SỔ TAY BẢO MẬT THÔNG TIN

Đơn vị: ISMS
Ngày ban hành: 15/07/2021
Ngày có hiệu lực: 15/07/2021
Lần ban hành: 02
Tài liệu số: ISO-STBM.01

TÌNH TRẠNG SỬA ĐỔI TÀI LIỆU

Lần sửa đổi	Tình trạng sửa đổi			Ngày có hiệu lực
	Nội dung trước khi sửa đổi	Nội dung sau khi sửa đổi	Trang	
1	Tạo mới tài liệu	Tạo mới tài liệu		15/07/2021
2	Quy định về ATTT khi sử dụng dịch vụ đám mấy	Cung cấp thêm các chỉ số đo lường	6	26/02/2023
3	An toàn mạng	Cập nhật quy định đo lường thời gian hoạt động Internet	21	26/02/2025

SỔ TAY BẢO MẬT THÔNG TIN

Mục Lục

SỔ TAY BẢO MẬT THÔNG TIN

1. MỤC ĐÍCH

Sổ tay này trình bày các kiểm soát cần thiết về hệ thống, vật lý và con người để bảo vệ tài sản một cách thích hợp, và các bước thực hiện.

2. PHẠM VI ÁP DỤNG

Áp dụng cho toàn bộ nhân viên thuộc các phòng / ban đang làm việc tại công ty Techvify software

3. ĐỊNH NGHĨA THUẬT NGỮ

Định nghĩa thuật ngữ thì tuân theo "**ISO/IEC 27001: 2022**"

Thuật ngữ	Định nghĩa
Trưởng ban bảo mật thông tin	Tổng hợp về việc thực hiện và vận hành hệ thống quản lý hệ thống bảo mật thông tin của công ty.
Ban ISO	Ban ISO là những người chịu trách nhiệm tổ chức thực hiện các hoạt động quản lý chất lượng tại các đơn vị khu vực văn phòng công ty, doanh nghiệp
Tổ chức	Tổ chức hình thành bởi người quản lý bộ phận liên quan đến vận hành, ứng dụng hệ thống quản lý bảo mật thông tin của công ty, và người chịu trách nhiệm quản lý các nghiệp vụ riêng biệt.
Nhân viên	Người lao động của công ty

4. CẤU TRÚC CỦA TÀI LIỆU NÀY

Bản sổ tay này được xây dựng dựa theo quy định của **"ISO/IEC 27001: 2022 - Phụ lục A"**.

5. CÁC BIỆN PHÁP KIỂM SOÁT VỀ TỔ CHỨC

5.1 Chính sách an toàn thông tin

5.2 Vai trò và trách nhiệm an toàn thông tin

Vai trò và trách nhiệm được thể hiện trong sơ đồ tổ chức và chức năng nhiệm vụ các phòng ban.

Công ty đã thành lập ban ISO phụ trách thực thi và giám sát liên quan đến bảo mật thông tin của công ty.

5.3 Phân tách nhiệm vụ

Được thể hiện trong chức năng nhiệm vụ các phòng ban và chức năng nhiệm vụ ban ISO.

5.4 Trách nhiệm của lãnh đạo

Ban lãnh đạo thể hiện sự cam kết với an toàn thông tin và đảm bảo rằng hệ thống

quản lý an toàn thông tin (ISMS) được thiết lập, triển khai và duy trì đúng cách.

5.5 Thiết lập và duy trì liên lạc với cơ quan chức năng

Ban ISO sẽ xác định cơ quan liên quan và thông tin liên lạc trong **"Danh sách nhóm chuyên gia hỗ trợ"** để xây dựng, duy trì phương án liên lạc một cách dễ dàng khi cần thiết.

5.6 Liên lạc thường xuyên với nhóm chuyên gia

Ban ISO sẽ xác định tổ chức chuyên môn và thông tin liên lạc trong **"Danh sách nhóm chuyên gia hỗ trợ"** để xây dựng, duy trì phương án liên lạc một cách dễ dàng khi cần thiết.

5.7 Cập nhật thông tin tình báo về các mối đe dọa

Ban ISO sẽ phụ trách việc cập nhật thông tin tình báo về các mối đe dọa và điền vào file theo dõi

5.8 An toàn thông tin trong quản lý dự án

Quản lý member trong dự án (ra vào dự án, đang thực hiện dự án, ở lại sau khi dự án kết thúc)

STT	Giai đoạn	Công việc	Mô tả nội dung	Nơi lưu trữ	Phân quyền	Note
1	Chuẩn bị	Lên kế hoạch nhân sự cho dự án	Sau khi tiếp nhận thông tin dự án, PL sẽ lên kế hoạch lựa chọn nhân sự cho dự án		PL	có thể trao đổi với trưởng phòng để thêm thông tin các thành viên
		Tạp môi trường cần thiết cho dự án	1. PL sẽ tạo Project lên hệ thống trao đổi thông tin và thêm các thành viên tham gia dự án vào 2. PL tạo môi trường phát triển ự án:+ Set up server + Tạo project trên gitlab và thêm các thành viên tham dự +Tạo thư mục dự án và cập	Cloud+Gitlab	PL, các thành viên trong dự án	
		Meeting: kickoff dự án	Tài liệu meeting kickoff dự án	Cloud+Gitlab	PL, Dự án, các thành viên khác	
2	Design & Development	Báo cáo định kỳ	Tài liệu báo cáo tiến độ, trạng thái dự án	Server/Cloud	PL,team leader, các thành viên khác	
		Meeting	Tài liệu meeting	Server/Cloud	PL,team leader, các thành viên khác	
		Design	Tàii liệu thiết kế hệ thống	Server/Cloud	PL,team leader, các thành viên khác	
		Coding	Source code hệ thống, các bản buid và tài liệu	Gitlab	PL, Team leader, Developer, các thành viên khác	
		QA/QC	Tài liệu kiểm thử và các tài liệu liên quan	Driver	PL, Team leader, QA/QC, các thành viên khác	
3	Release	Release bàn giao cho khách hàng	Lưu các phiên bản release + tài liệu liên quan	Gitlab + Cloud	PL, Team leader, các thành viên khác	
4	Maintennance	Quản lý và maintance cho KH	Hỗ trợ quản lý và maintance cho KH	Gitlab + Cloud	PL, Thành viên chủ chốt của dự án(tuỳ thuộc vào thực tế dự án)	
5	Close	Backup	Lưu trữ thông tin tài liệu và source mới nhất	Gitlab + Cloud	PL, Thành viên chủ chốt của dự án(tuỳ thuộc vào thực tế dự án)	
		Cập nhật phân quyền	Xoá các thành viên không còn trực thuộc ra khỏi hệ thống quản lý dự án :gitlab,...	Gitlab + Cloud	PL, Thành viên chủ chốt của dự án(tuỳ thuộc vào thực tế dự án)	

Phân quyền các thành viên trên gitlab:

Mỗi một PL sẽ có một group project riêng với quyền maintainer.

