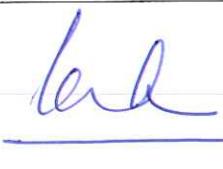


 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: <u>20/09/2024</u>

CHÍNH SÁCH AN TOÀN BẢO MẬT THÔNG TIN

TRÁCH NHIỆM	BIÊN SOẠN	XEM XÉT	XEM XÉT	PHÊ DUYỆT
CHỮ KÝ		<u>lkd</u>	 <u>Le N. Hoang Minh</u>	 <u>Pham Van Dat</u>
HỌ TÊN	NGUYỄN ĐỨC DOANH	LÊ N. HOÀNG MINH	DƯƠNG HỒNG CẨM	NGUYỄN VĂN ĐẠT
CHỨC VỤ	TBP HẠ TẦNG VÀ BẢO MẬT	GĐ BAN CNTT	TỔNG GIÁM ĐỐC	CHỦ TỊCH
	Ngày <u>23/09/2024</u>	Ngày <u>28/09/2024</u>	Ngày <u>30/09/2024</u>	Ngày <u>26/09/2024</u>

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: <u>26/09/2024</u>

LỊCH SỬ SOÁT XÉT

Lần ban hành	Hạng mục thay đổi	Mô tả chi tiết nội dung chính đã thay đổi		Ngày hiệu lực
		Nội dung cũ	Nội dung mới	
01	Ban hành mới			<u>26/09/2024</u>

MỤC LỤC

LỊCH SỬ SOÁT XÉT	2
I. MỤC ĐÍCH	5
II. PHẠM VI ÁP DỤNG	5
III. TÀI LIỆU THAM KHẢO	5
IV. ĐỊNH NGHĨA VÀ CHỮ VIẾT TẮT	5
V. NỘI DUNG	8
V.1 Các thành phần liên quan đến Chính sách ATBMTT	8
V.2 Trách nhiệm	8
V.2.1 Trách nhiệm của Ban điều hành	8
V.2.2 Trách nhiệm của Ban CNTT	8
V.2.3 Trách nhiệm của các Ban trong PDH và các Phòng CNTT trong CTTV	8
V.2.4 Những trường hợp ngoại lệ	9
V.2.5 Xử lý vi phạm	9
V.3 Mục tiêu của chính sách ATBMTT	9
V.4 Định hướng công tác ATBMTT	9
V.4.1 Các chính sách ATBMTT	9
V.4.2 Công tác rà soát chính sách ATBMTT	9
V.5 Tổ chức cho công tác ATBMTT	10
V.5.1 Yêu cầu đối với các đơn vị trong PDH & CTTV	10
V.5.2 Yêu cầu đối với thiết bị di dời được và làm việc từ xa	11
V.6 ATBMTT trong quản lý nguồn nhân lực	12
V.7 Quản lý tài sản thông tin	13
V.8 Kiểm soát truy cập hệ thống CNTT	15
V.8.1 Yêu cầu trong quản lý truy cập	15
V.8.2 Quản lý truy cập người sử dụng	16
V.8.3 Trách nhiệm của người sử dụng trong quản lý mật khẩu	17

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS CHÍNH SÁCH AN TOÀN BẢO MẬT THÔNG TIN	Mã số: PDH-CNTT-CS01 Lần ban hành: 01 Ngày hiệu lực: <u>26/07/2024</u>
--	--	--

V.8.4	Kiểm soát truy cập hệ thống và ứng dụng	17
V.9	Mã hóa	18
V.9.1	Quy định về sử dụng các thuật toán mã hóa	18
V.9.2	Quản lý khóa mã hóa	18
V.10	An ninh vật lý và môi trường cho TTDL/PMC	18
V.10.1	Khu vực an ninh.....	18
V.10.2	Trang thiết bị	20
V.11	An ninh trong vận hành hệ thống công nghệ thông tin.....	21
V.11.1	Trách nhiệm và quy trình vận hành	21
V.11.2	Phòng chống mã độc tấn công	22
V.11.3	Sao lưu dự phòng	23
V.11.4	Giám sát và ghi nhật ký	23
V.11.5	Kiểm soát vận hành phần mềm	24
V.11.6	Quản lý lỗ hổng kỹ thuật	24
V.11.7	Kiểm toán hệ thống thông tin	25
V.12	An ninh mạng và truyền thông	25
V.12.1	Quản lý an ninh mạng	25
V.12.2	Truyền thông	25
V.13	An ninh khi sử dụng các dịch vụ đám mây	26
V.14	Mua sắm, phát triển và bảo trì hệ thống CNTT	27
V.14.2	An ninh trong phát triển và hỗ trợ hệ thống CNTT	27
V.14.3	Dữ liệu kiểm thử	29
V.15	Quản lý mối quan hệ nhà cung cấp	29
V.15.1	ATBMTT trong quản lý mối quan hệ nhà cung cấp	29
V.15.2	Quản lý chuyển giao dịch vụ với nhà cung cấp	30
V.16	Quản lý sự cố ATBMTT	30
V.16.1	Quy trình và trách nhiệm	30
V.16.2	Thông báo các sự kiện về ATBMTT	30
V.16.3	Báo cáo điểm yếu ATBMTT	31
V.16.4	Đánh giá và ra quyết định các sự kiện ATBMTT	31
V.16.5	Phản ứng lại các sự cố ATBMTT	31
V.16.6	Rút kinh nghiệm từ các sự cố ATBMTT đã xảy ra	31
V.16.7	Thu thập bằng chứng	32
V.17	ATBMTT trong quản lý hoạt động liên tục của hệ thống CNTT	32
V.17.1	ATBMTT liên tục	32

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 20/09/2024

V.17.2	Dự phòng	32
V.18	Tuân thủ	32
V.18.1	Tuân thủ các yêu cầu của pháp luật và các hợp đồng đã ký	32
V.18.2	Rà soát công tác ATBMTT.....	33

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS CHÍNH SÁCH AN TOÀN BẢO MẬT THÔNG TIN	Mã số: PDH-CNTT-CS01 Lần ban hành: 01 Ngày hiệu lực: 26/01/2024
--	--	---

I. MỤC ĐÍCH

- Mô tả và liệt kê chi tiết các yêu cầu đối với An toàn bảo mật thông tin (ATBMTT) tại Công ty Phát Đạt Holdings và Công ty Thành viên (PDH & CTTV).
- Áp dụng Chính sách ATMBTT vào các hoạt động hàng ngày tại PDH & CTTV.

II. PHẠM VI ÁP DỤNG

- Áp dụng cho các trường hợp lưu trữ, truy cập, truyền tải, hủy bỏ thông tin từ các trung tâm dữ liệu/ phòng máy chủ hay dịch vụ điện toán đám mây của PDH & CTTV. Vì vậy, chính sách này cũng được áp dụng để kiểm soát đối với tất cả cán bộ nhân viên chính thức, nhân viên thử việc, nhân viên thực tập, cố vấn, đối tác và khách hàng của PDH & CTTV có truy cập đến thông tin nói trên của PDH & CTTV từ bất kỳ địa điểm và thời gian nào. Ngoài ra, các phần mềm ứng dụng, các hệ thống thông tin, các thiết bị công nghệ thông tin có kết nối đến các trung tâm dữ liệu/ phòng máy chủ hay dịch vụ điện toán đám mây của PDH & CTTV cũng thuộc phạm vi kiểm soát của chính sách này.
- Chính sách này không áp dụng đến giá trị tài chính kế toán của các thiết bị chứa thông tin được nêu trong chính sách này.

III. TÀI LIỆU THAM KHẢO

- Tài liệu này có sử dụng các thuật ngữ và định nghĩa của ISO/IEC 27000.
- Tài liệu này có tham khảo một số thông tin từ các nguồn và tổ chức khác để xây dựng phù hợp với hoạt động thực tế của PDH & CTTV.

IV. ĐỊNH NGHĨA VÀ CHỮ VIẾT TẮT

Định nghĩa/ Viết tắt	Giải thích
Công ty/PDH	Công ty TNHH Phát Đạt Holdings
PDH & CTTV	Công ty Phát Đạt Holdings và Công ty Thành viên
Ban điều hành	Tổng Giám đốc, các Phó Tổng Giám đốc, Giám đốc các Ban thuộc PDH và Tổng Giám đốc CTTV.
Tài sản thông tin	Tài sản thông tin (trong tài liệu này có thể gọi vẫn tắt là “tài sản”) là bao gồm thông tin, thiết bị hoặc hệ thống thiết bị liên quan đến thông tin đó, có giá trị với Công ty bao gồm: Tài sản vô hình: <ul style="list-style-type: none">Tài sản thông tin (cơ sở dữ liệu, tập tin dữ liệu, tài liệu điện tử).Tài sản phần mềm (phần mềm ứng dụng, phần mềm hệ thống, công cụ phát triển và các ứng dụng tiện ích). Tài sản hữu hình: <ul style="list-style-type: none">Tài liệu chứng từ giấyThiết bị máy tính, thiết bị truyền thông, thiết bị lưu trữ,...Thiết bị kỹ thuật khác (nguồn điện, bộ lưu điện, ...)

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/01/2024

Định nghĩa/ Viết tắt	Giải thích
CNTT	Công nghệ thông tin
Ban CNTT	Ban CNTT - PDH
BP HT&BM	Bộ phận hạ tầng và bảo mật thuộc Ban CNTT
ATBMTT	An toàn Bảo mật Thông tin
TTDL/PMC	Bao gồm các trung tâm dữ liệu/ phòng máy chủ hay dịch vụ điện toán đám mây của PDH
Đơn vị	Các Ban (PDH), Công ty thành viên
Trưởng đơn vị	Giám đốc/ Phó giám đốc các Ban, Tổng giám đốc/ Phó Tổng giám đốc Công ty thành viên
Người dùng cuối	Là cán bộ nhân viên của PDH & CTTV có sử dụng dịch vụ CNTT nhằm phục vụ mục đích công việc.
An toàn Bảo mật Thông tin	<p>An toàn bảo mật thông tin là việc bảo vệ thông tin và hệ thống thông tin tránh khỏi những hành vi vi phạm tính bảo mật, tính toàn vẹn và sẵn sàng của thông tin, bao gồm việc truy cập, sử dụng, tiết lộ, chỉnh sửa và tiêu hủy thông tin trái phép.</p> <p>Công tác An toàn Bảo mật Thông tin là nhằm đảm bảo các đặc tính sau của thông tin:</p> <ul style="list-style-type: none"> • Tính bảo mật: là đảm bảo không tiết lộ hoặc công bố thông tin cho các đối tượng (cá nhân, tổ chức hay quy trình) không được phép. • Tính toàn vẹn: là đảm bảo thông tin phải chính xác và đầy đủ. • Tính sẵn sàng: là đảm bảo thông tin có thể truy cập và sử dụng được bất kỳ khi nào cần đến.
Chính sách ATBMTT	Là một loại tài liệu quản lý cấp cao mà đối tượng được áp dụng phải tuân thủ theo hoặc không được vi phạm. Chính sách là một loại văn bản không mang tính kỹ thuật. Mục đích và mục tiêu của chính sách được trình bày theo kiểu tổng quát và nội dung của chính sách sẽ đề cập đến việc làm thế nào để đạt được các mục tiêu và mục đích của chính sách.
Hệ thống quản lý ATBMTT	Là một bộ tài liệu quản lý (như chính sách, quy trình, hướng dẫn, biểu mẫu...) được thực hiện nhằm để đảm bảo hệ thống CNTT của PDH được an toàn bảo mật một cách phù hợp với mục tiêu kinh doanh.
Đơn vị chịu trách nhiệm về ATBMTT	Là đơn vị được Ban điều hành giao nhiệm vụ chịu trách nhiệm phụ trách các hoạt động ATBMTT trong Công ty và cho Công ty Thành viên.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/03/2024

