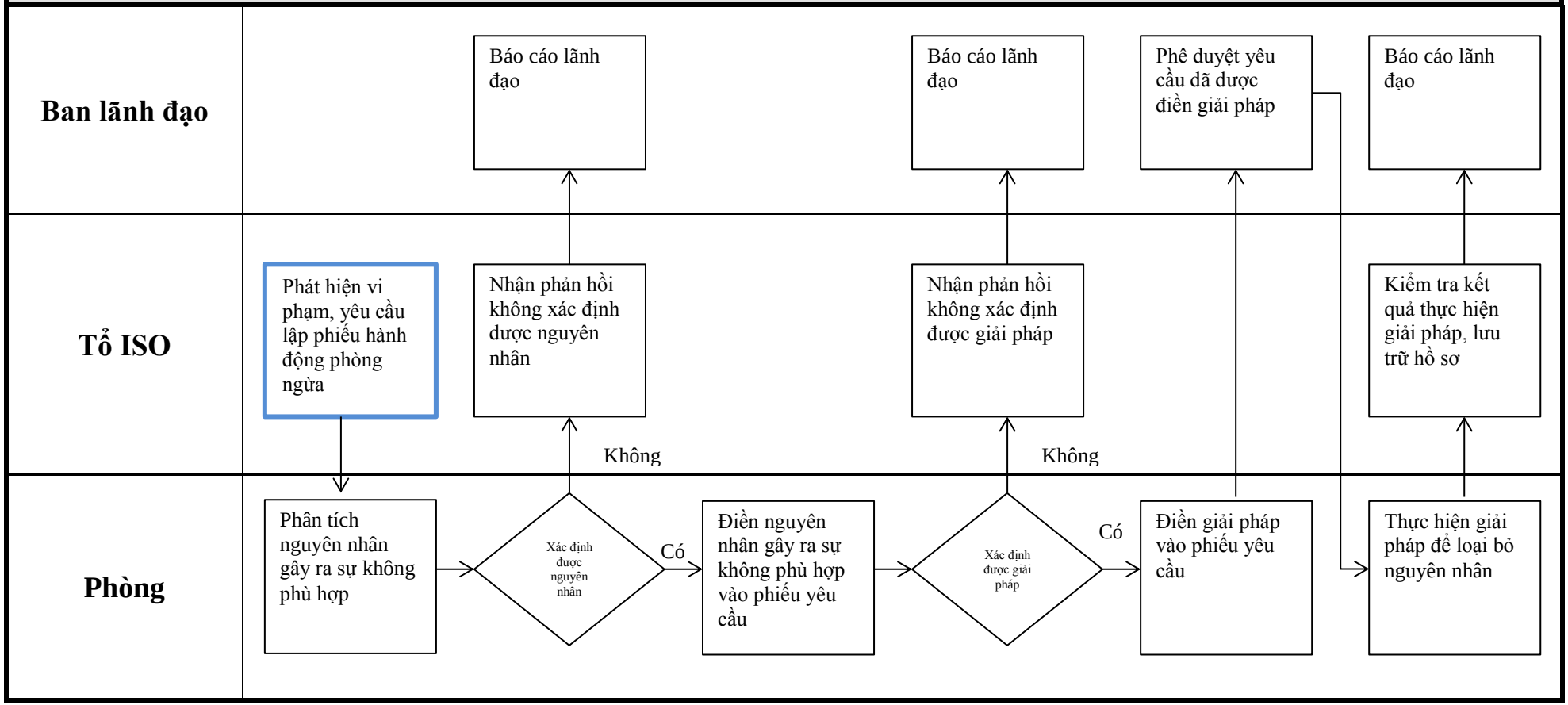
- Mục đích nhằm đưa ra những hành động để loại bỏ nguyên nhân của sự không phù hợp đã được phát hiện hay tình trạng không mong muốn tiềm tàng khác.

- Giúp cải tiến, sửa đổi quy trình của hệ thống quản lý an toàn thông tin sao cho phù hợp với thực tiễn, nâng cao hiệu quả của hệ thống quản lý an toàn thông tin.

- Đảm bảo không lặp lại các sai phạm xảy ra đối với vi phạm về an toàn thông tin trong tổ chức.