Trưởng bộ phận được có quyền truy cập vào tất cả các dự án của bộ phận mình thông qua các group project với quyền maintainer.

Các thành viên khác sẽ được gán quyền trong project tương ứng với quyền maintainer.

5.9 Kiểm kê thông tin và các tài sản liên quan khác

Được thể hiện trong quy trình quản lý tài sản.

5.10 Việc sử dụng thông tin và các tài sản liên quan khác được chấp nhận

Được thể hiện trong quy trình quản lý tài sản.

5.11 Hoàn trả tài sản

Đối với trường hợp nghỉ việc, ban bảo mật thông tin sẽ yêu cầu trưởng bộ phận xử lý như sau, và sẽ xác minh đã được thực hiện hay chưa.

5.11.1.1 Thu hồi thẻ nhân viên, nhận diện chấm công (khuôn mặt)

5.11.1.2 Thu hồi máy tính, laptop, thiết bị làm việc và điện thoại di động mà công ty đã cấp.

5.11.1.3 Thu hồi hoặc hủy hồ sơ lưu trên giấy.

5.11.1.4 Thu hồi các tài khoản Email

5.12 Phân loại thông tin

Được thể hiện trong quy trình quản lý tài sản.

5.13 Ghi nhãn thông tin

Được thể hiện trong quy trình quản lý tài sản.

5.14 Chuyển giao thông tin

Được thể hiện trong quy trình quản lý tài sản.

5.15 Kiểm soát truy cập

a) Thông tin chỉ người cần thiết cho nghiệp vụ mới được truy cập, còn quyền truy cập và quyền thao tác thì chỉ cấp cho các trường hợp đã được phê chuẩn.
b) Lưu lại log của việc truy cập vào hệ thống.
c) Lưu lại log các thao tác trên dữ liệu (tạo, sửa, xoá, chia sẻ) trên hệ thống Nextcloud.
d) Thông tin phân quyền truy cập vào các vùng thông tin được thể hiện trong bảng ma trận phân quyền.

5.16 Quản lý danh tính

a) Nhân viên chỉ có thể truy cập vào hệ thống được cấp bởi công ty bằng tài khoản được cấp theo mã nhân viên. Mỗi tài khoản chỉ được cấp cho một nhân viên.
b) Nhân viên chỉ có thể truy cập vào hệ thống kênh chat của công ty (phần mềm Microsoft Teams) bằng tài khoản được cấp theo mã nhân viên. Mỗi tài khoản chỉ được cấp cho một nhân viên.
c) Đối với tất cả các ứng dụng được sử dụng tại cong ty, công ty cung cấp quyền truy cấp qua email cá nhân, mỗi cá nhân tương ứng một user. Cá nhân không được sử dụng account của người khác để đăng nhập hệ thống.
d) Đối với hệ thống Azure Cloud để lưu trữ các tài liệu, truy cập bằng tài khoản công ty.

5.17 Thông tin xác thực

a) Tài khoản Office 365 của cty cấp được xác thực bởi mật khẩu, vàphải được xác thực 2 lớp MFA.

b) Cửa ra vào công ty dùng nhận diện khuôn mặt để xác thực.

5.18 Quyền truy cập

Thông tin truy cập sẽ được cung cấp trong ngày nhân viên onboard và người nhận được yêu cầu đổi mật khẩu và bật tính năng MFA (xác thực 2 lớp) khi đăng nhập lần đầu.

5.19 An toàn thông tin trong các mối quan hệ với nhà cung cấp

a) Dưới đây là các nhà cung cấp của công ty.

1) Nhà cung cấp ISP

2) Nhà cung cấp thiết bị máy tính phục vụ sản xuất, kinh doanh.

3) Nhà cung cấp thiết bị camera

4) Nhà cung cấp thiết bị kiểm soát ra vào

5) Server Cloud

b) Ký cam kết bảo mật thông tin đối với các nhà cung cấp

5.20 Giải quyết vấn đề an toàn thông tin trong thỏa thuận với nhà cung cấp

a) Việc sử dụng dịch vụ được cung cấp phải tuân theo quy trình sau

1) Thực hiện đánh giá đối với nhà cung cấp dựa vào **Phiếu đánh giá nhà cung cấp.**

2) Cân nhắc các mục yêu cầu bảo mật thông tin, ký hợp đồng gồm các mục sau:

① Ký kết hợp đồng liên quan đến xử lý thông tin như hợp đồng bảo mật.

② Thỏa thuận liên quan đến bản quyền, quyền sở hữu code và sở hữu trí tuệ của code (trường hợp phát triển).

③ Quản lý nơi ra vào và khu vực làm việc.

④ Thỏa thuận liên quan đến hợp đồng đặt cọc trong trường hợp bên ủy thác không thực hiện hợp đồng.

Ban ISO sẽ cân nhắc đến rủi ro có thể xảy ra và kí kết hợp đồng với bên thứ ba nếu cần thiết

5.21 Quản lý an toàn thông tin trong chuỗi cung ứng CNTT-TT

a) Trong hợp đồng với nhà cung cấp sẽ bao gồm các mục liên quan đến việc tái ủy thác khi cần thiết.

b) Sau khi cân nhắc đến tính liên tục trong kinh doanh và các hạng mục bảo mật liên quan đến dịch vụ dưới đây của nhà cung cấp cloud service, thì mới tiến hành chọn sử dụng cloud service.

1) Khả năng truy cập toàn cầu và độ sẵn sàng.

2) An toàn – Bảo mật

3) Quản lý dịch vụ

5.22 Giám sát, xem xét và quản lý thay đổi các dịch vụ của nhà cung cấp

Đối với người cung cấp dịch vụ, ban bảo mật thông tin sẽ dựa vào "Danh sách nhà cung cấp" để tiến hành xác nhận tình trạng thực hiện và tuân thủ hợp đồng với tần suất đã được quy định (ít nhất 1 lần 1 năm).

Trường hợp có thay đổi trong nội dung hợp đồng và mức độ dịch vụ giữa công ty và nhà cung cấp, kiểm tra xem có thể chấp nhận điểm thay đổi hay không, và tiến hành xem lại nội dung hợp đồng.