Định nghĩa/ Viết tắt	Giải thích
Hệ thống thông tin	Hệ thống thông tin là tập hợp bao gồm một vài hoặc tất cả các đối tượng như phần cứng, phần mềm, thiết bị, dữ liệu, thông tin, cơ sở dữ liệu, v.v. nhằm lưu trữ, xử lý và cung cấp thông tin phục vụ cho một mục đích nào đó.
Chủ sở hữu tài sản thông tin	Đơn vị hoặc cá nhân chịu trách nhiệm về tài sản thông tin, có thẩm quyền quyết định phân quyền truy cập/ sử dụng tài sản thông tin.
ISO 27001	Là tiêu chuẩn quốc tế về An toàn bảo mật thông tin.
Thông tin	<p>Thông tin là những dữ liệu có giá trị được PDH & CTTV sử dụng cho mục đích kinh doanh của mình.</p> <p>Thông tin được tồn tại ở nhiều hình thức khác nhau: giấy, trang web, tập tin máy tính, các bản fax, báo cáo, quyết định, email, video, pano áp-phích, v.v.</p> <p>Thông tin là một loại hình tài sản cần được bảo vệ của PDH & CTTV.</p>
Quản lý tài sản	Là quá trình duy trì thông tin về tài sản của Công ty và Công ty Thành viên một cách đầy đủ và chính xác. Các thông tin cần được quản lý bao gồm các thông tin cơ bản về tài sản, kho quản lý tài sản, xác nhận của người sở hữu tài sản, các thông tin lưu vết kiểm toán về các thay đổi liên quan đến tài sản, hoặc quy trình duy trì thông tin về tài sản.
Tài khoản đặc quyền	Là các tài khoản quản trị cao nhất trong mỗi hệ thống CNTT dùng để thực hiện các công việc quan trọng (ví dụ như: root, administrator, sys, system, sa...)
Tiện ích đặc quyền	Là các phần mềm hoặc công cụ tiện ích dùng để thực hiện các công việc quan trọng lên hệ thống CNTT (ví dụ như: Tool for Oracle Application Developers – TOAD, Putty,...)
Thông tin nhạy cảm hoặc Dữ liệu nhạy cảm	Là các thông tin được xếp vào loại hạn chế đối tượng truy cập.
Thông tin nội bộ	Là các thông tin chỉ phổ biến trong nội bộ PDH & CTTV.
Môi trường production	Là môi trường chính thức đang vận hành phục vụ công việc của hệ thống CNTT PDH & CTTV.
User acceptance testing (UAT)	Là công việc thực hiện kiểm thử của người sử dụng nhằm đào tạo hệ thống CNTT sắp triển khai đáp ứng các yêu cầu trước khi đưa vào vận hành chính thức trong môi trường production.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS CHÍNH SÁCH AN TOÀN BẢO MẬT THÔNG TIN	Mã số: PDH-CNTT-CS01 Lần ban hành: 01 Ngày hiệu lực: 26/05/2024
---	--	---

V. NỘI DUNG

V.1 Các thành phần liên quan đến Chính sách ATBMTT

	Thành phần liên quan	Yêu cầu về ATBMTT
Bên ngoài	Cơ quan nhà nước	Tuân thủ an toàn thông tin mạng
	Khách hàng	Tuân thủ các cam kết, thỏa thuận đã ký
	Nhà cung cấp, đối tác	Tuân thủ các hợp đồng, thỏa thuận đã ký
Bên trong	Người dùng cuối (cán bộ nhân viên và tất cả các đối tượng có truy cập đến các trung tâm dữ liệu/ phòng máy chủ hay dịch vụ điện toán đám mây của PDH & CTTV)	Nhận thức về ATBMTT
	Các Trưởng đơn vị phòng/ban	Dịch vụ công nghệ thông tin hỗ trợ tốt cho hoạt động kinh doanh
	Ban điều hành	Đảm bảo ATBMTT cho dữ liệu và các hệ thống thông tin đặt tại các trung tâm dữ liệu/ phòng máy chủ hay dịch vụ điện toán đám mây của PDH & CTTV

V.2 Trách nhiệm

V.2.1 Trách nhiệm của Ban điều hành

- Đảm bảo chính sách ATBMTT và các mục tiêu an toàn thông tin được thiết lập và tương thích với các định hướng chiến lược của tổ chức.
- Đảm bảo sự tích hợp của các yêu cầu hệ thống quản lý ATBMTT vào các quá trình hoạt động của tổ chức.
- Đảm bảo rằng các nguồn lực cần thiết cho hệ thống quản lý an toàn thông tin được đáp ứng.
- Truyền đạt tầm quan trọng của hiệu lực quản lý ATBMTT và sự tuân thủ với các yêu cầu hệ thống quản lý an toàn thông tin đến PDH & CTTV
- Đảm bảo hệ thống quản lý an toàn thông tin đạt được các kết quả mong muốn.
- Chỉ đạo và hỗ trợ nhân sự ban hành và áp dụng hệ thống quản lý ATBMTT.
- Thúc đẩy cải tiến liên tục chính sách ATBMTT.

V.2.2 Trách nhiệm của Ban CNTT

- Xây dựng, ban hành, phổ biến và giám sát tuân thủ chính sách ATBMTT.
- Phối hợp với Ban nhân sự hành chính tổ chức các chương trình tuyên truyền, đào tạo nhận thức cho PDH & CTTV để nâng cao trách nhiệm của mỗi nhân viên về công tác ATBMTT.

V.2.3 Trách nhiệm của các Ban trong PDH và các Phòng CNTT trong CTTV

- Tuân thủ các quy định của chính sách ATBMTT.
- Phân công nhiệm vụ cho các bộ phận và cá nhân thuộc Ban mình chịu trách nhiệm hoặc phòng CNTT của CTTV các công việc liên quan đến công tác ATBMTT.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/03/2024

- Phòng CNTT của CTTV thực hiện báo cáo định kỳ hàng quý về công tác ATBMTT tại đơn vị mình cho Ban CNTT tổng hợp và nắm tình hình.
- Khi có vấn đề phát sinh liên quan đến công tác ATBMTT nằm ngoài các quy định đã ban hành, đơn vị phải báo cáo ngay về cho Ban điều hành để xin ý kiến chỉ đạo.

V.2.4 Những trường hợp ngoại lệ

- Trong thực tế triển khai, có những trường hợp ngoại lệ nhằm phục vụ nhu cầu công việc dẫn đến không thể tuân thủ được một hoặc một vài nội dung trong chính sách này, các đơn vị phải làm tờ trình gửi Tổng Giám đốc PDH để báo cáo và xin ý kiến chỉ đạo.

V.2.5 Xử lý vi phạm

- Mọi hành vi không tuân thủ những nội dung được quy định trong tài liệu này sẽ bị xử lý theo quy định hiện hành của công ty.

V.3 Mục tiêu của chính sách ATBMTT

- Bảo vệ thông tin của công ty tránh bị truy cập trái phép.
- Bảo vệ thông tin của công ty tránh bị thay đổi trái phép.
- Giảm thời gian gián đoạn hoạt động của các hệ thống thông tin.
- Công ty tuân thủ các cam kết, hợp đồng và thỏa thuận đã ký với khách hàng và đối tác.
- Kế hoạch hoạt động liên tục của hệ thống CNTT được xây dựng và thực hiện diễn tập định kỳ hàng năm.
- Tất cả các đối tượng là quản trị viên các hệ thống CNTT đặt tại các TTDL/PMC của PDH & CTTV được đào tạo nhận thức ATBMTT.

V.4 Định hướng công tác ATBMTT

V.4.1 Các chính sách ATBMTT

- Ban CNTT chịu trách nhiệm ban hành và giám sát tuân thủ các chính sách ATBMTT.
- Chính sách ATBMTT bao gồm các quy định nhằm để bảo vệ tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin.
- Các đơn vị có thể xây dựng bổ sung thêm các chính sách, quy định, quy trình, hướng dẫn nhằm phục vụ công việc trong đơn vị mình. Tuy nhiên, các tài liệu bổ sung phải phù hợp chứ không được xung đột với chính sách này.
- Các đơn vị phải cung cấp cho Ban CNTT bản sao của các chính sách, quy định, quy trình, hướng dẫn về ATBMTT do đơn vị mình xây dựng (nếu có).

V.4.2 Công tác rà soát chính sách ATBMTT

- Ban CNTT tối thiểu mỗi năm một lần hoặc đột xuất (theo chỉ đạo của Tổng Giám đốc PDH) thực hiện rà soát các chính sách, quy định, quy trình, hướng dẫn về ATBMTT đảm bảo các tài liệu này phù hợp và hiệu quả với thực tiễn PHD & CTTV. Công tác rà soát lại phải xem xét các yếu tố:
 - o Phản hồi từ các bên liên quan.
 - o Việc thay đổi các quy định pháp luật, các chính sách có tác động đến công tác quản lý ATBMTT.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/03/2024

- Các trường hợp triển khai mới hoặc thay đổi đáng kể hệ thống CNTT tại PHD & CTTV, lưu ý cả trường hợp chưa triển khai nhưng đã có kế hoạch thực hiện.
- Các báo cáo kiểm toán CNTT có ghi nhận lỗ hổng bảo mật nguy hiểm.
- Các sự cố ATBMTT được ghi nhận.
- Báo cáo của các tổ chức bên ngoài về xu hướng mới nổi trong lĩnh vực ATBMTT.
- Các đơn vị trong công ty tối thiểu mỗi năm một lần phải thực hiện rà soát các chính sách, quy định, quy trình, hướng dẫn về ATBMTT do đơn vị mình xây dựng (nếu có), và cung cấp cho Ban CNTT các phiên bản cập nhật.

V.5 Tổ chức cho công tác ATBMTT

V.5.1 Yêu cầu đối với các đơn vị trong PDH & CTTV

V.5.1.1 Trách nhiệm trong công tác ATBMTT

a) Trách nhiệm của BPHT&BM PDH

- Phổ biến các chính sách ATBMTT đến toàn thể cán bộ nhân viên PDH & CTTV.
- Thực hiện đào tạo nhận thức ATBMTT cho tất cả cán bộ nhân viên PDH & CTTV.
- Giám sát, theo dõi việc tuân thủ chính sách ATBMTT trên toàn PDH & CTTV.
- Đầu mối tiếp nhận thông báo về các vấn đề liên quan đến mất ATBMTT.
- Cung cấp các thông tin cập nhật hoặc cảnh báo về các vấn đề liên quan đến ATBMTT.
- Đưa ra ý kiến về ATBMTT trong việc phát triển hoặc cải tiến các hệ thống thông tin.
- Hỗ trợ, giải thích các chính sách ATBMTT cho các đơn vị trong PDH & CTTV.
- Rà soát các chính sách đảm bảo hiệu quả và phù hợp tình hình thực tế tại công ty.
- Thiết lập và triển khai các giải pháp, công cụ để kiểm soát ATBMTT.

b) Trách nhiệm của Trưởng BPHT&BM PDH

- Kiểm soát chính sách ATBMTT.
- Xây dựng các giải pháp để kiểm soát ATBMTT.

c) Trách nhiệm của Giám đốc Ban CNTT

- Tham mưu cho Chủ tịch Hội đồng Quản trị PDH và Tổng Giám đốc PDH về các chính sách ATBMTT.
- Kiểm soát chính sách ATBMTT.
- Đảm bảo các chính sách phù hợp với công nghệ đang sử dụng tại PDH & CTTV.

d) Trách nhiệm của Chủ tịch Hội đồng Quản trị PDH và Tổng Giám đốc PDH

- Xem xét và phê duyệt để ban hành các chính sách ATBMTT, đảm bảo các chính sách phù hợp với chiến lược kinh doanh của PDH & CTTV.
- Hỗ trợ nguồn lực đầy đủ cho công tác triển khai và vận hành hệ thống quản lý ATBMTT.