3.5.2. Quy trình

BẢNG 3.6 QUY TRÌNH HÀNH ĐỘNG PHÒNG NGỪA ĐỐI VỚI HỆ THỐNG QUẢN LÝ AN TOÀN THÔNG TIN



Chú ý: Định kỳ hàng tháng, quý, tổ ISO lập báo cáo theo dõi hành động phòng ngừa và gửi về ban lãnh đạo để báo cáo, đưa ra quyết định.

3.6. Chính sách

I. Kiểm soát truy cập

1. Đăng ký người sử dụng

a) Sử dụng một tên truy cập cá nhân duy nhất để người sử dụng có thể kết nối và chịu trách nhiệm với các hoạt động của mình;

b) Kiểm tra mức cho phép truy cập có phù hợp với mục đích doanh nghiệp và có nhất quán với chính sách an ninh của tổ chức;

c) Đưa cho người sử dụng một bản công bố quyền truy cập của họ;

d) Yêu cầu người sử dụng ký các bản kê để chỉ ra rằng họ hiểu các điều kiện truy cập;

e) Duy trì một bản lưu chính thức toàn bộ những người đăng ký sử dụng dịch vụ;

f) Bỏ quyền truy cập của người sử dụng ngay khi người sử dụng thay đổi công việc hoặc rời tổ chức;

g) Kiểm tra định kỳ để xóa bỏ các tên truy cập và tài khoản cá nhân không cần thiết;

h) Đảm bảo rằng các tên truy cập cá nhân dư thừa không được phát hành cho người sử dụng khác.

2. Quản lý đặc quyền

a) Xác định các đặc quyền kết hợp với cơ sở dữ liệu: ai có quyền View, ai có quyền Create, ai có quyền Update, ai có quyền Delete, và các đặc quyền đối với cơ sở dữ liệu được phân phối đối với nhân viên dựa trên vai trò và chức năng của họ;

b) Một quy trình cấp quyền và một bản lưu toàn bộ các đặc quyền được phân phối được bảo lưu. Các đặc quyền không được cho phép cho đến khi quy trình cấp quyền hoàn tất;

3. Quản lý mật khẩu người sử dụng

a) Yêu cầu người sử dụng ký kết một bản cam kết để giữ bí mật các mật khẩu cá nhân (điều này có thể thêm vào trong các điều khoản và điều kiện thuê nhân công);

b) Đảm bảo rằng lúc đầu họ được cung cấp một mật khẩu tạm thời an toàn mà họ buộc phải thay đổi ngay lập tức;

c) Yêu cầu đưa các mật khẩu tạm thời cho người sử dụng một cách an toàn. Người sử dụng nên thông báo đã nhận được các mật khẩu.

4. Soát xét các quyền truy cập của người sử dụng

a) Quyền truy cập của người sử dụng được soát xét sau mỗi khoảng thời gian đều đặn định kỳ 6 tháng và sau bất kỳ sự thay đổi nào;

b) Việc cấp đặc quyền truy cập đặc biệt được soát xét sau khoảng thời gian ngắn hơn, định kỳ 3 tháng;

c) Phân phối đặc quyền được kiểm tra thường sau mỗi khoảng thời gian đều đặn để đảm bảo rằng không có các đặc quyền trái phép.

5. Người sử dụng sử dụng mật khẩu

a) Giữ bí mật các mật khẩu;

b) Tránh giữ lại một tờ giấy ghi mật khẩu, trừ phi nó được lưu giữ an toàn;

c) Thay đổi mật khẩu bất kỳ lúc nào có dấu hiệu hệ thống hoặc mật khẩu có thể bị tổn hại;

d) Chọn các mật khẩu có chất lượng với độ dài ít nhất 6 ký tự và:

1) Dễ nhớ;

2) Không dựa trên bất kỳ cái gì mà một ai khác có thể dễ dàng đoán ra hoặc có được các thông tin liên quan đến cá nhân, ví dụ tên, số điện thoại, ngày sinh v..v.;

3) Tránh các nhóm ký tự giống nhau liên tiếp hoặc các số hoặc các chữ cái.

e) Thay đổi các mật khẩu sau mỗi khoảng thời gian đều đặn hoặc theo những lần truy cập (các mật khẩu của cá tài khoản đặc quyền được thay đổi thường xuyên hơn các mật khẩu thông thường) và tránh sử dụng lại, quay lại các mật khẩu cũ;

f) Thay đổi mật khẩu tạm thời vào lần khởi động đầu tiên;

g) Không tính đến các mật khẩu trong bất kỳ quá trình khởi động tự động hoá nào, ví dụ được lưu trữ trong một phím chức năng hoặc macro;

h) Không chia sẻ các mật khẩu cá nhân.