5.23 An toàn thông tin khi sử dụng các dịch vụ đám mây

Tiêu chí lựa chọn dịch vụ cloud:

1. Khả năng truy cập toàn cầu và độ sẵn sàng: hỗ trợ toàn cầu và luôn hoạt động 24/24 để có thể truy cập được
2. An toàn – Bảo mật : độ bảo mật an toàn, có hệ thống backup sao lưu dữ liệu khi gặp sự cố
3. Quản lý dịch vụ: dễ quản lý phù hợp với doanh nghiệp, hệ thống có sự hỗ trợ gì
4. Chi phí: Gửi mail thông báo khi vượt quá chi phí quy định cho cloud 10%

Các dịch vụ cloud đang sử dụng:

1. AWS
2. Azure
3. Microsoft Office 365

Các biện pháp xử lý nếu dịch vụ cloud có sự cố:

1. Đối với server : khi gặp sự cố cần nhanh chóng khắc phục, nếu không giải quyết được thì phải sử dụng bản backup nếu có, thời gian uptime phải >=99%
2. Đối với hệ thống quan trọng cần có bản backup (tùy vào từng dự án mà PM sẽ quyết định)

Phương pháp giám sát và đánh giá:

1. Đối với các server web : định kì kiểm tra sự kết nối hệ thống xem có ổn định hay không
2. Cấu hình giám sát hệ thống, nếu có vấn đề xảy ra sẽ mail thông báo (CPU server chạy vượt 70%, Account sử dụng phí vượt ngưỡng qui định….)

5.24 Lập kế hoạch và chuẩn bị quản lý sự cố an toàn thông tin

Trách nhiệm và quy trình quản lý và cải thiện sự cố bảo mật thông tin được mô tả trong tài liệu **"Quy trình_Quản lý sự cố"**. (Xử lý, khắc phục, phòng ngừa)

5.25 Đánh giá và quyết định các sự kiện an toàn thông tin

Định nghĩa sự cố, sự kiện được mô tả trong tài liệu **"Quy trình_Quản lý sự cố"**

5.26 Ứng phó các sự cố an toàn thông tin

Quy trình xử lý cho sự cố bảo mật thông tin thì được mô tả trong tài liệu **"Quy trình_Quản lý sự cố"**

5.27 Rút kinh nghiệm từ các sự cố an toàn thông tin

Ban ISO sẽ quản lý, phân tích sự cố bảo mật, nếu có vấn đề trong vận hành

ISMS hiện tại thì sẽ lập kế hoạch và kiến nghị với Tổng Giám đốc. Ngoài ra, trong bản kế hoạch, làm rõ cách thức xử lý, chi phí, ngày dự định thực hiện, người chịu trách nhiệm giải quyết.

5.28 Thu thập bằng chứng

Trong trường hợp cá nhân hay tổ chức nào đó trong lúc xử lý sau sự cố có liên đới đến pháp luật mà nguyên nhân đến từ hệ thống thông tin, thì ban bảo mật thông tin sẽ nỗ lực thu thập và bảo toàn chứng cứ.

5.29 An toàn thông tin trong thời gian gián đoạn

a) Quy trình kinh doanh liên tục

b) Phân tích rủi ro tài sản

Trong số các trang thiết bị, cơ sở xử lý thông tin đã xác định tại **Danh mục tài sản**, đối tượng phân tích rủi ro bảo mật thông tin liên tục được xác định theo mức độ quan trọng của tài sản.

c) Đối với tài sản ở a), sẽ cân nhắc về rủi ro dưới đây:

1) Thiên tai như động đất, hỏa hoạn, lũ lụt.

2) Lỗi do con người.

3) Lỗi hệ thống

4) Vấn đề về sức khỏe

5) Xác định những quy trình vận hành chịu ảnh hưởng khi phát sinh rủi ro của b) ở trên, lên kế hoạch phục hồi cho trường hợp phát sinh rủi ro.

d) Xem xét về khả năng phát sinh rủi ro và độ ảnh hưởng trong trường hợp phát sinh rủi ro, quyết định thứ tự ưu tiên dựa trên kết quả xem xét.

5.30 Sẵn sàng về CNTT-TT cho hoạt động kinh doanh liên tục

5.31 Các yêu cầu pháp lý, luật định, quy định và hợp đồng

a) Ban ISO sẽ cập nhật những quy định, luật hay các mục yêu cầu liên quan đến bảo mật thông tin trên hợp đồng mà công ty cần phải tuân thủ, và đưa vào trong **Danh mục yêu cầu pháp luật cần tuân thủ**. **Danh mục yêu cầu pháp luật cần tuân thủ** sẽ xem xét lại 1 lần 1 năm.

b) Ban ISO sẽ đảm bảo nhân viên của công ty đều có thể tham khảo trên Bảng quy định pháp lệnh liên quan đến hệ thống thông tin khi cần thiết.

c) Để đáp ứng được các yêu cầu đã chỉ định thì sẽ tiến hành đào tạo khi cần

5.32 Quyền sở hữu trí tuệ

a) Bảo vệ bản quyền của sách hoặc các tài liệu khách cho mượn.

b) Người quản lý hệ thống thông tin sẽ quản lý bản quyền của tất cả các gói phần mềm bán trên thị trường.

c) Những gói phần mềm, hay phần mềm miễn phí khi sử dụng phải tuân thủ hợp đồng cho phép sử dụng đó.