e) Trách nhiệm của các phòng/bộ phận vận hành hệ thống công nghệ thông tin tại các CTTV

- Tuân thủ các chính sách ATBMTT.
- Phối hợp với Ban CNTT PDH để thiết lập và triển khai các giải pháp, công cụ để kiểm soát ATBMTT tại CTTV.

f) Trách nhiệm của Trưởng đơn vị và chủ sở hữu tài sản thông tin

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/09/2024

- Xây dựng các quy trình, hướng dẫn (nếu có) để xử lý công việc của đơn vị mình đảm bảo tuân thủ quy định của các chính sách ATBMTT.
- Phối hợp rà soát các chính sách đảm bảo hiệu quả và phù hợp tình hình thực tế tại đơn vị mình.
- Xác định yêu cầu về ATBMTT trong giai đoạn lập kế hoạch của bất kỳ dự án/công việc nào liên quan triển khai mới hoặc thay đổi một hệ thống thông tin.
- Xác định các quyền hạn được phép truy cập thông tin và phê duyệt quyền truy cập thông tin cho từng người hoặc từng nhóm người sử dụng.
- Cử cán bộ nhân viên đơn vị mình tham gia đầy đủ các hoạt động đào tạo nhận thức ATBMTT.
- Giám sát tuân thủ ATBMTT của cán bộ nhân viên đơn vị mình.

g) Phân tách nhiệm vụ

- Các trường hợp chồng chéo trách nhiệm phải được tách rời để giảm nguy cơ vô tình hay cố ý sửa đổi hoặc lạm dụng tài sản thông tin của công ty.
- Chủ sở hữu thông tin phải giảm rủi ro bằng cách:
 - Yêu cầu có tài liệu đầy đủ và chính xác cho tất cả hệ thống thông tin.
 - Yêu cầu không cho phép bất kỳ cá nhân có quyền truy cập được tất cả chức năng trong cùng một hệ thống thông tin.
- Ban CNTT phải đảm bảo rằng:
 - Khi tạo các tài khoản đặc quyền cần phải ghi nhận lại thành tài liệu, và phải được phê duyệt bởi Giám đốc Ban CNTT.
 - Nhiệm vụ quản trị ứng dụng, dịch vụ và hệ thống phải được tách biệt.
 - Nhiệm vụ quản trị cơ sở dữ liệu và phát triển ứng dụng phải được tách biệt.
 - Tài khoản truy cập của một người bất kỳ phải được tạo bởi một người khác.
 - Không có cá nhân nào được cấp quyền thực hiện toàn bộ quy trình từ đầu đến cuối.

h) Duy trì liên lạc với các bên liên quan

- Ban CNTT phải đảm bảo luôn có tài liệu ghi nhận danh sách thông tin liên lạc của nhà cung cấp dịch vụ và các tổ chức, cá nhân có chức năng hỗ trợ, ứng cứu khẩn cấp các sự cố về ATBMTT.
- Tối thiểu mỗi năm một lần, danh sách thông tin liên lạc này phải được rà soát và cập nhật.

i) Tham gia thành viên các diễn đàn và các hiệp hội về ATBMTT

- Các chuyên viên ATBMTT phải duy trì tham gia các diễn đàn trao đổi thông tin để cập nhật kiến thức về các thông lệ thực hành tốt nhất, công nghệ mới, các mối đe dọa, lỗ hổng hay các cảnh báo tấn công.

j) ATBMTT trong thực hiện dự án

- ATBMTT phải được đưa vào trong giai đoạn đầu dự án, bắt kể đó là loại dự án nào, nhằm đảm bảo các rủi ro về ATBMTT được nhận diện sớm và giải quyết trong suốt chu kỳ của dự án.

V.5.2 Yêu cầu đối với thiết bị di dời được và làm việc từ xa

a) Phải triển khai các biện pháp kiểm soát thích hợp để giảm thiểu rủi ro ATBMTT liên quan đến sử dụng thiết bị di dời được trong công việc:

- Phải có quy trình cấp phát và thu hồi thiết bị di dời được.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/01/2024

- Đảm bảo tất cả thiết bị di dời được phải được kiểm kê định kỳ tối thiểu mỗi năm một lần.
 - Đảm bảo các dữ liệu nhạy cảm lưu trên thiết bị di dời được phải được mã hóa bằng các phương pháp đã được phê duyệt.
 - Đảm bảo các thiết bị di dời được được bảo vệ bằng mật khẩu (nếu công nghệ hỗ trợ), và có tính năng tự động khóa sau một số lần đăng nhập không thành công, hoặc sau một khoảng thời gian không hoạt động.
 - Các thiết bị di dời được phải được cài đặt phần mềm chống mã độc (nếu có hỗ trợ).
 - Đảm bảo người sử dụng được đào tạo về sử dụng đúng cách thiết bị di dời được để giảm rủi ro rò rỉ dữ liệu, hư hỏng thiết bị, bị đánh cắp và thực hiện báo cáo khi có sự cố ATBMTT.
 - Đảm bảo người sử dụng được thông báo và xác nhận chấp nhận các quy định của chính sách về sử dụng thiết bị di dời được.
- b) Đối với làm việc từ xa, phải có giải pháp kiểm soát ATBMTT được triển khai để giảm thiểu rủi ro
- Dữ liệu nhạy cảm của PDH & CTTV ở dạng tập tin không được phép lưu trữ trên những thiết bị khác ở nơi làm việc từ xa trừ khi chúng được mã hóa bằng các phương pháp đã được phê duyệt.
 - Dữ liệu nhạy cảm của PDH & CTTV ở dạng tài liệu giấy không được phép lưu trữ ở nơi làm việc từ xa trừ khi chúng được để trong thiết bị lưu trữ có khóa.
 - Chỉ có máy tính của PDH & CTTV cấp phát mới được truy cập để quản trị hay xử lý thông tin của PDH & CTTV khi làm việc từ xa.
 - Chỉ những phương pháp truy cập từ xa được phê duyệt mới được phép truy cập vào hệ thống mạng của PDH & CTTV.

V.6 ATBMTT trong quản lý nguồn nhân lực

V.6.1 Trước khi làm việc

- a) Sàng lọc
 - Tất cả ứng viên phải được sàng lọc về kiến thức, kinh nghiệm trong việc hiểu và áp dụng ATBMTT.
 - Đối với ứng viên sẽ làm việc với thông tin nhạy cảm hoặc với các công việc quan trọng, phải có quy trình sàng lọc nghiêm ngặt tương ứng.
- b) Điều khoản và điều kiện làm việc
 - Tất cả cán bộ nhân viên của PDH & CTTV phải thực hiện ký cam kết bảo mật thông tin nhạy cảm của PDH & CTTV.
 - Cam kết bảo mật phải bao gồm tối thiểu những nội dung sau:
 - Mô tả thông tin cần được bảo vệ.
 - Thời gian thực hiện cam kết.
 - Trách nhiệm của bên cam kết nếu không tuân thủ.
 - Những yêu cầu sau khi hết thời gian cam kết (nếu có).
 - Tuyên bố đồng ý bảo mật dữ liệu (Data Privacy Consent Statement) đính kèm.

V.6.2 Trong thời gian làm việc

- a) Quản lý trách nhiệm

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/09/2024

- Trưởng đơn vị yêu cầu tất cả cán bộ nhân viên và nhà cung cấp thực hiện đúng theo các chính sách, quy định và quy trình ATBMTT của PDH & CTTV đã ban hành.
- Đảm bảo tất cả cán bộ nhân viên được phổ biến vai trò và trách nhiệm về ATBMTT trước khi được cấp quyền truy cập thông tin.
- Đảm bảo tất cả nhân viên có quyền truy cập chính sách ATBMTT.
- b) Đào tạo về nhận thức ATBMTT
 - Nhân viên phải được đào tạo về nhận thức ATBMTT phù hợp, được phổ biến và thông báo cập nhật những thay đổi của chính sách, quy định, quy trình ATBMTT.
 - Chương trình đào tạo nhận thức cho tất cả nhân viên phải thực hiện liên tục hàng năm. Chủ đề đào tạo tối thiểu gồm:
 - o Cách thức bảo vệ thông tin nhạy cảm của PDH & CTTV.
 - o Các mối đe dọa đối với ATBMTT tại PDH & CTTV.
 - o Các chính sách, quy trình, hướng dẫn về ATBMTT.
 - o Cách thức báo cáo sự việc liên quan đến ATBMTT.
 - Hình thức kỷ luật sẽ thực hiện theo “Nội quy lao động” của PDH & CTTV.

V.6.3 Thôi việc hay thay đổi công việc

- Trưởng đơn vị phải xác định những điều khoản còn hiệu lực về trách nhiệm bảo mật thông tin sau khi thay đổi công việc hoặc nghỉ việc để thông báo cho cán bộ nhân viên tuân thủ.
- Trước khi nhân viên chuyển việc hoặc nghỉ việc, tất cả tài sản thông tin PDH & CTTV đã cấp phát để xử lý công việc phải được thu hồi, và tất cả quyền hạn truy cập vào các hệ thống thông tin cũng phải được thu hồi.

V.7 Quản lý tài sản thông tin

V.7.1 Trách nhiệm đối với tài sản thông tin

- a) Kiểm kê tài sản thông tin
 - Chủ sở hữu tài sản thông tin phải nhận diện và tài liệu hóa danh sách tài sản thông tin để kiểm soát bao gồm:
 - Phần mềm (các ứng dụng, các hệ thống phần mềm, các công cụ và tiện ích phát triển phần mềm).
 - Phần cứng (Các máy tính, thiết bị mạng, phương tiện lưu trữ,...).
 - Dịch vụ (Các dịch vụ mạng máy tính và truyền thông).
 - Cơ sở dữ liệu và các tập tin dữ liệu, các thỏa thuận hợp đồng, các tài liệu hệ thống, thông tin nghiên cứu, hướng dẫn sử dụng, tài liệu đào tạo, quy trình hỗ trợ vận hành, kế hoạch hoạt động kinh doanh liên tục...
 - Mức độ bảo mật của các tài sản thông tin.
- b) Trách nhiệm của chủ sở hữu tài sản thông tin
 - Kiểm soát việc sản xuất, phát triển, bảo trì, sử dụng và bảo mật tài sản thông tin trong phạm vi quyền hạn của mình.
 - Đảm bảo rằng các tài sản thông tin được phân loại và bảo vệ thích hợp.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/03/2024

- Định nghĩa quyền hạn truy cập và phân loại tài sản, thường xuyên rà soát quyền hạn và phân loại này đảm bảo phù hợp với các chính sách hiện hành.
- c) Quản lý sử dụng tài sản thông tin
- Tất cả người sử dụng các hệ thống thông tin phải có trách nhiệm và nghĩa vụ bảo vệ tài sản thông tin.
- d) Thu hồi tài sản thông tin
 - Cán bộ nhân viên phải hoàn trả lại tài sản thông tin cho PDH khi chấm dứt hoặc thay đổi công việc.
 - Trưởng đơn vị phải đảm bảo thu hồi các tài sản sau:
 - Các tài sản thông tin được tạo bởi nhân viên đó trong thời gian làm việc.
 - Tất cả thư điện tử liên quan đến công việc của nhân viên (kể cả liên quan đến công việc hiện tại hay trước đó).
 - Phần cứng máy tính, bản quyền phần mềm và các thiết bị liên quan.
 - Các phương tiện lưu trữ di dời được.
 - Các thẻ, chìa khóa ra vào các cửa và những thiết bị tương tự khác.
 - Với những thiết bị truy cập không được trả lại phải được ghi nhận thành tài liệu theo dõi và từng bước xử lý để đảm bảo chúng không được sử dụng để xâm nhập trái phép vào các tòa nhà, phòng làm việc, TTDL/PMC hoặc các hệ thống thông tin của PDH & CTTV.