6. Kiểm soát truy cập mạng

a) Các mạng và dịch vụ mạng được phép mới được truy cập;

b) Các thủ tục cấp phép để xác định rõ người được phép truy cập các mạng và dịch vụ mạng đó;

c) Các kiểm soát và thủ tục quản lý để bảo vệ truy cập tới các kết nối mạng và dịch vụ mạng.

II. Quản lý truyền thông và hoạt động

1. Sao lưu thông tin

a) Technical leader của công ty là người sẽ tiến hành thực hiện sao lưu, kiểm tra việc thực hiện sao lưu.

b) Mức thông tin sao lưu nhỏ nhất, sao lưu toàn bộ dữ liệu cơ sở dữ liệu có được, cùng với lưu trữ các bản sao chép dự phòng và các thủ tục lưu trữ được ghi chép lại chính xác và đầy đủ được lưu ở một nơi tách biệt, với khoảng cách đủ để thoát khỏi các hư hại do một tai hoạ xảy ra ở vị trí chính.

c) Nếu có thể, tool thực hiện backup được kiểm tra đều đặn để đảm bảo rằng chúng có thể chông cậy được trong lúc khẩn cấp khi cần;

d) Việc tiến hành sao lưu cơ sở dữ liệu phải đảm bảo ít nhất 6 tháng kể từ khi người chơi ngừng sử dụng dịch vụ và việc sao lưu được tiến hành hàng ngày vào ban đêm (khi hệ thống dịch vụ game ít người chơi truy cập nhất)

2. Bảo vệ chống lại phần mềm cố ý gây hại

a) Một chính sách chính thức đòi hỏi tuân theo giấy phép phần mềm và ngăn cấm việc sử dụng trái phép phần mềm;

- Xuất bản một chính sách tuân thủ bản quyền phần mềm xác định việc sử dụng pháp lý các sản phẩm phần mềm và thông tin;

- Việc duy trì nhận thức về bản quyền phần mềm và các chính sách giành được và đưa ra thông báo về mục đích thự hiện hoạt động

- Kỷ luật đối với các nhân viên vi phạm;

b) Một chính sách chính thức để bảo vệ chống lại cá rủi ro liên quan đến việc sử dụng các tệp và phần mềm từ cả các mạng bên ngoài hoặc trên bất kỳ phương tiện truyền thông khác, cho biết các biện pháp bảo vệ được sử dụng

- Chỉ mua các chương trình có nguồn đáng tin;

- Mua các chương trình có mã nguồn mà có thể được xác minh;

- Sử dụng các sản phẩm đã được đánh giá;

c) Việc lắp đặt và nâng cấp thông thường phần mềm chống virút và sửa chữa để quét máy vi tính

d) Chỉ đạo việc soát xét thông thường phần mềm và nội dụng dữ liệu của các hệ thống hỗ trợ các quá trình kinh doanh quyết định. Sự hiện diện của bất kỳ tệp không được chấp nhận hoặc các sửa đổi trái phép được điều tra một cách chính thức;

e) Kiểm tra virút bất kỳ tệp nào trên phương tiện truyền thông điện tử có nguồn gốc không rõ ràng hoặc trái phép hoặc các tệp nhận được từ các mạng không đáng tin trước khi sử dụng ;

f) Kiểm tra các phần mềm gây hại trên bất kỳ tệp gửi kèm thư điện tử hoặc các phần tải trên mạng trước khi sử dụng. Việc kiểm tra này được tiến hành ở nhiều vị trí khác nhau, ví dụ như các máy chủ thư điện tử, máy tính bàn hoặc ở các cổng mạng của tổ chức;

g) Các thủ tục quản lý và các trách nhiệm giải quyết vấn đề bảo vệ chống virút

trên các hệ thống, đào tạo việc sử dụng, báo cáo và khắc phục sự tấn công của virút