5.33 Bảo vệ hồ sơ

Loại bản ghi *Phải lưu trữ bản ghi của công ty dựa trên pháp lệnh liên quan trong thời gian lưu trữ được ghi trong bảng dưới đây.*	**Thời gian lưu trữ**
■ Điều lệ ■ Tài liệu liên quan đăng kí kinh doanh ■ Tài liệu liên quan đến tố tụng ■ Tài liệu liên quan đến quyền sở hữu trí tuệ như bằng sáng chế ■ Tài liệu pháp lý liên quan đến hoạt động của công ty ■ Quy tắc, nội quy công ty	Vĩnh viễn
■ Sổ kế toán thương mại Sổ kế toán (sổ nhật ký, sổ ký sự, sổ cái), bảng đối chiếu vay nợ, bản tính toán lỗ lãi, bản chi tiết phụ thuộc ■ Tài liệu quan trọng liên quan đến kinh doanh Danh sách cổ đông, sổ gốc trái phiếu, biên bản họp đại hội cổ đông, biên bản họp ban lãnh đạo công ty, bản báo cáo kinh doanh, phương án xử lý lợi nhuận (đề xuất xử lý tổn thất), tài liệu có thể trở thành bằng chứng quan trọng trong trường hợp phát sinh tranh chấp (VD: hợp đồng)	10 năm
■ Sổ nhật ký định khoản, sổ cái tổng thanh toán, sổ thu chi tiền mặt, sổ tài sản cố định, sổ thu, sổ chi, sổ chi phí ■ Tài liệu được tạo liên quan đến bảng kiểm kê, bảng đối chiếu vay và cho vay, bảng tính toán lỗ lãi, quyết toán ■ Phiếu đặt hàng, bản hợp đồng, giấy gửi hàng, biên lai, bản báo giá và những tài liệu liên quan khác (vd: giấy yêu cầu thanh toán)	3 năm
■ Bản kê khai (luân chuyển) khấu trừ phụ thuộc của người nhận lương. ■ Bản kê khai khấu trừ đặc biệt của người vợ/chồng kiêm giấy báo cáo khấu trừ phí bảo hiểm của người nhận lương. ■ Sổ khấu trừ thuế	3 năm
■ Đơn đăng ký không đánh thuế tài sản hình thành tiết kiệm, đơn xin luân chuyển	3 năm
■ Tài liệu liên quan đến người được bảo hiểm bởi bảo hiểm tuyển dụng	3 năm

▪ Danh sách người lao động ▪ Sổ cái tiền lương ▪ Tài liệu quan trọng liên quan đến việc tuyển vào/cho thôi việc/bồi thường tai nạn/tiền lương khác liên quan đến lao động	3 năm
▪ Tài liệu liên quan đến việc thu phí bảo hiểm lao động	
▪ Tài liệu liên quan đến bảo hiểm lao động	
▪ Biên bản họp của ủy ban an toàn ▪ Biên bản họp của ủy ban vệ sinh ▪ Biên bản họp của ủy ban an toàn vệ sinh	
▪ Tài liệu liên quan đến bảo hiểm y tế ▪ Tài liệu liên quan đến bảo hiểm lương hưu phúc lợi xã hội ▪ Tài liệu liên quan đến bảo hiểm tuyển dụng	3 năm
▪ Tài liệu liên quan đến dự án ▪ Tài liệu yêu cầu (Requirement Document) ▪ Tài liệu thiết kế ▪ Task, bug report ▪ Testcase ▪ Meeting note ▪ Biên bản kick-off ▪ Source code dự án ▪ Tài liệu hướng dẫn sử dụng (User Manual)	Bàn giao hoàn toàn cho khách hang sau khi xong dự án
▪ Yêu cầu (request) ▪ Yêu cầu làm việc tại nhà (WFH) ▪ Yêu cầu tạo máy ảo, VPS server, AWS account ▪ Yêu cầu mua mới/sửa chữa thiết bị ▪ Yêu cầu thanh toán liên quan đến tài chính, kế toán ▪ Yêu cầu tuyển dụng nhân sự ▪ Yêu cầu trợ cấp chứng chỉ/bằng cấp ▪ Yêu cầu soạn thảo/sửa đổi/huỷ tài liệu, hồ sơ ▪ Yêu cầu khoá học/đào tạo	3 năm
▪ Đánh giá sau thử việc ▪ Đánh giá phỏng vấn	3 năm
▪ Report về nguyên nhân critical bug và cách khắc phục	3 năm

5.34 Quyền riêng tư và bảo vệ thông tin định danh cá nhân

Thông tin cá nhân sẽ được bảo vệ theo các quy định bảo mật thông tin và pháp luật.

5.35 Xem xét độc lập về an toàn thông tin

Trường hợp phát sinh thay đổi có ảnh hưởng đến ISMS, ví dụ như dưới đây, phải tiến hành xem xét độc lập bằng đánh giá nội bộ. Thêm hoặc thay đổi kinh doanh, thay đổi trên diện rộng về quy trình nghiệp vụ.

a) Thay đổi địa chỉ, thiết lập trụ sở mới

b) Thay đổi người phụ trách chính liên quan đến bảo mật thông tin.

c) Thay đổi lớn trên hợp đồng, hoặc liên quan đến quy chế, pháp lệnh.

5.36 Tuân thủ các chính sách, quy tắc và tiêu chuẩn về an toàn thông tin

a) Để đảm bảo quy trình liên quan đến bảo mật, cũng như việc thực hiện đúng tiêu chuẩn, ban bảo mật thông tin sẽ kiểm tra định kỳ 1 năm 1 lần vào kỳ đánh giá nội bộ hoặc kiểm tra đột xuất.

b) Thành viên ban bảo mật thông tin sẽ yêu cầu bộ phận HC-KT lưu trữ các thông tin ra vào công ty. Định kỳ 1 năm 1 lần sẽ tiến hành kiểm tra việc lưu trữ và công tác quản lý ra vào. Khi có phát sinh sự cố, sẽ xem xét thực tế trên hệ thống.

Ngoài ra, sẽ kiểm tra định kỳ việc quản lý ra vào có đang được thực hiện hợp lý và hiệu quả hay không, và trường hợp phát hiện thiếu sót thì phải nhanh chóng xử lý chỉnh sửa.

5.37 Quy trình vận hành được lập thành văn bản

Người sử dụng phải làm theo các quy trình đã được xây dựng

6. CÁC BIỆN PHÁP KIỂM SOÁT VỀ CON NGƯỜI

6.1 Sàng lọc

Việc thẩm tra lý lịch nhân sự được thể hiện tại Quy trình tuyển dụng.

6.2 Điều khoản và điều kiện làm việc

Khi tuyển dụng nhân viên, cam kết bảo mật thông tin cần được ghi vào hợp đồng, lấy chữ ký vào bản cam kết bảo mật thông tin nếu có yêu cầu thêm.

6.3 Nhận thức, giáo dục và đào tạo về an toàn thông tin

Tất cả nhân viên được đào tạo và huấn luyện để nâng cao ý thức về Chính sách và quy trình an toàn bảo mật thông tin.

6.4 Quy trình xử lý kỷ luật

Được thể hiện tại Quy định về ANTT và xử lý vi phạm

6.5 Trách nhiệm sau khi thôi việc hoặc thay đổi công việc

Được thể hiện trong Quy trình Offboard.