V.7.2 Phân loại tài sản thông tin

- a) Phân loại cấp độ bảo mật tài sản tài sản thông tin
 - Ban CNTT có trách nhiệm xây dựng hướng dẫn phân loại tài sản thông tin. Hướng dẫn phân loại này dựa trên yêu cầu về tính bảo mật, tính toàn vẹn và tính sẵn sàng của tài sản thông tin.
 - Chủ sở hữu tài sản thông tin phải xác định cấp độ bảo mật phù hợp theo hướng dẫn phân loại tài sản thông tin được ban hành.
- b) Dán nhãn tài sản thông tin
 - Tài sản thông tin (kể cả ở dạng vật lý hay điện tử) phải được gắn nhãn cấp độ bảo mật phù hợp. Việc này nhằm thông báo cho người sử dụng biết mức độ yêu cầu cần được bảo vệ của tài sản thông tin.
- c) Quản lý tài sản thông tin
 - Tài sản thông tin phải được quản lý phù hợp với cấp độ bảo mật của nó. Ban CNTT có trách nhiệm xây dựng hướng dẫn để bảo vệ tài sản trong quá trình xử lý, lưu trữ, truyền nhận, tiêu hủy.
 - Tài liệu hướng dẫn bảo vệ tài sản thông tin tối thiểu bao gồm những thông tin sau:
 - Những yêu cầu giới hạn truy cập cho từng cấp độ bảo mật.
 - Những yêu cầu bảo vệ các bản sao của tài sản thông tin.

V.7.3 Quản lý phương tiện lưu trữ

- a) Quản lý phương tiện lưu trữ di dời được
 - Tất cả phương tiện lưu trữ di dời được phải được quản lý và kiểm soát phù hợp với cấp độ bảo mật của thông tin đang lưu trữ bên trong nó.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/01/2024

- Những dữ liệu nhạy cảm lưu trong phương tiện di dời được phải được mã hóa bằng các giải pháp đã được phê duyệt.
 - Các trường hợp được cấp phát sử dụng phương tiện lưu trữ di dời được phải được phê duyệt bằng chứng từ của Giám đốc Ban CNTT.
 - Phương tiện lưu trữ di dời được phải được cài đặt mật khẩu bảo vệ (nếu có hỗ trợ).
 - Phương tiện lưu trữ di dời được tiếp nhận từ đối tác bên ngoài phải được thực hiện quét mã độc trước khi sử dụng.
 - Người sử dụng phải thông báo ngay về BP HT&BM – Ban CNTT khi phương tiện lưu trữ di dời được bị mất hoặc bị đánh cắp.
- b) Xử lý phương tiện lưu trữ khi không còn nhu cầu sử dụng
- Phương tiện lưu trữ có chứa dữ liệu nhạy cảm phải được tiêu hủy an toàn bằng biện pháp vật lý (như thiêu đốt, đập vỡ, cắt) khi không còn nhu cầu sử dụng.
 - Trường hợp cần chuyển cho người khác trong PDH & CTTV sử dụng lại phương tiện lưu trữ thì tất cả dữ liệu lưu trữ bên trong phải được xóa hết.
- c) Vận chuyển phương tiện lưu trữ
- Phương tiện lưu trữ có chứa thông tin phải được bảo vệ khỏi truy cập trái phép hoặc hỏng hóc trong quá trình vận chuyển.
 - Đối tác thực hiện vận chuyển phương tiện lưu trữ phải được phê duyệt bởi cấp Giám đốc Ban CNTT.
 - Phải thực hiện bao bọc để tránh hỏng hóc vật lý.
 - Phải thực hiện các biện pháp bảo vệ theo hướng dẫn từ nhà sản xuất để tránh hỏng hóc do nhiệt độ, độ ẩm hay từ trường.
 - Nhật ký vận chuyển phải được ghi nhận lại như thời gian, nơi đi, nơi đến, người vận chuyển, người nhận.

V.8 Kiểm soát truy cập hệ thống CNTT

V.8.1 Yêu cầu trong quản lý truy cập

- a) Yêu cầu chung về kiểm soát truy cập
- Quyền hạn truy cập vào hệ thống CNTT phải được phê duyệt, quản lý, giám sát và kiểm soát đảm bảo chỉ phục vụ vừa đủ yêu cầu công việc và tuân thủ các yêu cầu về ATBMTT.
 - Quyền hạn truy cập vào hệ thống CNTT phải phù hợp với mô tả công việc và vai trò của người sử dụng.
 - Nhân sự yêu cầu cấp phát, phê duyệt, thực hiện cấp phát tài khoản truy cập phải được tách biệt trách nhiệm thực hiện.
- b) Quy định về truy cập mạng
- Người sử dụng chỉ được cấp quyền truy cập vào dịch vụ và hệ thống mạng giới hạn vừa đủ để phục vụ công việc.
 - Các truy cập mạng phải được giám sát nhằm sớm phát hiện và xử lý các trường hợp xâm nhập trái phép.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 20/01/2024

V.8.2 Quản lý truy cập người sử dụng

- a) Đăng ký và hủy tài khoản truy cập người sử dụng
 - Phải xây dựng quy trình đăng ký và hủy tài khoản truy cập người sử dụng.
 - Đăng ký tài khoản truy cập:
 - Yêu cầu cấp phát quyền truy cập phải phù hợp với vai trò và nhiệm vụ của người sử dụng và phải được phê duyệt bởi Trưởng đơn vị.
 - Mỗi người sử dụng được cấp phát tài khoản riêng biệt, không đăng ký sử dụng chung tài khoản truy cập.
 - Thay đổi quyền trên tài khoản truy cập:
 - Phải đánh giá lại quyền hạn truy cập mỗi khi người sử dụng thay đổi vai trò và nhiệm vụ công việc.
 - Khóa tài khoản truy cập:
 - Khi người sử dụng thôi việc hoặc quyền truy cập không còn nhu cầu sử dụng phải thực hiện theo quy trình khóa tài khoản truy cập.
- b) Cấp quyền truy cập người sử dụng
 - Phải xây dựng quy trình cấp phát, thay đổi quyền truy cập cho người sử dụng để thực hiện gán và thu hồi quyền truy cập vào tất cả các hệ thống CNTT.
 - Quyền hạn truy cập được cấp phát phải phù hợp với vai trò và chức năng công việc.
 - Quyền truy cập chỉ được kích hoạt sau khi người sử dụng xác nhận đã nhận được đầy đủ thông tin như yêu cầu đăng ký cấp phát.
- c) Quản lý tài khoản đặc quyền
 - Tài khoản đặc quyền phải hạn chế đối tượng được cấp phát và phải thực hiện kiểm soát việc sử dụng.
 - Nhật ký hệ thống (system log) phải ghi nhận đầy đủ hoạt động của các tài khoản đặc quyền, nhật ký này phải được bảo vệ tránh bị thay đổi bởi chính người sử dụng tài khoản đặc quyền.
- d) Quản lý mật khẩu người dùng
 - Mật khẩu chỉ được cấp phát cho người sử dụng đã được phê duyệt.
 - Mật khẩu gửi đến người sử dụng phải theo quy trình được kiểm soát bảo mật tránh bị tiết lộ.
 - Mật khẩu cấp phát lần đầu phải được thay đổi trước khi sử dụng.
 - Mật khẩu được lưu trữ trên hệ thống CNTT phải được mã hóa bằng các thuật toán đã được PDH chấp nhận.
- e) Rà soát quyền truy cập người sử dụng
 - Định kỳ tối thiểu mỗi năm một lần phải thực hiện rà soát quyền truy cập của người sử dụng.
 - Định kỳ tối thiểu mỗi năm một lần phải thực hiện rà soát quyền truy cập của các tài khoản đặc quyền.
 - Phải thực hiện rà soát lại quyền truy cập khi người sử dụng có thay đổi chức danh công việc, hoặc thay đổi mô tả công việc, hay bất kỳ thay đổi nào ảnh hưởng đến nhu cầu truy cập hệ thống thông tin.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/01/2024

V.8.3 Trách nhiệm của người sử dụng trong quản lý mật khẩu

- Phải thực hiện thay đổi mật khẩu tạm được cấp ngay lần đầu tiên đăng nhập thành công.
- Phải thay đổi mật khẩu định kỳ phù hợp với chính sách mật khẩu.
- Không được tiết lộ mật khẩu của mình cho bất kỳ người nào khác.
- Không ghi mật khẩu ra bất kỳ nơi nào trừ khi có giải pháp bảo vệ phù hợp đã được PDH chấp nhận.
- Phải thay đổi mật khẩu ngay lập tức khi nghi ngờ hoặc xác định đã bị lộ.
- Chính sách mật khẩu bao gồm tối thiểu các nội dung sau:
 - Độ dài mật khẩu tối thiểu 12 ký tự.
 - Phải kết hợp tối thiểu 04 yếu tố sau: có ký tự chữ in (A-Z), có ký tự chữ thường (a-z), có ký số (0-9), có ký tự đặc biệt (ví dụ: !, @, #, \$, %...).
 - Mật khẩu phải được thay đổi tối thiểu mỗi 120 ngày.
 - Không sử dụng lại 02 mật khẩu gần nhất.
 - Tài khoản truy cập phải được khóa sau tối đa 06 lần liên tiếp đăng nhập không thành công.

V.8.4 Kiểm soát truy cập hệ thống và ứng dụng

- a) Hạn chế truy cập thông tin
 - Mỗi hệ thống CNTT phải có chức năng phân quyền truy cập.
 - Việc phân quyền truy cập phải được cấu hình tham số hóa để có thể linh hoạt thay đổi quyền truy cập mà không phải thay đổi mã nguồn.
 - Hệ thống cung cấp thông tin phổ biến phải được tách biệt với các hệ thống thông tin nhạy cảm của PDH & CTTV.
- b) Kiểm soát đăng nhập an toàn
 - Không hiển thị các thông tin nhạy cảm trước khi đăng nhập thành công.
 - Phải ghi nhận lại lịch sử các lần đăng nhập không thành công của người sử dụng.
 - Mật khẩu phải được mã hóa từ thiết bị đầu cuối trước khi gửi về máy chủ để xác thực, không truyền mật mã chưa được mã hóa qua hệ thống mạng.
- c) Hệ thống quản lý mật khẩu phải có các tính năng
 - Xác thực người sử dụng trước khi truy cập vào hệ thống CNTT.
 - Cho phép người sử dụng tự thay đổi mật khẩu của mình.
 - Bắt buộc người sử dụng thay đổi mật khẩu tạm được cấp phát lần đầu trước khi truy cập vào hệ thống.
 - Bắt buộc người sử dụng thay đổi mật khẩu định kỳ theo chính sách mật khẩu của PDH, và phải có thông báo cho người sử dụng khi mật khẩu gần đến hạn phải thay đổi.
 - Cấm sử dụng lại mật khẩu cũ theo chính sách mật khẩu.
 - Lưu trữ và truyền nhận mật khẩu dưới dạng đã mã hóa.
 - Hỗ trợ cơ chế xác thực nhiều yếu tố (Multi-factor Authentication).
- d) Sử dụng các tiện ích đặc quyền
 - Hạn chế đến mức thấp nhất số lượng người sử dụng các tiện ích đặc quyền.
 - Phải ghi nhận đầy đủ lịch sử truy cập và sử dụng các tiện ích đặc quyền.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: <u>26/03/2024</u>

- Định kỳ phải thực hiện rà soát việc sử dụng các tiện ích đặc quyền.
- Phải sử dụng biện pháp đăng nhập an toàn đối với các tiện ích đặc quyền, bắt buộc phải sử dụng xác thực nhiều yếu tố (Multi-factor Authentication).
- e) Kiểm soát truy cập mã nguồn phần mềm
 - Mã nguồn phần mềm phải được lưu trữ tập trung.
 - Không lưu trữ thư viện mã nguồn phần mềm trong môi trường production (nếu kỹ thuật cho phép).
 - Chỉ cấp quyền truy cập vào thư viện mã nguồn phần mềm vừa đủ phục vụ nhu cầu công việc.
 - Nhật ký thay đổi mã nguồn phần mềm phải được ghi nhận lại đầy đủ.