h) Các kế hoạch liên tục trong kinh doanh phù hợp với việc khắc phục sự tấn công của virút, bao gồm toàn bộ dữ liệu cần thiết và phần mềm sao lưu và các sắp xếp khôi phục;

i) Các thủ tục thẩm tra toàn bộ thông tin liên quan đến phần mềm có hại và đảm bảo rằng bản tin cảnh báo chính xác và đầy đủ thông tin. Các nhà quản lý đảm bảo rằng các nguồn đủ tiêu chuẩn, ví dụ các báo chí danh tiếng, các địa chỉ mạng hoặc các nhà cung cấp phần mềm diệt virút đáng tin, được sử dụng để phân biệt các trò lừa và virút thực. Nhân viên nhận thức được vấn đề về các trò lừa bịp và phải làm gì khi nhận được chúng.

3. Kiểm soát chung

a) Những tài liệu, thiết bị, tài sản của công ty đều không được phép mang về nhà (điều này có thể thêm vào trong các điều khoản và điều kiện thuê nhân công).

III. An ninh môi trường và vật lý

1. Vành đai an ninh vật lý

a) Vành đai an ninh được thiết lập rõ ràng:

- Văn bản, công văn trao đổi trong nội bộ công ty được lưu trữ trong tủ kính, chống cháy, có khóa và được đặt trong phòng riêng, do người phụ trách của phòng hành chính, tổn hợp và nhân sự quản lý. Phòng ra vào có cơ chế kiểm soát bằng thẻ từ.

- Văn bản, công văn, hóa đơn, bảng kê khai thuế trao đổi với khách hàng bên ngoài được lưu trữ trong tủ kính, chống cháy, có khóa và được đặt trong phòng riêng, do người phụ trách của phòng hành chính, tổng hợp và nhân sự quản lý. Phòng ra vào có cơ chế kiểm soát bằng thẻ từ.

- Chiến lược phát triển kinh doanh, thông tin đối thủ cạnh tranh, thông tin về lương, thưởng của nhân viên… được lưu trữ trong tủ kính, chống cháy, có khóa và được đặt trong phòng riêng, do người phụ trách của phòng hành chính, tổng hợp và nhân sự quản lý. Phòng ra vào có cơ chế kiểm soát bằng thẻ từ.

- Tài liệu source code, ảnh, các tài liệu liên quan đến dự án sản xuất game bằng giấy… được lưu trữ trong tủ kính, chống cháy, có khóa và được đặt trong phòng riêng, do người phụ trách của phòng sản xuất game quản lý. Phòng ra vào có cơ chế kiểm soát bằng thẻ từ.

- Thiết bị Wacom được lưu trữ trong tủ kính, chống cháy, có khóa và được đặt trong phòng riêng, do người phụ trách của phòng sản xuất game quản lý. Phòng ra vào có cơ chế kiểm soát bằng thẻ từ.

- Các thiết bị lưu trữ (USB, ổ cứng, CD-ROM) được lưu trữ trong tủ kính, chống cháy, có khóa và được đặt trong phòng riêng, do người phụ trách của phòng sản xuất game quản lý. Phòng ra vào có cơ chế kiểm soát bằng thẻ từ.

- Các máy điện thoại để test game được lưu trữ trong tủ kính, chống cháy, có khóa và được đặt trong phòng riêng, do người phụ trách của phòng sản xuất game quản lý. Phòng ra vào có cơ chế kiểm soát bằng thẻ từ.

2. Kiểm soát xâm nhập vật lý

a) Các khách đến các khu vực an ninh được giám sát hoặc rà soát và ghi lại ngày giờ ra vào của họ. Họ chỉ được cho phép truy cập vì các mục đích cụ thể.

b) Truy cập tới các công văn, văn bản được kiểm soát và hạn chế chỉ cho các cá nhân được cấp phép.

c) Các quyền truy cập tới các khu vực an ninh được xem xét và cập nhật một cách đều đặn.