6.6 Thỏa thuận bảo mật hoặc không tiết lộ thông tin

a) Người lao động của công ty sẽ kí cam kết bảo mật thông tin. Ngoài ra, trong cùng thỏa thuận này bao gồm cả những điều khoản yêu cầu phải bảo mật thông tin kể cả sau khi kết thúc hợp đồng gốc.

b) Giữa công ty và bên ủy thác, sẽ ký hợp đồng cam kết bảo mật khi cần thiết.

6.7 Làm việc từ xa

a) Làm việc tại nhà có thể thực hiện chỉ khi đã có sự phê duyệt của trưởng bộ phận và bộ phận ISMS.

b) Máy tính sử dụng cho làm việc tại nhà được xem như là máy tính mượn từ công ty, và không được chia sẻ với gia đình hay người sống cùng.

6.8 Báo cáo sự kiện an toàn thông tin

Được thể hiện trong danh sách thống kê sự cố, sự kiện.

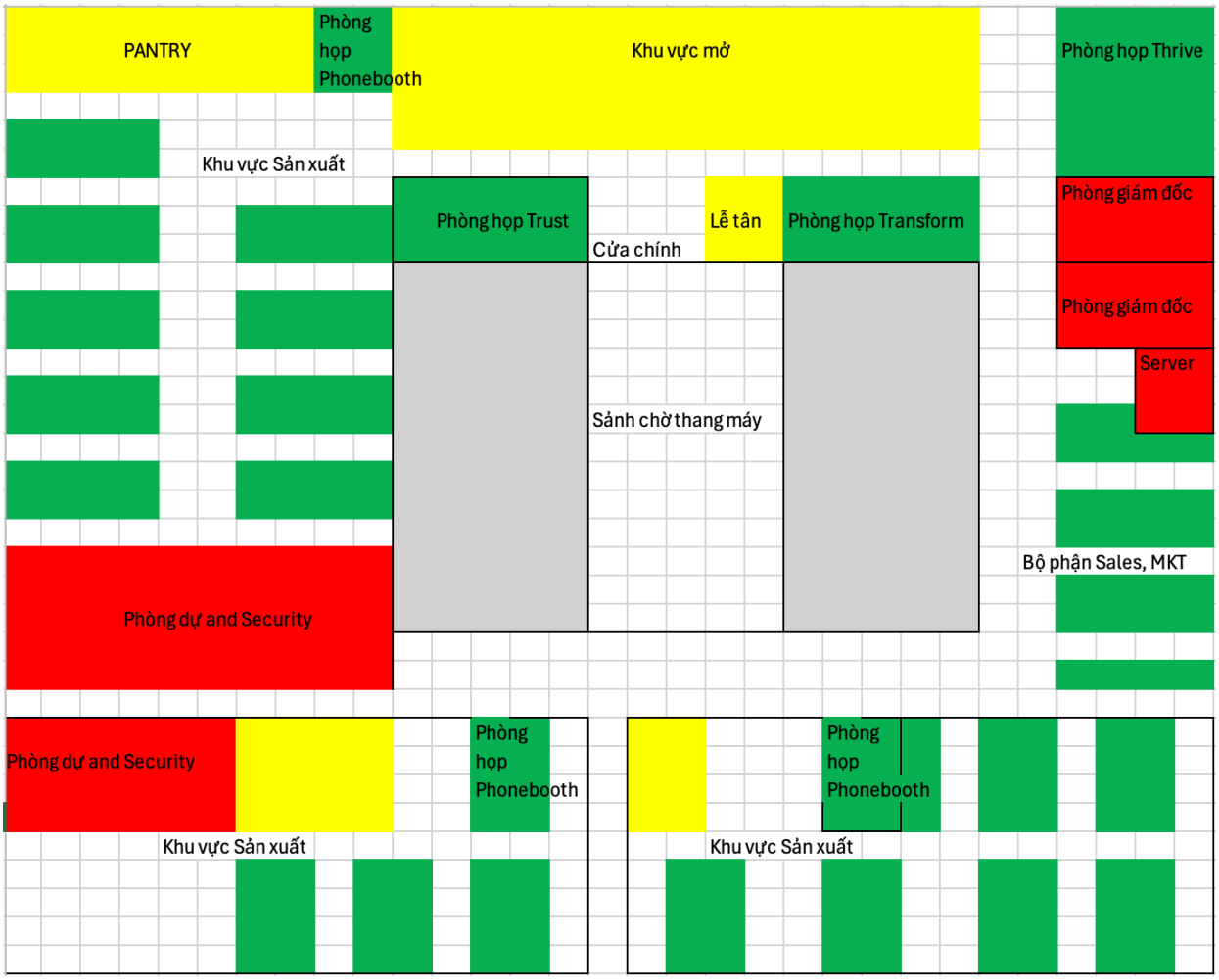
7. CÁC BIỆN PHÁP KIỂM SOÁT VỀ CƠ SỞ VẬT CHẤT

7.1 Các vành đai vật lý

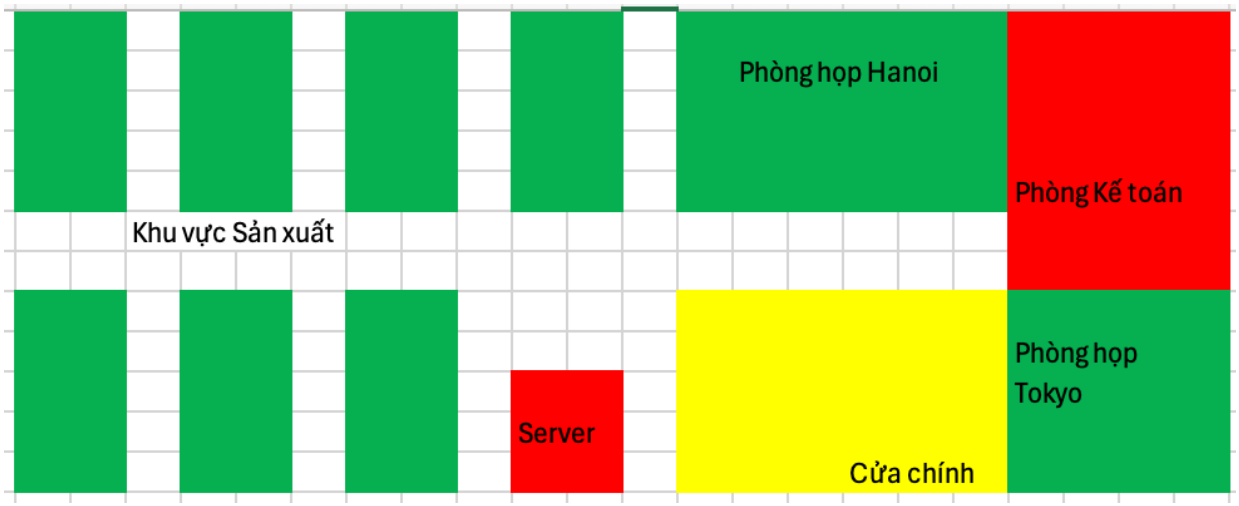
Kiểm soát việc ra vào bằng thẻ từ.