V.9 Mã hóa

V.9.1 Quy định về sử dụng các thuật toán mã hóa

- Các thuật toán mã hóa sau đây được chấp nhận sử dụng tại PDH:
 - Danh mục thuật toán mã hóa đối xứng:
 - TDEA | Triple Data Encryption Algorithm
 - AES | Advanced Encryption Standard.
 - Danh mục thuật toán mật mã phi đối xứng:
 - RSA | Ron Rivest, Adi Shamir và Leonard Adleman
 - DSA | Digital Signatures Algorithm
 - Danh mục thuật toán băm:
 - SHA-256, SHA-384, SHA-512/256, SHA-512 | Secure Hash Algorithm
- Chiều dài khóa mã hóa của các thuật toán TDEA, AES tối thiểu phải là 192 bits.
- Độ dài khóa mã hóa của thuật toán RSA tối thiểu phải là 3027 bits, DSA với $L \geq 3072$, $N \geq 256$.
- Danh sách thuật toán và độ dài khóa mã hóa được chấp nhận phải được rà soát tối thiểu mỗi năm một lần.

V.9.2 Quản lý khóa mã hóa

- Các khóa mã hóa phải được quản lý, theo dõi trong suốt vòng đời từ lúc tạo ra đến khi hủy bỏ.
- Tất cả các khóa mã hóa phải được bảo vệ tránh rò rỉ, mất mát hoặc thay đổi trái phép.
- Không sử dụng chung một khóa mã hóa cho nhiều hệ thống phần mềm ứng dụng tài chính khác nhau.
- Phải thực hiện vô hiệu hóa khóa mã hóa ngay khi nó bị rò rỉ, hoặc khi người nắm giữ nó thay đổi chức năng công việc không còn nhu cầu sử dụng hay thôi việc.
- Phải sao lưu khóa mã hóa để phòng bị mất.

V.10 An ninh vật lý và môi trường cho TTDL/PMC

V.10.1 Khu vực an ninh

- a) Chu vi an ninh
 - Vách ngăn của tòa nhà hoặc của khu vực chứa TTDL/PMC phải được thiết kế chắc chắn về mặt vật lý, đảm bảo không dễ dàng bị xâm nhập trái phép; mái nhà, các bức tường xung quanh và sàn nhà phải được xây dựng vững chắc; tất cả các cổng ra vào bên ngoài phải được sử dụng các cơ chế kiểm soát để tránh bị xâm nhập trái phép (ví dụ: thanh chắn, chuông báo động, khóa).

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: <u>16/09/2024</u>

- Chỉ cho phép những cá nhân có thẩm quyền được vào bên trong.
- Phải có thiết bị giám sát xâm nhập trái phép như camera và luôn ở trạng thái đang hoạt động, đảm bảo bao phủ được tất cả các cửa ra vào. Thiết bị phải được kiểm tra định kỳ tối thiểu 01 tháng một lần.
- b) Kiểm soát vào ra
 - Tất cả những quyền vào ra TTDL/PMC phải được ghi nhận thành danh sách và phải được phê duyệt bởi giám đốc Ban CNTT.
 - Các cá nhân không có quyền vào ra TTDL/PMC, khi có nhu cầu công việc cần vào ra khu vực này phải:
 - Được giám đốc Ban CNTT phê duyệt từng lần với thời gian giới hạn.
 - Được cá nhân có quyền ra vào khu vực TTDL/PMC giám sát trong suốt quá trình tác nghiệp. Cá nhân giám sát cũng phải được thể hiện trong chứng từ phê duyệt.
 - Xuất trình giấy tờ định danh/ giấy giới thiệu khi ra vào TTDL/PMC.
 - Nhật ký ra vào TTDL/PMC phải được ghi nhận lại, thông tin tối thiểu gồm: ngày giờ vào, ngày giờ ra, họ tên, đơn vị, mục đích công việc.
 - Những khu vực lưu trữ hay xử lý thông tin bảo mật phải được hạn chế vào ra, phải trang bị hệ thống kiểm soát vào ra đủ mạnh thích hợp (ví dụ sử dụng phương thức xác thực kết hợp 2 yếu tố: khuôn mặt và mật mã).
 - Sổ vật lý hoặc thông tin điện tử ghi nhật ký vào ra phải được bảo quản an toàn.
 - Tất cả cá nhân phải mang thẻ nhận diện khi vào TTDL/PMC, và thông báo ngay cho nhân viên an ninh nếu gặp cá nhân nào không mang thẻ nhận diện bên trong khu vực này.
 - Quyền vào ra khu vực này phải được rà soát định kỳ tối thiểu 06 tháng 01 lần, với những quyền vào ra TTDL/PMC đã được cấp trước đây mà không còn cần thiết cho nhu cầu công việc hiện tại phải được vô hiệu hóa ngay. Việc vô hiệu hóa quyền vào ra TTDL/PMC phải thực hiện đầy đủ các bước:
 - Vô hiệu hóa quyền trên hệ thống (thẻ từ, vân tay, nhận diện khuôn mặt,...).
 - Thu hồi thẻ từ, khóa cửa (nếu có).
 - Cập nhật lại danh sách nhân sự được phép vào ra TTDL/PMC.
- c) An ninh vật lý cho khu vực đặt TTDL/PMC
 - Khu vực đặt TTDL/PMC phải độc lập và tách biệt với khu vực chung (nếu có thê).
 - Không được phô trương quảng bá hoặc đặt các biển hiệu, biển tên minh bạch về TTDL/PMC kể cả bên trong và bên ngoài tòa nhà.
 - Tài liệu lưu trữ vị trí của TTDL/PMC phải được bảo mật, những người không có thẩm quyền không được phép truy cập.
- d) Bảo vệ chống lại các mối đe dọa từ môi trường bên ngoài
 - TTDL/PMC phải được thiết kế có các biện pháp phòng chống nguy cơ do cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên và con người gây ra; trang bị đầy đủ thiết bị phòng chống cháy nổ, lũ lụt, hệ thống chống sét.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/03/2024

- TTDL/PMC phải đảm bảo không dột; không thấm nước; không bị ánh nắng chiếu rọi trực tiếp; độ ẩm, nhiệt độ đạt tiêu chuẩn quy định cho các thiết bị mạng, thiết bị tường lửa, thiết bị lưu trữ và máy chủ CNTT.
- Phải có các thiết bị hỗ trợ công tác kiểm tra kiểm soát và vận hành TTDL/PMC như hệ thống máy quay an ninh, hệ thống giám sát và điều khiển nhiệt độ, độ ẩm từ xa.
- e) Làm việc trong TTDL/PMC
 - Các trường hợp làm việc trong TTDL/PMC đều phải được giám sát cho cả lý do an toàn và cung tránh được các rủi ro hoạt động trái phép.
 - Không được mang thức ăn, thức uống, thú cưng,... vào TTDL/PMC.
 - Không được tự ý chụp ảnh, quay phim, ghi âm khi chưa có phê duyệt của Giám đốc Ban CNTT.
- f) Khu vực vận chuyển
 - Chỉ những người đã được phê duyệt mới được phép vào khu vực này.
 - Khu vực này phải được thiết kế an toàn đảm bảo những người vận chuyển không thể vào được các khu vực khác cùng tòa nhà.
 - Hàng hóa chuyển đi và chuyển đến phải được dán nhãn để phân biệt.

V.10.2 Trang thiết bị

- a) Bảo vệ trang thiết bị
 - Không được đặt máy móc, thiết bị, vật liệu bên trong TTDL/PMC khi không có nhu cầu đang sử dụng tại TTDL/PMC.
 - Hệ thống thông tin xử lý dữ liệu nhạy cảm phải đảm bảo tránh bị nhìn thấy bởi những cá nhân không được phép tiếp cận trong quá trình làm việc tại TTDL/PMC.
 - Phải đóng hoặc đăng xuất khỏi phiên làm việc ngay khi kết thúc công việc.
 - Phải có cơ chế kiểm soát bảo mật (như đăng nhập mật khẩu) để tránh truy cập trái phép vào trang thiết bị.
 - Phải có hệ thống chống sét cho TTDL/PMC riêng, điện nguồn cùng với các đường truyền dữ liệu phải được lắp đặt bộ lọc chống sét lan truyền.
 - Không được tự ý tháo dỡ trang thiết bị ra khỏi hệ thống trừ khi cá nhân đó đã được phê duyệt bởi Giám đốc Ban CNTT.
 - Thời gian trang thiết bị được tháo dỡ phải được xác định, khi hoàn trả phải có chứng từ xác nhận.
 - Trang thiết bị được tháo dỡ ra khỏi hệ thống và khi được lắp lại vào hệ thống đều phải được ghi nhận.
- b) Tiện ích hỗ trợ
 - Phải có hệ thống máy phát điện dự phòng để thay thế khi hệ thống điện chính ngưng hoạt động.
 - Phải có thiết bị lưu điện công suất đủ đáp ứng cho TTDL/PMC vận hành bình thường trong thời gian tối thiểu 15 phút.
 - Định kỳ tối thiểu mỗi năm một lần thực hiện đánh giá để đảm bảo công suất hoạt động của hệ thống điều hòa và thiết bị lưu điện dự phòng.
- c) An ninh dây cáp

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: <u>26/03/2024</u>

- Các đường dây điện và cáp viễn thông vào bên trong TTDL/PMC phải được đi ngầm dưới sàn hoặc phải có máng treo bên trên.
- Cáp điện nguồn phải được tách rời với cáp viễn thông để tránh bị nhiễu tín hiệu.
- d) Bảo trì sửa chữa trang thiết bị
 - Trang thiết bị phải được giữ gìn, bảo quản đúng theo khuyến cáo của nhà sản xuất.
 - Chỉ những cá nhân được phê duyệt thì mới được thực hiện sửa chữa/ bảo trì.
 - Phải ghi nhận lại nhật ký việc bảo dưỡng và sửa chữa các trang thiết bị bị lỗi.
 - Lịch bảo dưỡng định kỳ của trang thiết bị phải được kiểm soát và thực hiện đúng.
- e) An ninh đối với trang thiết bị/tài sản thông tin do PDH & CTTV cấp để sử dụng bên ngoài văn phòng làm việc của PDH & CTTV
 - Việc sử dụng trang thiết bị lưu trữ hoặc xử lý thông tin bên ngoài trụ sở làm việc của PDH & CTTV phải được phê duyệt bởi Trưởng Đơn Vị.
 - Không được để trang thiết bị do PDH & CTTV cấp nơi công cộng khi không có cơ chế giám sát.
 - Phải luôn thực hiện đúng theo hướng dẫn của nhà sản xuất về việc bảo vệ trang thiết bị nhằm tránh hư hỏng.
- f) An ninh cho trang thiết bị thanh lý, sửa chữa hay tái sử dụng
 - Những trang thiết bị hư hỏng có chứa dữ liệu phải được đánh giá rủi ro để quyết định tiêu hủy vật lý hay gửi đi sửa hoặc vứt bỏ thông thường.
 - Phải tiêu hủy tất cả dữ liệu trên thiết bị được thanh lý, hoặc xóa tất cả dữ liệu trên thiết bị được dùng vào mục đích tái sử dụng.