3. An ninh cho các thiết bị ngoại vi

a) Nghiêm cấm việc sử dụng USB, thẻ nhớ trong nội bộ công ty, có thể niêm phong các ổ USB, thẻ nhớ.

b) Nghiêm cấm việc cài đặt các phần mềm cho phép gửi file peer-to-peer, ngăn chặn các trang web cho phép upload, gửi file.

c) Tất cả các máy tính có gắn camera khi sử dụng trong quá trình làm việc tại công ty phải gián giấy che.

d) Tất cả các nhân viên mang máy tính cá nhân ra, vào công ty phải được nhân viên kỹ thuật kiểm tra, được sự đồng ý của lãnh đạo

4. Kiểm soát chung

a) KHI THÍCH HỢP, công văn và các văn bản trao đổi trong nội bộ công ty do các cá nhân liên quan lưu nên được lưu trữ trong các tủ có khoá riêng của cá nhân, đặc biệt ngoài giờ làm việc;

b) KHI THÍCH HỢP, văn bản, công văn, hóa đơn, bảng kê khai thuế trao đổi với khách hàng bên ngoài do các cá nhân liên quan lưu nên được lưu trữ trong các tủ có khoá riêng của cá nhân, đặc biệt ngoài giờ làm việc;

c) KHI THÍCH HỢP, chiến lược phát triển kinh doanh, thông tin đối thủ cạnh tranh, thông tin về lương, thưởng của nhân viên… do các cá nhân liên quan lưu nên được lưu trữ trong các tủ có khoá riêng của cá nhân, đặc biệt ngoài giờ làm việc;

d) Các máy photo nên được khóa ngoài giờ làm việc chính thức (hoặc bảo đảm an toàn khỏi việc sử dụng trái phép bằng cách này cách khác);

e) Thông tin nhạy cảm hoặc được phân loại, khi in xong nên được xoá ngay khỏi máy in.

f) Chính sách màn hình "sạch": máy tính cá nhân và cổng in và các cổng khác của máy tính nên được đóng khi không dùng và nên được bảo vệ bằng các khóa mật mã, mật khẩu hoặc các kiểm soát khác khi không sử dụng.

g) Các thiết bị lưu trữ (USB, ổ cứng, CD-ROM) khi sử dụng phải được log lại bằng văn bản, sử dụng xong phải trả lại, có ký nhận và phải được sự cho phép của lãnh đạo.

h) Các máy điện thoại để test game khi sử dụng phải được log lại bằng văn bản, sử dụng xong phải trả lại, có ký nhận và phải được sự cho phép của lãnh đạo.

i) Nghiêm cấm việc sử dụng các chức năng liên quan đến ghi âm, ghi hình trong công ty.

IV. An ninh cá nhân

1. Giáo dục và đào tạo an toàn thông tin

a) Toàn bộ các nhân viên của tổ chức được đào tạo thích hợp và các cập nhật thường xuyên về chính sách và thủ tục của tổ chức. Điều này bao gồm các yêu cầu an toàn, trách nhiệm pháp lý và các kiểm soát kinh doanh, cũng như đào tạo việc sử dụng đúng các phương tiện xử lý thông tin trước khi truy cập tới thông tin hoặc các dịch vụ được cho phép ví dụ thủ tục đăng nhập, sử dụng các gói phần mềm.

b) Toàn bộ các nhân viên của công ty được đào tạo thích hợp và các cập nhật thường xuyên về chính sách và thủ tục của tổ chức, được đào tạo việc sử dụng đúng các phương tiện xử lý thông tin trước khi truy cập tới thông tin cơ sở dữ liệu.

c) Technical leader được đào tạo thích hợp và cập nhật thường xuyên về chính sách và thủ tục của tổ chức, được đào tạo việc sử dụng các tool backup để thực hiện việc sao lưu cơ sở dữ liệu.

d) Toàn bộ các nhân viên, cá nhân liên quan của công ty được đào tạo thích hợp và các cập nhật thường xuyên về chính sách và thủ tục của tổ chức, được đào tạo việc sử dụng các chính sách, quy trình về việc sử dụng mật khẩu truy cập tới cơ sở dữ liệu.

e) Toàn bộ các nhân viên, cá nhân liên quan của công ty được đào tạo, giải thích về các khu vực an ninh và được chỉ dẫn về các yêu cầu an ninh của khu vực đó.

f) Toàn bộ các nhân viên, cá nhân liên quan của công ty được đào tạo, giải thích về quy chế, chính sách sử dụng mạng máy tính nội bộ trong công ty và hướng dẫn thi hành.