7.2 Cổng ra vào vật lý

Văn phòng HUD tầng 9



Văn phòng HUD tầng 22



Vùng A: Khu vực giới hạn người ra vào

Vùng B: Không gian làm việc mở

Vùng C: Khu vực công cộng

a) Quyền hạn

1) Thiết lập quyền hạn ra vào và cấm người không có quyền.

2) Quyền hạn ra vào sẽ được cấp bằng nhận diện khuôn mặt hoặc vân tay.

3) Tuyệt đối không mở cửa cho người ngoài ra vào công ty, trương trường hợp khách hang của công ty đến thì phải có thẻ khách.

b) Lịch sử ra vào

1) Khi ra vào, bằng thiết bị máy chấm công và camera giám sát, sẽ lưu lại giờ vào của người đầu tiên và giờ ra của người sau cùng.

2) Khi người ngoài đến thăm công ty cần lưu lại lịch sử ra vào, tên, thông tin người bảo lãnh trên Sổ theo dõi Khách và Ứng viên ra vào công ty. Bộ phận HC-KT sẽ cấp thẻ ra vào cho khách.

7.3 Bảo vệ văn phòng, phòng và cơ sở vật chất

a) Khu vực tủ hồ sơ ở khu vực HC-KT là khu vực bảo vệ đặc biệt.

b) Quy định chỉ có 2 đối tượng được phép ra vào khu vực này là: bộ phận HC-KT, BGĐ

7.4 Giám sát an ninh vật lý

a) Công ty thiết lập hệ thống giám sát bằng camera và sổ kiểm soát ra vào

b) Kiểm soát cửa ra vào bằng FaceID với nhân viên, và thẻ từ với khách

7.5 Bảo vệ chống lại các mối đe dọa vật lý và môi trường

a) Bố trí bình cứu hỏa ở khu vực gần thang máy dưới sự quản lý của tòa nhà.

b) Hệ thống báo cháy của toà nhà.

c) Tất cả khu vực của kính ở công ty đều được dán mờ.

7.6 Làm việc trong các khu vực an toàn

Khu vực cần đảm bảo bảo mật của tổ chức là khu vực HC-KT & BGĐ. Có camera giảm sát, tủ hồ sơ được bảo vệ bằng khoá.

7.7 Bàn sạch và màn hình sạch

a) Bàn làm việc gọn gàng

1) Sắp xếp, thu dọn để có thể phân biệt được tài liệu/ dữ liệu thông thường và quan trọng.

2) Khi rời khỏi chỗ ngồi và khi về nhà thì tuyệt đối không để lại tài liệu hoặc thiết bị ghi nhớ có ghi thông tin cá nhân hay thông tin quan trọng ở trên bàn hay các khu vực xung quanh.

b) Màn hình gọn gàng

1) Trường hợp người sử dụng rời khỏi chỗ ngồi thì phải thực hiện khóa PC, laptop. Ngoài ra, khi ra về phải tắt máy.

2) Nghiêm cấm việc dán mật khẩu đăng nhập lên trên bàn.

3) Không để tài liệu cần bảo mật ngoài màn hình desktop.

7.8 Bố trí và bảo vệ thiết bị

a) Công tắc điện tổng được khoá cẩn thận

b) Modem tổng được đặt trọng phòng server

c) Các cửa kính đều có rèm cửa hoặc dán mờ để tránh quan sát thông tin quan trọng từ bên ngoài

7.9 An toàn tài sản bên ngoài trụ sở

Các thiết bị đã được bàn giao thì người được cấp phát sẽ có trách nhiệm bảo quản và quản lý thiết bị như trong thoả thuận bảo mật thông tin

7.10 Phương tiện lưu trữ

Các dữ liệu thông tin quan trọng đều được lưu trữ trên cloud, không lưu trữ trên local.

7.11 Các tiện ích hỗ trợ

Có 2 đường mạng (Viettel và VNPT) để backup.

Toà nhà có máy phát điện. Công ty có UPS

7.12 An toàn dây cáp

a) Đường dây mạng tổng được đấu trên trần nhà

7.13 Bảo trì thiết bị

Kế hoạch bảo trì, bảo dưỡng thiết bị hàng năm.

7.14 Xử lý hoặc tái sử dụng thiết bị an toàn

a) Trường hợp cần xử lý laptop/PC, nhân viên sẽ không tự xử lý mà cần thông báo bộ phận IT để tiến hành xử lý theo quy trình của công ty.

b) Trong trường hợp tái sử dụng thiết bị, bộ phận IT sẽ thực hiện xóa trắng dữ liệu trước khi cấp phát.

8. CÁC BIỆN PHÁP KIỂM SOÁT VỀ KỸ THUẬT

8.1 Thiết bị đầu cuối của người dùng

Các thiết bị truy cập vào hệ thống mạng của công ty phải được đăng ký trong danh sách thiết bị đăng ký.

Các thiết bị do nhân viên mang đến công ty không được phép lưu trữ các dữ liệu của công ty, không được truy cập vào mạng của công ty khi chưa được phê duyệt bởi trưởng bộ phận và bộ phận ISMS.

Các máy tính đã đăng ký phải đảm bảo chỉ cài đặt các phần mềm trong danh sách các phần mềm được phép cài đặt.

Các máy tính đều phải bật window defender, firewall

8.2 Quyền truy cập đặc quyền

Các tài khoản đặc quyền được mô tả trong **QT cấp quyền huỷ quyền truy cập**

8.3 Hạn chế truy cập thông tin

Được thể hiện trong biểu mẫu phân quyền

Hệ thống lưu trữ Azure, AWS có phân quyền truy cập, tạo, sửa, xoá dữ liệu theo phân quyền và có lưu log các hoạt động thao tác trên dữ liệu.

8.4 Truy cập mã nguồn

Nhân viên được truy cập các mã nguồn liên quan theo phân quyền của mình trên máy tính công ty cấp.