V.11 An ninh trong vận hành hệ thống công nghệ thông tin

V.11.1 Trách nhiệm và quy trình vận hành

- a) Tài liệu hóa quy trình vận hành
 - Phải có tối thiểu các tài liệu về quy trình vận hành:
 - Quy trình giám sát các thiết bị đảm bảo hạ tầng TTDL/PMC (điều hoà, UPS, báo cháy, rò rỉ chất lỏng)
 - Quy trình xử lý sự cố các hệ thống hạ tầng TTDL/PMC (điều hoà, UPS, báo cháy, rò rỉ chất lỏng)
 - Quy trình giám sát hệ thống máy chủ, thiết bị mạng và các thiết bị khác trong TTDL/PMC
 - Quy trình xử lý sự cố hệ thống máy chủ, thiết bị mạng và các thiết bị khác trong TTDL
 - Quy trình giám sát hệ thống mạng
 - Quy trình xử lý sự cố hệ thống mạng
 - Quy trình cấp phát, thu hồi tài khoản người dùng
 - Quy trình cấp phát, thu hồi tài khoản đặc quyền
 - Quy trình quản lý sự thay đổi CNTT
 - Quy trình tiếp nhận và xử lý sự cố an ninh thông tin.
 - Phải có tối thiểu các tài liệu hướng dẫn:
 - Hướng dẫn cài đặt và cấu hình máy chủ.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: <u>26/03/2024</u>

- Hướng dẫn cài đặt và cấu hình máy mạng.
- Hướng dẫn các bước khởi động lại và phục hồi khi hệ thống thông tin bị lỗi.
- Hướng dẫn xử lý các trường hợp lỗi phát sinh trong quá trình thực hiện các tác vụ theo lịch định kỳ.
- Hướng dẫn xử lý dữ liệu nhạy cảm của PDH & CTTV được sinh ra từ các tác vụ chạy theo lịch định kỳ nhưng bị thất bại.
- Phải có tài liệu ghi nhận đầy đủ thông tin liên lạc các cấp độ để hỗ trợ xử lý (kể cả thông tin liên lạc hỗ trợ từ bên ngoài) cho các phát sinh không mong muốn xảy ra trong quá trình vận hành.
- Phải có tài liệu mô tả các tác vụ chạy theo lịch định kỳ (job schedules), tài liệu phải ghi rõ ngày giờ thực hiện, tổng thời gian tối đa chấp nhận được để tác vụ này thực hiện là bao nhiêu.
- b) Quản lý thay đổi
 - Phải ghi nhận lại tất cả các thay đổi trên hệ thống production.
 - Phải có bản kế hoạch và biên bản kiểm thử sự thay đổi trước khi cập nhật lên hệ thống production.
 - Phải có đánh giá những tác động tiềm ẩn và đảm bảo việc thay đổi này đáp ứng các yêu cầu về ATBMTT mà PDH đã ban hành.
 - Tất cả các thay đổi lên hệ thống produciotn phải có chứng từ phê duyệt của Giám đốc Ban CNTT hoặc Tổng Giám đốc tùy vào trường hợp cụ thể.
 - Thông tin chi tiết của việc thay đổi phải được truyền thông tới tất cả những người liên quan.
 - Phải có kịch bản hướng dẫn từng bước thực hiện việc phục hồi lại trạng thái ban đầu trong trường hợp thay đổi không thành công.
- c) Quản lý khả năng đáp ứng của hệ thống
 - Khả năng đáp ứng của hệ thống thông tin cần phải được xác định, kể cả khả năng ở hiện tại và tương lai để đáp ứng nhu cầu kinh doanh trong tối thiểu 02 năm tới.
 - Thực hiện kiểm tra để kịp thời phát hiện các sự cố ảnh hưởng đến khả năng đáp ứng của hệ thống CNTT.
 - Định kỳ tối thiểu 01 năm một lần phải thực hiện việc xóa bỏ hoặc di chuyển những dữ liệu cũ/ dữ liệu rác phát sinh mà hiện tại không còn nhu cầu sử dụng, việc thực hiện xóa bỏ hay di chuyển phải có chứng từ phê duyệt của Giám đốc Ban CNTT.
- d) Tách biệt môi trường phát triển, thử nghiệm và production
 - Môi trường phát triển, thử nghiệm và production phải được tách riêng biệt để giảm rủi ro xảy ra truy cập hay thay đổi trái phép lên môi trường prodution.
 - Môi trường phát triển và production phải được đặt tách biệt ở hai hệ thống khác nhau.
 - Tất cả thay đổi trên môi trường production phải được thực hiện kiểm thử trước trong môi trường thử nghiệm.
 - Thông tin dùng để đăng nhập vào hệ thống production và hệ thống thử nghiệm phải khác nhau.

V.11.2 Phòng chống mã độc tấn công

- Chỉ được cài đặt những phần mềm có nguồn gốc từ chính hãng và đã được phê duyệt bởi Tổng Giám đốc PDH.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/03/2024

- Định kỳ tối thiểu 01 năm một lần phải thực hiện việc rà soát lại danh sách phần mềm đã cài đặt trên hệ thống thông tin để kịp thời phát hiện và xử lý những trường hợp thay đổi trái phép.
- Phải cài đặt phần mềm phòng chống mã độc để bảo vệ hệ thống thông tin, phần mềm này phải tự động cập nhật dữ liệu nhận diện mã độc tức thời từ hãng sản xuất.

V.11.3 Sao lưu dự phòng

- Phải có tài liệu hướng dẫn sao lưu dự phòng, bao gồm sao lưu dữ liệu; phần mềm và cấu hình hệ thống.
- Công việc sao lưu đầy đủ phải được thực hiện định kỳ tối thiểu 02 tuần một lần để đảm bảo tất cả thông tin/ dữ liệu, phần mềm và cấu hình hệ thống có thể được phục hồi sau thảm họa hoặc thiết bị lưu trữ bị hư hỏng.
- Các lần sao lưu và phục hồi dữ liệu phải được ghi nhận lại thành tài liệu.
- Dữ liệu sao lưu phải được lưu trữ ở một địa điểm vật lý khác và đủ xa với nơi đặt hệ thống thông tin để tránh bị tác động bởi thiên tai.
- Dữ liệu sao lưu phải được phục hồi thử nghiệm ngẫu nhiên tối thiểu 06 tháng một lần để đảm bảo rằng dữ liệu có thể sử dụng được trong các trường hợp khẩn cấp.
- Đối với dữ liệu nhạy cảm của PDH & CTTV, dữ liệu sau khi sao lưu phải được mã hóa hoặc bảo vệ bằng mật mã.

V.11.4 Giám sát và ghi nhật ký

- a) Nhật ký sự kiện
 - Nhật ký hoạt động của người sử dụng; lỗi phát sinh; sự kiện liên quan đến ATBMTT phải được hệ thống ghi nhận lại và phải được bảo vệ an toàn.
 - Nhật ký sự kiện tối thiểu phải lưu lại các thông tin sau:
 - Định danh những người sử dụng (user ID).
 - Các hoạt động hệ thống (system activities).
 - Ngày giờ và thông tin chi tiết của các sự kiện chính (key events: log-on, log-off).
 - Truy cập thành công hay thất bại vào hệ thống.
 - Thay đổi cấu hình hệ thống.
 - Quyền hạn truy cập.
 - Tập tin bị truy xuất và kiểu truy xuất.
 - Địa chỉ mạng và giao thức truy cập.
- b) Bảo vệ thông tin nhật ký
 - Phải có giải pháp bảo vệ phương tiện lưu trữ nhật ký, và thông tin nhật ký đảm bảo không bị truy cập/ sửa/ xóa trái phép.
 - Năng lực lưu trữ còn lại của phương tiện lưu trữ nhật ký phải được kiểm soát và có cảnh báo khi vượt quá 90% khả năng lưu trữ.
 - Nhật ký hệ thống được sao chép theo thời gian thực (real-time) sang một hệ thống khác nằm ngoài khả năng quản lý của những người quản trị hệ thống này.
 - Nhật ký hoạt động của người quản trị và vận hành hệ thống thông tin

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/01/2024

- Nhật ký hoạt động của những người quản trị và vận hành hệ thống thông tin phải được ghi nhận đầy đủ, bảo vệ và định kỳ rà soát tối thiểu 01 năm một lần.
- c) Đồng bộ thời gian
- Thời gian của tất cả các hệ thống thông tin liên quan của PDH phải được đồng bộ cùng một nguồn thời gian giống nhau.
- Phải tài liệu hóa những yêu cầu về việc đồng bộ thời gian (gồm cả yêu cầu từ bên trong nội bộ lẫn bên ngoài như quy định của luật pháp, các cam kết trong hợp đồng,...). Ghi rõ nguồn thời gian đồng bộ và độ sai lệch tối đa được chấp nhận.

V.11.5 Kiểm soát vận hành phần mềm

- Việc cập nhật những thư viện chương trình, ứng dụng, phần mềm vận hành phải được thực hiện bởi người quản trị đã được Giám đốc Ban CNTT phê duyệt.
- Phần mềm ứng dụng và hệ điều hành chỉ được cập nhật lên hệ thống vận hành sau khi đã kiểm thử thành công. Công việc kiểm thử phải được thực hiện trên một hệ thống độc lập với hệ thống vận hành.
- Phải có tài liệu ghi nhận lại tất cả cấu hình phần mềm đang vận hành.
- Kịch bản trả về trạng thái ban đầu (rollback) phải được xây dựng trước mỗi lần cập nhật thay đổi trên hệ thống phần mềm.
- Phiên bản trước khi cập nhật của phần mềm ứng dụng phải được lưu giữ lại cùng với tất cả dữ liệu, tài liệu tham số, cấu hình, quy trình nhằm mục đích dự phòng.
- Dịch vụ hỗ trợ phần mềm cho phiên bản trước khi cập nhật cũng phải được duy trì đủ dài theo thời gian lưu trữ phiên bản cũ.
- Việc truy cập của nhà cung cấp phần mềm vào hệ thống chỉ được cho phép khi đã có sự phê duyệt của Giám đốc Ban CNTT, và có giới hạn thời gian truy cập. Tất cả hoạt động của nhà cung cấp trên hệ thống phải được giám sát.

V.11.6 Quản lý lỗ hổng kỹ thuật

- Phải thực hiện đầy đủ việc rà soát định kỳ tối thiểu 01 năm một lần đối với các hệ thống thông tin, thông tin rà soát ghi nhận tối thiểu gồm: nhà cung cấp và phiên bản phần mềm, nhà cung cấp và cấu hình phần cứng, hiện trạng của việc triển khai (phần mềm gì được cài lên hệ thống gì), các cá nhân trong công ty chịu trách nhiệm quản lý/ vận hành phần mềm/ hệ thống đó. Đánh giá và nhận diện lại các lỗ hổng kỹ thuật của hệ thống.
- Phải phân công rõ vai trò và trách nhiệm trong việc quản lý lỗ hổng kỹ thuật bao gồm: giám sát, đánh giá rủi ro, cập nhật bản vá lỗ hổng kỹ thuật.
- Mốc thời gian để phản ứng từ khi nhận biết thông tin về lỗ hổng kỹ thuật cần phải được xác định rõ, tối đa không quá 05 ngày làm việc.
- Với mỗi lỗ hổng kỹ thuật đã được nhận diện, phải thực hiện việc đánh giá rủi ro và xây dựng kế hoạch xử lý như cập nhật bản vá hoặc bổ sung/ thay đổi việc kiểm soát.
- Nếu bản vá cho lỗ hổng kỹ thuật đã có sẵn từ nguồn hợp lệ, phải thực hiện việc đánh giá để quyết định xem nên cập nhật bản vá hay chấp nhận rủi ro tồn tại lỗ hổng sẽ phù hợp hơn.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH AN TOÀN BẢO MẬT THÔNG TIN	Lần ban hành: 01 Ngày hiệu lực: 26/01/2024

- Trường hợp chưa có bản vá để cập nhật, phải đưa ra các kiểm soát để hạn chế rủi ro từ lỗ hổng kỹ thuật này, ví dụ như: tắt dịch vụ hoặc tính năng liên quan lỗ hổng này; cấu hình bổ sung thêm kiểm soát truy cập như hệ thống tường lửa (firewall), tường lửa ứng dụng web (web application firewall); gia tăng giám sát; nâng cao nhận thức người sử dụng.
- Hệ thống có độ rủi ro cao phải được ưu tiên thực hiện xử lý lỗ hổng trước.
- Quá trình quản lý lỗ hổng kỹ thuật phải liên kết với các hoạt động quản lý sự cố.