2. An ninh theo định nghĩa và nguồn công việc

2.1 An ninh theo các trách nhiệm công việc

a) Các vai trò và trách nhiệm an ninh, khi được đặt trong chính sách an ninh thông tin của tổ chức được tài liệu hóa một cách thích hợp. Chúng nên gồm mọi trách nhiệm chung đối với việc thực hiện hoặc duy trì chính sách an ninh cũng như mọi trách nhiệm đặc biệt đối với việc bảo vệ các tài sản cụ thể hoặc đối với

việc thi hành các quy trình hoặc các hoạt động an ninh cụ thể.

2.2 Chính sách và kiểm tra nhân sự

a) Tính sẵn có của các giấy tờ dẫn chứng về các đặc điểm, ví dụ về công việc và cá nhân;

b) Kiểm tra (đầy đủ và chính xác) hồ sơ của ứng viên;

c) Xác nhận bằng cấp được yêu cầu và phẩm chất nghề nghiệp;

d) Kiểm tra nhận dạng (hộ chiếu hoặc giấy tờ tương tự).

2.3 Thỏa thuận về tính bảo mật

a) Các thỏa thuận về tính bảo mật hoặc không làm lộ được sử dụng để đưa ra lưu ý rằng thông tin là bảo mật hoặc bí mật. Các nhân viên ký kết một thỏa thuận như một phần của các điều khoản và điều kiện tuyển dụng ban đầu của họ.

Yêu cầu những người sử dụng không chủ định, nhân viên và bên thứ ba, chưa có hợp đồng bao gồm thỏa thuận về tính bảo mật, ký kết một thỏa thuận về tính bảo mật trước khi được phép truy cập tới các phương tiện xử lý thông tin.

Các thỏa thuận về tính bảo mật được soát xét khi có các thay đổi về thời hạn công việc hoặc hợp đồng, cụ thể là khi những người lao động rời tổ chức hoặc các hợp đồng đã hết hạn.

3. Chính sách và kiểm tra nhân sự

a) Đảm bảo quyền lợi, đưa ra những mục tiêu thăng tiến, phát triển rõ ràng của nhân viên, lương thưởng ở mỗi cấp.

CHƯƠNG 4.

KẾT LUẬN

Với dân số 90 triệu người, trong đó gần 44% sử dụng Internet, nhiều người truy cập sử dụng Internet trên thiết bị di động, thị trường công nghệ đang rất phát triển tại Việt Nam. Việt Nam trở thành mục tiêu của các nhà phát triển ứng dụng và được các nhà đầu tư trong và ngoài nước để mắt. Nhiều tập đoàn đa quốc gia như Samsung và Intel đang có sự hiện diện vô cùng lớn tại đây, trong khi các startup công nghệ của Việt Nam cũng nhanh chóng nhập cuộc. Tuy chưa có số liệu chính thức nào về bức tranh khởi nghiệp Việt Nam, tập đoàn Softbank của Nhật Bản ước tính có khoảng 1.500 startup đang hoạt động, trong đó phần lớn là các startup liên quan đến công nghệ, từ con số có thể thấy Việt Nam có tỉ lệ startup trên số dân cao hơn hẳn các láng giềng như Trung Quốc, Indonesia và Ấn Độ.[8]

Đặc điểm của các startup công nghệ ở Việt Nam là quy mô mới chỉ ở mức vừa và nhỏ, các doanh nghiệp này tập trung phần lớn công sức, thời gian vào việc phát triển kinh doanh, tìm kiếm những ý tưởng, sáng tạo, sản xuất sản phẩm ứng dụng công nghệ mới… nhưng chưa để ý, dành thời gian, công sức, chưa hiểu rõ các phương pháp tiếp cận đến việc đảm bảo an toàn thông tin cho doanh nghiệp của mình.