8.5 Xác thực an toàn

1. Sử dụng mật khẩu để truy cập tài khoản
2. Sử dụng thông tin chứng thực 2 lớp cho account AWS, Office 365 phương thức xác thực là Multi-Factor Authentication (MFA)

8.6 Quản lý năng lực

Cơ sở vật chất có: camera, mạng, máy chấm công

8.7 Bảo vệ chống lại phần mềm độc hại

1. Tất cả các máy tính kết nối với mạng cần bật phần mềm diệt virus window defender, firewall.

2. Hạn chế cài đặt phần mềm, các máy tính nhân viên chỉ được phép cài đặt các phần mềm trong danh sách các phần mềm được phép cài đặt.

3. Đối với email có mục tiêu lừa đảo:

a. Hệ thống đã hạn chế mail bên ngoài công ty gửi đến hòm mail mà công ty

cung cấp (vd gmail, hotmail…)

b. Khi nhận mail không rõ nguồn gốc, không tự ý phán đoán, mở mail mà phải nhanh chóng liên lạc với ban bảo mật thông tin.

c. Thiết lập cho hiển thị đuôi file, trường hợp đuôi file đính kèm không thuộc loại được sử dụng thông thường thì không mở file. (Ví dụ về đuôi file không được sử dụng thông thường *.exe, pif, scr).

8.8 Quản lý các lỗ hổng kỹ thuật

a) Thực hiện quét lỗ hổng cho hệ thống trên thiết bị Fortinet định kỳ 1 tháng/lần

b) Nếu có lỗ hổng nghiêm trọng, team dự án sẽ tiến hành xử lý và update bản vá

c) Các lỗ hổng nhỏ, không nghiêm trọng có thể không cần xử lý

8.9 Quản lý cấu hình

a) Phần cứng: quy chuẩn thiết bị tại công ty

b) Phần mềm: đảm bảo cài đặt version tối thiểu trong danh sách phần mềm được phép cài đặt

8.10 Xóa thông tin

a) Xoá tài liệu điện tử: dùng tổ hợp phím Shift+Del để xoá

b) Xoá tài liệu bản cứng: cho vào máy huỷ tài liệu trước khi bỏ vào thùng rác

c) Xoá ổ cứng: thiết bị sẽ bị xáo trắng toàn bộ dữ liệu, hệ điều hành khi nghỉ hoặc bàn giao cho người sử dụng mới

8.11 Che dấu dữ liệu

Các tài liệu quan trọng của bộ phận HC-KT sẽ lưu trữ trên HC-KT và account HC-KT này sẽ do bộ phận HC-KT quản lý.

Nếu có các dữ liệu ở mức đặc biệt cao trong quá trình chia sẻ dữ liệu sẽ áp dụng che dấu dữ liệu bằng cách bôi đen thông tin.

8.12 Ngăn chặn rò rỉ dữ liệu

a) Dạng điện tử: Account được set quyền truy cập dữ liệu theo cấu trúc phân quyền

b) Dạng bản cứng: Tài liệu hồ sơ quan trọng được đựng trong tủ hồ sơ có khoá

c) Trường hợp gửi thông tin quan trọng ra bên ngoài, cần sử dụng dịch vụ giao hàng hoặc dịch vụ bưu điện có lưu lại lịch sử chuyển phát.

8.13 Sao lưu thông tin

a) Theo quy trình backup và phục hồi dữ liệu của công ty

b) Source code sao lưu tự động trên Gitlab của công ty

8.14 Dự phòng các phương tiện xử lý thông tin

a) Trang bị PC, laptop dự phòng

b) Hệ thống điện: máy phát điện toà nhà, UPS của công ty

c) Hệ thống mạng dự phòng: 2 đường mạng khác nhau (1 line VNPT, 1 line Viettel)

8.15 Ghi nhật ký

Lưu trữ log thao tác trên dữ liệu hệ thống Azure cloud

8.16 Các hoạt động giám sát

a) Camera giám sát 24/7 ở khu vực cửa ra vào và khu vực sản xuất

b) Cửa ra vào được khoá bằng nhận diện khuôn mặt

8.17 Đồng bộ thời gian

Đồng bộ thời gian của toàn bộ các thiết bị trong công ty theo đúng múi giờ UTC +7

8.18 Sử dụng các chương trình tiện ích đặc quyền

Máy tính của kế toán được phép cài đặt và sử dụng các phần mềm liên quan tới xuất hoá đơn, xuất chứng từ thuế và kế toán.

Bộ phận HC-KT, tuyển dụng, Sales được phép dùng mạng xã hội cho các mục đích tuyển dụng, quảng bá công ty

8.19 Cài đặt phần mềm trên các hệ điều hành

a) Phần mềm sử dụng tại máy tính, về nguyên tắc chỉ chấp nhận trong danh sách phần mềm được phép cài đặt. Trường hợp sử dụng phần mềm khác thì sẽ phải được sự cho phép của ban ISO.

b) Nghiêm cấm cài đặt và sử dụng các phần mềm trong danh sách phần mềm không được phép cài đặt

c) Định kỳ 3 tháng 1 lần ban ISO sẽ kiểm tra, rà soát ngẫu nhiên danh sách phần mềm cài đặt của các bộ phận.

8.20 An toàn mạng

a) Sử dụng mạng trong công ty

1) Đối với thiết bị của khách sử dụng mạng wifi Guest

2) Máy tính đã ngắt kết nối tạm thời khỏi mạng trong công ty, sau khi xác nhận an toàn như kiểm tra virus, thì mới kết nối lại.

3) Các đường mạng đều được đặt mật khẩu và thể hiện trong biểu mẫu phân quyền.

b) Sử dụng Internet

1) Các bộ phận và cá nhân trong công ty đều được quyền sử dụng các dịch vụ mạng hiện có của công ty và có trách nhiệm bảo đảm an toàn, an ninh cho hệ thống thiết bị và thông tin trên mạng.

2) Trong thời gian làm việc tại công ty, nhân viên không được chơi game, xem phim, sử dụng các dịch vụ mạng xã hội: facebook, tiktok, instagram…, truy cập

các trang web độc hại.

3) Định kỳ kiểm tra sự kết nối hệ thống xem có ổn định hay không, thời gian hoạt động yêu cầu >=99%

8.21 An toàn các dịch vụ mạng

Trường hợp sử dụng dịch vụ mạng bên ngoài, người quản lý hệ thống thông tin phải đánh giá, chỉ định mức độ an toàn của dịch vụ, các hạng mục bảo mật với công ty đó và thay đổi hợp đồng khi cần thiết.