V.11.7 Kiểm toán hệ thống thông tin

- Những yêu cầu truy cập vào dữ liệu/ hệ thống nhằm mục đích kiểm toán CNTT phải được sự đồng ý bởi Tổng Giám đốc PDH.
- Phạm vi kiểm toán phải xác định rõ và phải được phê duyệt bởi Tổng Giám đốc PDH.
- Quyền truy cập dữ liệu/ phần mềm để phục vụ kiểm toán chỉ giới hạn ở mức độ chỉ đọc (read only).
- Với những yêu cầu truy cập dữ liệu cao hơn quyền hạn chỉ đọc thì phải được phê duyệt bởi Tổng Giám đốc PDH, chỉ cung cấp bản sao dữ liệu yêu cầu, chúng phải được xóa bỏ hoặc phải được bảo vệ phù hợp nếu cần lưu trữ để làm chứng cứ kiểm toán.
- Những thực hiện kiểm toán có thể ảnh hưởng đến độ sẵn sàng hay hiệu năng của hệ thống cần phải được thực hiện vào giờ thấp điểm (ví dụ ngoài giờ làm việc).
- Tất cả những truy cập phải được giám sát và ghi nhật ký để tham chiếu khi cần.

V.12 An ninh mạng và truyền thông

V.12.1 Quản lý an ninh mạng

a) Kiểm soát mạng

- Phải thực hiện ghi nhận nhật ký hoạt động mạng, và thực hiện giám sát nhật ký thường xuyên để kịp thời phát hiện các hành động trái phép.
- Việc cấp phát các tài khoản mạng riêng ảo (VPN-Virtual Private Network) để truy cập vào hệ thống mạng PDH & CTTV phải được phê duyệt của Giám đốc Ban CNTT.

b) An ninh dịch vụ mạng

- Các cam kết thỏa thuận dịch vụ mạng phải được thiết lập rõ ràng với nhà cung cấp, nội dung tối thiểu gồm dịch vụ được cung cấp, mức độ dịch vụ, các yêu cầu bảo mật.
- Xác định rõ các thông tin liên lạc của hai bên và quy trình hoặc hướng dẫn các bước phối hợp hỗ trợ dịch vụ hay xử lý sự cố.

c) Tách biệt hệ thống mạng

- Từng nhóm dịch vụ, từng nhóm người sử dụng, và từng nhóm hệ thống thông tin phải được phân tách để hạn chế rủi ro xâm nhập trái phép.
- Phải triển khai các giải pháp/thiết bị để thực hiện cấu hình kiểm soát truy cập giữa các vùng mạng với nhau trên các thiết bị này.

V.12.2 Truyền thông

a) Quy định về truyền tải thông tin

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/09/2024

- Cán bộ nhân viên không được tự ý chuyển tiếp thông tin nhạy cảm hoặc thông tin nội bộ của PDH & CCTV ra bên ngoài.
- Cán bộ nhân viên không được tự ý chuyển tiếp dữ liệu nhạy cảm và dữ liệu nội bộ của PDH & CTTV đến các nơi lưu trữ bên ngoài hệ thống CNTT của PDH & CTTV (ví dụ lưu trữ lên các máy chủ không thuộc là tài sản của PDH & CTTV trên môi trường mạng Internet, các dịch vụ lưu trữ điện toán đám mây không thuộc là tài sản của PDH & CTTV, các thiết bị lưu trữ cá nhân, ...)
- b) Thỏa thuận trong truyền thông
 - Trước khi trao đổi thông tin nhạy cảm của PDH & CTTV với các đối tác bên ngoài, các yêu cầu về bảo mật thông tin phải được xác định và thống nhất với đối tác.
 - Tùy vào cấp độ bảo mật của thông tin mà có yêu cầu bảo mật phù hợp.
 - Nội dung và thành phần tham gia buổi truyền thông phải được ghi nhận đầy đủ.
- c) Thư điện tử (email)
 - Nội dung truyền nhận qua thư điện tử phải được bảo vệ tránh truy cập hoặc chỉnh sửa trái phép.
 - Đảm bảo truyền đến đúng địa chỉ người nhận.
 - Cán bộ nhân viên không được cấu hình tự động chuyển tiếp thư điện tử PDH & CTTV ra thư điện tử bên ngoài.
 - Dữ liệu nhạy cảm của PDH & CTTV gửi kèm qua thư điện tử phải được đặt mật khẩu bảo vệ theo chính sách mật khẩu, hoặc sử dụng các giải pháp đã được PDH phê duyệt.
 - Dữ liệu của PDH & CTTV phải được gửi bằng thư điện tử của PDH & CTTV, không sử dụng thư điện tử bên ngoài vào mục đích công việc của PDH & CTTV.
 - Tất cả thư điện tử của PDH & CTTV phải được lưu trữ lại phục vụ tìm kiếm sau này, và phải được bảo vệ tránh truy cập hay thay đổi trái phép.

V.13 An ninh khi sử dụng các dịch vụ đám mây

V.13.1 Các yêu cầu đối với nhà cung cấp dịch vụ đám mây

- a) Các chứng chỉ và tiêu chuẩn
 - Các nhà cung cấp tuân thủ các tiêu chuẩn và khung kiểm định chất lượng đã được công nhận để thể hiện độ uy tín của nhà cung cấp đó trong ngành. Ví dụ: chứng chỉ như ISO 27001 hoặc chương trình Cyber Essentials Scheme.
- b) Công nghệ
 - Đảm bảo nền tảng (platform) và công nghệ của nhà cung cấp phù hợp với môi trường hiện tại của PDH & CTTV, và luôn tiên phong trong các công nghệ mới (state of the art).
 - Cung cấp các dịch vụ hỗ trợ chuyển đổi sang dịch vụ đám mây.
- c) Quản trị và bảo mật dữ liệu
 - Các nhà cung cấp dịch vụ đám mây phải minh bạch về vị trí đặt trung tâm dữ liệu (data center) của mình.
 - Các nhà cung cấp dịch vụ đám mây phải có khả năng bảo vệ dữ liệu trong quá trình truyền tải thông qua mã hóa dữ liệu di chuyển đến hoặc trong dịch vụ đám mây. Ngoài ra, các vùng dữ liệu được định nghĩa nhạy cảm phải được mã hóa ở trạng thái lưu trữ để hạn chế khả năng truy cập bất thường.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/03/2024

- Các nhà cung cấp dịch vụ đám mây phải có các quy trình về thông báo vi phạm và mất dữ liệu rõ ràng, đồng thời phải đảm bảo các quy trình này phù hợp với mức độ rủi ro cũng như các nghĩa vụ pháp lý hoặc quy định của PDH & CTTV.
- d) Thỏa thuận cấp độ dịch vụ
- Phải chứa 3 thành phần chính:
 - Mục tiêu cấp độ dịch vụ.
 - Chính sách khắc phục và hình phạt/khuyến khích liên quan đến các mục tiêu này.
 - Loại trừ và cảnh báo.

V.13.2 Các biện pháp kiểm soát an ninh

- Tổ chức các buổi đào tạo nâng cao nhận thức ATBMTT cho người dùng cuối.
- Cộng tác với nhà cung cấp dịch vụ đám mây đáng tin cậy.
- Xây dựng các kịch bản khôi phục dữ liệu sau sự cố và lập kế hoạch duy trì liên tục.
- Thường xuyên kiểm tra bảo mật và đánh giá rủi ro.
- Chủ động phát hiện mối đe dọa.

V.14 Mua sắm, phát triển và bảo trì hệ thống CNTT

V.14.1 Các yêu cầu

- a) Đặc tả yêu cầu chung
 - Xác định rõ các yêu cầu về tính bảo mật, toàn vẹn, sẵn sàng của hệ thống.
 - Phải thực hiện các kiểm soát rủi ro ATBMTT.
 - Xác định rõ vai trò và trách nhiệm liên quan đến công tác quản lý ATBMTT.
- b) Đặc tả yêu cầu cho hệ thống phần mềm CNTT
 - Đối với các hệ thống liên quan đến tài khoản khách hàng (nghĩa là khách hàng mở tài khoản để thực hiện giao dịch mua bán bất động sản, tham gia tuyển dụng,...), phải:
 - Thực hiện phân tích các yêu cầu về ATBMTT.
 - Đảm bảo người sử dụng đã được thông báo và chấp nhận các điều khoản và điều kiện về ATBMTT trước khi sử dụng dịch vụ, bao gồm tuyên bố đồng ý bảo mật dữ liệu (Data Privacy Consent Statement).
 - Phải kết hợp xác thực đa nhân tố (từ 02 yếu tố xác thực trở lên).
 - Bảo vệ các giao dịch của dịch vụ ứng dụng CNTT
 - Tất cả thông tin bảo mật của người sử dụng phải được xác thực hợp lệ.
 - Tất cả các thông tin của các bên tham gia giao dịch phải được lưu trữ và bảo vệ.
 - Kênh kết nối mạng giữa các bên tham gia giao dịch phải được mã hóa.
 - Giao thức sử dụng để giao dịch của các bên tham gia phải là giao thức an toàn.
 - Cơ sở dữ liệu của các giao dịch phải được đặt bên trong mạng nội bộ (TTDL/PMC) của PDH & CTTV, trong trường hợp bắt buộc phải đặt bên trong mạng nội bộ của đối tác cung cấp dịch vụ thì phải được phê duyệt của Tổng Giám đốc PDH.