Sau khi lựa chọn một doanh nghiệp vừa và nhỏ đặc thù, với lĩnh vực hoạt động liên quan đến công nghệ thông tin, cụ thể là sản xuất và phân phối game online trên điện thoại di động, một ngành mới nổi và rất nhiều tiềm năng phát triển tại Việt Nam, tiến hành khảo sát về thực trạng đảm bảo an toàn thông tin đối với doanh nghiệp này, xác định các rủi ro, nguy cơ và đưa ra các biện pháp kiểm soát, luận văn đã xây dựng được cho doanh nghiệp này những chính sách, quy trình, quy định trong việc đảm bảo an toàn thông tin theo đúng tiêu chuẩn ISO27001, cụ thể như sau:

1. 01 chính sách về các lĩnh vực:

- Kiểm soát truy cập

[8] Theo http://ictnews.vn

- Quản lý truyền thông và hoạt động

- An ninh môi trường và vật lý

- An ninh cá nhân

- Đào tạo nhân viên

2. 04 quy trình:

- Quy trình đo lường của hệ thống quản lý an toàn thông tin

- Quy trình về quản lý source code, các bản mềm tài liệu

- Quy trình về giáo dục nhận thức, đào tạo về an toàn thông tin

- Quy trình hành động phòng ngừa đối với hệ thống quản lý an toàn thông tin

3. 02 quy định:

- 01 quy định chung đối với nhân viên

- 01 quy định những việc phải làm và những việc không được làm đối với nhân viên mới.

Các tiêu chuẩn của ISO27001 đã được áp dụng

01 chính sách, 04 quy trình và 02 quy định đã tuân thủ các tiêu chuẩn sau của ISO27001:

- 7 điều khoản bắt buộc về phạm vi tổ chức, lãnh đạo, lập kế hoạch, hỗ trợ, vận hành hệ thống, đánh giá hiệu năng hệ thống, cải tiến hệ thống.

- Các lĩnh vực kiểm soát liên quan bao gồm: chính sách ATTT, ATTT trong tổ chức, ATTT nhân sự, quản lý tài sản, kiểm soát truy cập, ATTT vật lý và nơi làm việc, ATTT trong quá trình vận hành, quản lý sự cố ATTT, đảm bảo tính hoạt động liên tục trong trường hợp thảm họa và sự tuân thủ.

Những lợi điểm mà những chính sách, quy trình và quy định mang lại

Luận văn đã giải quyết được những khó khăn mà một doanh nghiệp vừa và nhỏ đã gặp phải trong việc đảm bảo an toàn thông tin:

- Nâng cao nhận thức của toàn tổ chức về việc đảm bảo ANTT

- Tiết kiệm chi phí doanh nghiệp phải bỏ ra để thực hiện các biện pháp kiểm soát rủi ro, mọi chi phí về nguồn lực và tài chính được giảm thiểu phù hợp với đặc trưng của một doanh nghiệp vừa và nhỏ như: về mặt nhân sự tham gia được giảm thiểu bao gồm 01 nhân viên phụ trách chính trong việc xây dựng và đảm bảo quy trình an toàn thông tin theo tiêu chuẩn ISO27001 trong tổ chức, các lãnh đạo và toàn thể nhân viên phòng ban, về mặt thời gian xây dựng và triển khai các chính sách, quy trình và quy định ngắn, dễ áp dụng cho các doanh nghiệp vừa và nhỏ, áp dụng nhiều công nghệ tiên tiến trong việc triển khai như các công cụ phần mềm trong việc quản lý các tài liệu, source code, các công cụ quản lý các sự cố, công việc của nhân viên và cuối cùng, sẽ dẫn đến tiết kiệm chi phí tài chính phải bỏ ra cho doanh nghiệp.

- Việc triển khai các chính sách, quy trình và quy định trong việc đảm bảo an toàn thông tin được tinh giản và nâng cao hiệu quả trong việc phối hợp, trao đổi giữa các bộ phận.

- Nâng cao nhận thức đối với các cam kết thực hiện của lãnh đạo.

Tuy nhiên với thời gian khảo sát ngắn có thể chưa liệt kê được tất cả các vấn đề mà doanh nghiệp gặp phải trong việc đảm bảo an toàn thông tin, khi tiến hành các chính sách, quy trình và quy định, sẽ gặp phải những vấn đề phát sinh, cần tiếp tục điều chỉnh, sửa đổi và bổ sung sao cho phù hợp nhất với thực tế của doanh nghiệp.