8.22 Phân tách mạng

Đối với hệ thống mạng được phân tách theo từng khu vực cụ thể, thể hiện trong biểu mẫu phân quyền.

8.23 Lọc Web

Chặn quyền truy cập các trang web độc hại đã biết trên thiết bị Firewall.

8.24 Sử dụng mật mã

a) Nhập mật khẩu phải là tương tác

b) Nghiêm cấm việc ghi nhớ mật khẩu vào hệ thống.

c) Người sử dụng phải tuân thủ chính sách đặt mật khẩu như sau:

1.Không chứa tên account của người dùng, hoặc 1 phần tên đầy đủ (họ, tên đệm hoặc tên) có độ dài hơn 2 ký tự.

2.Chứa ít nhất 8 ký tự

3.Chứa các ký tự thuộc tối thiểu 3 nhóm trong danh sách 4 nhóm sau:

- Ký tự tiếng Anh viết hoa (A-Z)
- Ký tự tiếng Anh viết thường (a-z)
- Ký tự số (0-9)
- Ký tự đặc biệt (ví dụ: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | ¥ " ; ' <> ? , . /)

4.Không trùng lặp với 1 trong 5 mật khẩu gần nhất

5.Các lần đổi mật khẩu cách nhau tối thiểu 3 ngày. Trường hợp đặc biệt cần liên hệ tới ban ISO để được hỗ trợ.

d) Người sử dụng phải thay đổi mật khẩu trong vòng 90 ngày có thể đổi được từ ngày 85 và khi cần thiết.

e) Mật khẩu của tài khoản quản trị hệ thống thì phải được quản lý nghiêm ngặt bởi người chịu trách nhiệm quản lý.

8.25 Vòng đời phát triển an toàn

a) Môi trường phát triển sẽ phân tách khỏi môi trường vận hành.

b) Để phòng tránh việc bị giả mạo hoặc vô tình xóa bỏ, cố ý xóa bỏ thì việc lưu trữ source code sẽ sử dụng gitlab của công ty.

Việc truy cập vào môi trường phát triển trên server sẽ được lưu trữ log

8.26 Yêu cầu an toàn ứng dụng

Nghiêm cấm sử dụng các mạng xã hội để gửi thông tin có mức độ quan trọng cao và đặc biệt cao ra ngoài.

Chỉ được phép cài đặt các phần mềm trong danh sách phần mềm được phép cài đặt. Trường hợp sử dụng phần mềm khác nằm ngoài danh sách thì sẽ phải thông báo và được sự cho phép của ban ISO.

8.27 Kiến trúc hệ thống an toàn và các nguyên tắc kỹ thuật

8.28 Mã hóa an toàn

Chính sách sử dụng kiểm soát mã hóa

Kiểm soát mã hóa

SSL

- Thông tin nhận từ form đầu vào của trang chủ công ty sẽ được mã hóa dựa vào SSL.
- Các service kết nối từ local ra ngoài internet đều đảm bảo được mã hóa.

LAN KHÔNG DÂY

- Việc truyền thông tin qua LAN không dây sẽ được mã hóa, bằng phương pháp wpa-2 và phương pháp xác thực tài khoản/mật khẩu

Quản lý khóa:

SSL

- Người quản lý hệ thống thông tin sẽ quản lý thời hạn hiệu lực của khóa mật mã, và gia hạn trước khi hết hạn.

LAN KHÔNG DÂY

- Chỉ người quản lý hệ thống thông tin mới có thể truy cập vào giao diện quản trị (admin) của điểm truy cập, và phải quản lý nghiêm ngặt mật khẩu đó.

8.29 Kiểm tra bảo mật trong quá trình phát triển

Tích hợp bảo mật vào quy trình phát triển phần mềm (Shift-Left Security):

- Đảm bảo các kiểm tra bảo mật được thực hiện từ giai đoạn thiết kế, lập trình và kiểm thử.

Thực hiện các hình thức kiểm thử bảo mật chính:

- Static Application Security Testing (SAST): Quét mã nguồn để phát hiện lỗi bảo mật ngay khi lập trình.
- Dynamic Application Security Testing (DAST): Kiểm thử bảo mật trong môi trường chạy thực tế.

- Interactive Application Security Testing (IAST): Kết hợp cả SAST và DAST để phát hiện lỗ hổng trong lúc ứng dụng hoạt động.

Thực hiện mô hình Threat Modeling:

- Phân tích, dự đoán và loại bỏ các mối đe dọa tiềm ẩn từ khi thiết kế sản phẩm.

8.30 Phát triển thuê ngoài

- **Không áp dụng**

8.31 Phân tách môi trường phát triển, kiểm thử và sản xuất

- Môi trường phát triển của đội phát triển
- Môi trường UAT
- Môi trường Production

8.32 Quản lý thay đổi

Được thể hiện trong **QT quản lý sự thay đổi.**

8.33 Thông tin kiểm thử

Quy định lưu trữ và xử lý thông tin kiểm thử bảo mật:

- Tất cả thông tin thu được từ quá trình kiểm thử (log, kết quả quét, báo cáo lỗi) cần được lưu trữ an toàn và phân loại theo mức độ nhạy cảm.

Mã hóa thông tin kiểm thử:

- Sử dụng cơ chế mã hóa để bảo vệ dữ liệu kiểm thử, đặc biệt là các lỗi bảo mật nghiêm trọng.

Bảo vệ môi trường kiểm thử:

- Đảm bảo môi trường kiểm thử tách biệt với môi trường sản xuất, nhằm hạn chế rủi ro rò rỉ dữ liệu hoặc khai thác lỗ hổng.

8.34 Bảo vệ hệ thống thông tin trong quá trình kiểm tra đánh giá

Phân tích và tổng hợp kết quả kiểm thử:

- Sau mỗi đợt kiểm thử bảo mật, cần có báo cáo tổng hợp kết quả, nêu rõ các lỗ hổng, mức độ ảnh hưởng và phương án khắc phục.

Thực hiện Post-Mortem:

- Đối với các lỗi nghiêm trọng hoặc lỗi tái diễn nhiều lần, cần tổ chức buổi phân tích nguyên nhân (RCA - Root Cause Analysis) và rút ra bài học kinh nghiệm.

Theo dõi và cải thiện liên tục:

- Xây dựng quy trình theo dõi tình trạng khắc phục các lỗ hổng đã phát hiện. Đảm bảo các vấn đề bảo mật được xử lý triệt để trước khi sản phẩm được triển khai..

SỔ TAY BẢO MẬT THÔNG TIN