So sánh các tiêu chí khi áp dụng quy trình của luận văn và thuê tư vấn ngoài trong việc đảm bảo an toàn thông tin theo chuẩn ISO27001 đối với các doanh nghiệp vừa và nhỏ

Các tiêu chí	Thuê tư vấn ngoài	Áp dụng quy trình của luận văn
Tài chính	- Các phần mềm được yêu cầu sử dụng đa số phải mua. - Phải tiến hành thuê các công ty đào tạo về ATTT để giảng dậy, nâng cao nhận	- Các phần mềm triển khai thực hiện được tận dụng từ phần mềm mã nguồn mở miễn phí. - Không cần thuê các công ty đào tạo về ATTT mà có thể sử

	thức cho nhân viên.	dụng bộ tài liệu trong quy trình để giảng dậy, nâng cao nhận thức cho nhân viên.
Thời gian	Mất một khoảng thời gian để khảo sát, đánh giá rủi ro, đưa ra biện pháp kiểm soát rồi mới tiến hành đưa vào áp dụng.	- Có thể triển khai được luôn với 70% khối lượng công việc của quy trình. - 30% khối lượng công việc còn lại sẽ tùy vào tình hình thực tế cụ thể của công ty mà tiến hành khảo sát, cập nhật, sửa đổi, đánh giá rủi ro, đưa ra biện pháp kiểm soát tương ứng.
Nhân sự tham gia chỉ đạo việc thực hiện quy trình	Một đội ngũ chiếm khoảng 10% nhân sự của công ty.	01 người.

Hướng phát triển tiếp theo

Hướng tiếp theo, tôi có đề xuất sẽ tiếp tục tiến hành khảo sát các doanh nghiệp vừa và nhỏ đặc trưng trong các lĩnh vực khác như công nghiệp, dịch vụ về vấn đề đảm bảo an toàn thông tin, và xây dựng, triển khai các chính sách, quy trình và quy định cho các doanh nghiệp này. Từ những kết quả thực tiễn thu được, luận văn mong muốn từ đó khái quát ra một bộ khung chính sách, quy trình và quy định đảm bảo về an toàn thông tin theo chuẩn ISO27001 cho các doanh nghiệp vừa và nhỏ tại Việt Nam.

Hy vọng với bộ khung chính sách, quy trình và quy định cho các doanh nghiệp vừa và nhỏ tại Việt Nam trong việc đảm bảo an toàn thông tin theo chuẩn ISO27001 này, sẽ giúp đỡ được một phần nào cho các doanh nghiệp vừa và nhỏ tại Việt Nam, hiện đang chiếm gần 95% tổng số các doanh nghiệp, đảm bảo an toàn về an toàn thông tin cho các công ty startup, góp một phần nhỏ bé vào công cuộc xây dựng và bảo vệ đất nước.

TÀI LIỆU THAM KHẢO

Tài liệu tiếng Việt

1. Bộ Thông tin và Truyền thông (2014), *Thông tư 24/2014/TT-BTTT Quy định chi tiết về hoạt động quản lý, cung cấp và sử dụng dịch vụ trò chơi điện tử trên mạng.*

2. Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ (2005), *Tiêu chuẩn quốc gia TCVN 7562 Công nghệ thông tin – Mã thực hành quản lý an ninh thông tin.*

3. Thế Hảo (2008), *Thực trạng triển khai ISO27001 tại Việt Nam*, http://antoanthongtin.vn.

4. *"Báo cáo tổng quan về tình hình doanh nghiệp"*, Báo cáo phục vụ Hội nghị Thủ tướng Chính phủ với doanh nghiệp.

5. KS. Đinh Quang Hùng (2015), *Hệ thống quản lý An toàn thông tin theo tiêu chuẩn ISO 27001:2013*, http://antoanthongtin.vn

Tài liệu tiếng Anh

6. International Organization for Standardization (2014), *ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

7. International Organization for Standardization (2013), *ISO/IEC 27001, Information technology - Security techniques - Information security management systems – Requirements.*

8. International Organization for Standardization (2013), *ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls.*

9. Gaffri Johnson Senior Security Advisor at Neupart (2014), *Measuring ISO 27001 ISMS processes.*

10. Scott Ritchie, *Security Risk Management.*