V.14.2 An ninh trong phát triển và hỗ trợ hệ thống CNTT

- a) ATBMTT trong phát triển phần mềm

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/09/2024

- Các yêu cầu về ATBMTT phải được xác định rõ trong giai đoạn thiết kế.
- Xây dựng kế hoạch và thực hiện kiểm tra ATBMTT theo từng cột mốc của dự án.
- Các công cụ, tiện ích để phát triển phần mềm phải có nguồn gốc rõ ràng, không được sử dụng các công cụ, tiện ích đã được biên dịch sẵn mà không có bản quyền.
- Phải xây dựng tài liệu hướng dẫn viết mã nguồn đảm bảo an toàn bảo mật cho từng ngôn ngữ lập trình được sử dụng để phát triển.
- Nếu là dự án phần mềm thuê ngoài, Ban CNTT phải yêu cầu đối tác đáp ứng các nội dung quy định ở mục này để tuân thủ.
- b) Kiểm soát thay đổi hệ thống
 - Thực hiện theo quy định tại mục V.11.1.b) của tài liệu này
 - c) Rà soát kỹ thuật cho phần mềm ứng dụng sau khi có thay đổi nền tảng vận hành
 - Phải thực hiện rà soát kỹ thuật các ứng dụng phần mềm để kiểm tra ảnh hưởng đến hoạt động kinh doanh của việc cập nhật, thay đổi hệ điều hành hay nền tảng hệ thống.
- d) Cập nhật phần mềm
 - Phần mềm đang vận hành chỉ được cập nhật thay đổi khi:
 - Nhà cung cấp dịch vụ hoặc đơn vị phát triển phần mềm đồng ý việc cập nhật.
 - Chức năng cần sử dụng có trong phiên bản cập nhật.
 - Phiên bản cập nhật phải tương thích với các phần mềm và hệ thống hiện có.
- e) Nguyên tắc kỹ thuật an toàn hệ thống
 - ATBMTT phải được thiết kế trong tất cả các lớp của kiến trúc phần mềm, ví dụ như lớp nghiệp vụ (business), lớp dữ liệu (data), lớp giao tiếp (presentation).
 - Đảm bảo các nguyên tắc kỹ thuật ATBMTT trong phát triển phần mềm phải được rà soát và cập nhật thường xuyên.
- f) Môi trường phát triển an toàn
 - Môi trường phát triển và tích hợp hệ thống phải được đảm bảo an toàn bảo mật trong suốt vòng đời của dự án.
 - Việc thiết lập bảo mật cho môi trường phát triển phải dựa trên các yếu tố sau:
 - Mức độ nhạy cảm của dữ liệu được xử lý, lưu trữ và truyền tải qua hệ thống đó.
 - Các yêu cầu nếu có của các bên liên quan (ví dụ như các cam kết, luật pháp,...).
 - Những kiểm soát bảo mật đã triển khai.
 - Mức độ thuê ngoài của dự án.
- g) Giám sát việc thuê bên ngoài để phát triển hệ thống phần mềm
 - Để đảm bảo hệ thống phần mềm hoạt động đúng như mong đợi, và đáp ứng các yêu cầu về ATBMTT của PDH & CTTV, các kiểm soát sau đây phải được thực hiện:
 - Tất cả thành phần được sử dụng cho việc vận hành hệ thống trong tương lai phải có đầy đủ bản quyền (trừ khi sử dụng mã nguồn mở không yêu cầu bản quyền).
 - Các yêu cầu ở mục V.14.2 a) của tài liệu này phải được đưa vào thỏa thuận hợp đồng với đối tác cung cấp phần mềm.
- h) Kiểm thử ATBMTT

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/09/2024

- Tất cả các thay đổi hoặc cập nhật hệ thống phải thực hiện kiểm thử trong suốt quy trình phát triển.
- Phải thực hiện kiểm thử ATBMTT và có biên bản ghi nhận trước khi chấp nhận hệ thống (kể cả hệ thống tự phát triển và thuê ngoài).
 - i) User Acceptance Test (UAT)
- Phải thực hiện kiểm thử chấp nhận hệ thống và có biên bản ghi nhận (kể cả hệ thống tự phát triển và thuê ngoài). Việc kiểm thử tối thiểu phải bao gồm các nội dung sau:
 - Các chức năng theo yêu cầu của dự án.
 - Các yêu cầu về hiệu năng hệ thống.
 - Đảm bảo việc cài đặt hệ thống mới sẽ không ảnh hưởng xấu đến các hệ thống hiện tại, đặc biệt vào các giờ cao điểm.

V.14.3 Dữ liệu kiểm thử

- Dữ liệu sử dụng để kiểm thử phải được bảo vệ giống như bảo vệ dữ liệu trong hệ thống đang vận hành.
- Không được sử dụng những dữ liệu cá nhân và các dữ liệu nhạy cảm từ hệ thống đang vận hành của PDH & CTTV vào mục đích kiểm thử.
- Việc trích xuất dữ liệu từ hệ thống đang vận hành phục vụ mục đích kiểm thử phải được phê duyệt của Tổng Giám đốc PDH, và phải ghi nhận lại lịch sử trích xuất.
- Dữ liệu được lấy từ môi trường vận hành phải được xóa khỏi môi trường thử nghiệm sau khi việc kiểm thử hoàn thành.

V.15 Quản lý mối quan hệ nhà cung cấp

V.15.1 ATBMTT trong quản lý mối quan hệ nhà cung cấp

- a) Quy định ATBMTT trong quản lý mối quan hệ nhà cung cấp
 - Phải xác định rõ các nhóm nhà cung cấp nào được phép truy cập thông tin của PDH & CTTV (ví dụ: dịch vụ IT, dịch vụ tài chính, dịch vụ hạ tầng,...).
 - Phải xác định rõ các kiểu truy cập thông tin cho các nhóm nhà cung cấp khác nhau được truy cập, cùng giải pháp kiểm soát và giám sát.
 - Xây dựng hướng dẫn xử lý sự cố liên quan đến truy cập của nhà cung cấp, bao gồm cả trách nhiệm phía nhà cung cấp và trách nhiệm phía PDH & CTTV.
- b) Nội dung ATBMTT trong các thỏa thuận hoặc hợp đồng với nhà cung cấp
 - Các yêu cầu về ATBMTT liên quan đến việc truy cập, lưu trữ, xử lý tài sản thông tin của PDH & CTTV phải được lập thành tài liệu và được thỏa thuận cam kết giữa hai bên.
 - Nội dung các điều khoản thỏa thuận tối thiểu bao gồm:
 - Mô tả rõ thông tin được phép truy cập và phương thức truy cập.
 - Phân loại cấp độ bảo mật của thông tin được phép truy cập theo mục V.7.2 của tài liệu này.
 - Thông tin liên lạc của những người có trách nhiệm hỗ trợ kỹ thuật hoặc xử lý sự cố ATBMTT.
 - Các cam kết thỏa thuận dịch vụ phải được thiết lập rõ ràng với nhà cung cấp, nội dung tối thiểu gồm dịch vụ được cung cấp, mức độ dịch vụ.
 - Các cam kết bảo mật thông tin.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: <u>26/03/2024</u>

c) Chuỗi cung ứng CNTT

- Phải xác định rõ các yêu cầu về ATBMTT để áp dụng vào việc mua sắm các sản phẩm hay dịch vụ CNTT.
- Nội dung các yêu cầu về ATBMTT này tối thiểu gồm:
 - Đối với các dịch vụ CNTT, yêu cầu các nhà cung cấp có trách nhiệm phổ biến các yêu cầu về ATBMTT của PDH đến với các nhà cung cấp phụ trong chuỗi cung ứng (nếu có).
 - Hướng dẫn giám sát, kiểm soát để xác nhận sản phẩm hoặc dịch vụ chuyển giao đáp ứng các yêu cầu về ATBMTT.
 - Sản phẩm chuyển giao phải đáp ứng các chức năng theo yêu cầu, và không có tính năng dư thừa không mong muốn.

V.15.2 Quản lý chuyển giao dịch vụ với nhà cung cấp

a) Giám sát chuyển giao dịch vụ với nhà cung cấp

- Giao trách nhiệm cho cá nhân giám sát, kiểm soát dịch vụ nhà cung cấp.
- Phải theo dõi mức độ thực hiện dịch vụ để xác định sự tuân thủ các thỏa thuận đã ký.
- Đánh giá các báo cáo về dịch vụ do nhà cung cấp gửi.

b) Quản lý thay đổi dịch vụ nhà cung cấp

- Việc thay đổi dịch vụ được cung cấp bởi nhà cung cấp phải đánh giá mức độ quan trọng của các hệ thống CNTT, các quy trình liên quan và các kết quả đánh giá rủi ro.
- Công tác ATBMTT liên quan đến quản lý thay đổi dịch vụ của nhà cung cấp gồm có:
 - Đánh giá và cập nhật đánh giá rủi ro, mối đe dọa để xác định tác động lên các kiểm soát bảo mật.
 - Triển khai các biện pháp kiểm soát ATBMTT mới khi xác định các lỗ hổng trong kết quả đánh giá rủi ro.

V.16 Quản lý sự cố ATBMTT

V.16.1 Quy trình và trách nhiệm

- Phải có tài liệu về quy trình quản lý sự cố an ninh thông tin. Quy trình phải quy định rõ trách nhiệm để đảm bảo có thể phản ứng nhanh, hiệu quả, theo đúng trình tự khi xảy ra sự cố ATBMTT.
- Phải giám sát, dò tìm, phân tích, và báo cáo các sự kiện và sự cố ATBMTT.
- Phải ghi nhận nhật ký hoạt động xử lý sự cố.
- Phải thực hiện đánh giá các sự kiện và điểm yếu ATBMTT.

V.16.2 Thông báo các sự kiện về ATBMTT

- Tất cả cán bộ nhân viên PDH & CTTV có sử dụng hệ thống CNTT phải có trách nhiệm thông báo khi phát hiện các sự kiện ATBMTT về BP HT&BM – Ban CNTT.
- Các sự kiện phải thông báo bao gồm nhưng không giới hạn như:
 - Kiểm soát ATBMTT không hoạt động đúng chức năng.
 - Phát hiện vi phạm tính bảo mật, toàn vẹn, sẵn sàng của thông tin.
 - Phát hiện vi phạm chính sách, quy định, quy trình, hướng dẫn ATBMTT đã ban hành.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: <u>26/03/2024</u>

- Phát hiện những thay đổi hệ thống chưa được phê duyệt.
- Phát hiện trường hợp cài đặt phần mềm hay phần cứng trái phép vào các thiết bị, máy tính của PDH & CTTV.
- Phát hiện truy cập trái phép vào hệ thống CNTT PDH & CTTV.
- Phát hiện máy tính bị nhiễm mã độc.
- Phát hiện tài sản thông tin bị mất, bị đánh cắp hoặc bị mã hóa trái phép.

V.16.3 Báo cáo điểm yếu ATBMTT

- Cán bộ nhân viên PDH & CTTV đang sử dụng hệ thống CNTT phải ghi nhận và báo cáo tất cả điểm yếu ATBMTT được phát hiện cho trưởng đơn vị của mình.
- Nghiêm cấm mọi trường hợp cố ý khai thác các điểm yếu ATBMTT khi chưa được phê duyệt của Tổng Giám đốc PDH.

V.16.4 Đánh giá và ra quyết định các sự kiện ATBMTT

- Tất cả sự kiện ATBMTT phải được đánh giá nhằm xác định có phải là sự cố ATBMTT hay không.
- Kết quả đánh giá phải được ghi chép chi tiết để phục vụ truy vấn, kiểm soát trong tương lai.

V.16.5 Phản ứng lại các sự cố ATBMTT

- Các sự cố ATBMTT phải được xem xét xử lý. Trong trường hợp có nhiều sự cố ATBMTT xảy ra cùng lúc, phải đánh giá và xử lý các sự cố có mức độ rủi ro cao hơn.
- Quá trình xử lý các sự cố ATBMTT tối thiểu gồm những việc sau:
 - Thu thập các chứng cứ càng sớm càng tốt sau khi sự cố xảy ra.
 - Báo cáo qua các cấp liên quan (nếu cần thiết).
 - Đảm bảo các hoạt động xử lý sự cố phải được ghi nhật ký đầy đủ nhằm phục vụ việc phân tích về sau.
 - Thông báo sự cố và kết quả khắc phục, cũng như ảnh hưởng của sự cố gây ra cho các bên liên quan nắm thông tin.
 - Xử lý các điểm yếu ATBMTT trực tiếp hoặc gián tiếp góp phần gây sự cố này.

V.16.6 Rút kinh nghiệm từ các sự cố ATBMTT đã xảy ra

- Kiến thức có được từ việc phân tích và giải quyết thành công sự cố phải được ghi nhận lại để sử dụng vào mục đích giảm thiểu khả năng xảy ra hoặc giảm ảnh hưởng của sự cố trong tương lai.
- Phải giám sát và đánh giá các sự cố ATBMTT như:
 - Thực hiện phân tích thống kê về tần suất sự cố, loại sự cố, vị trí xảy ra sự cố để xác định xu hướng của sự cố.
 - Sử dụng các thông tin ghi nhận sự cố và xu hướng sự cố để liên tục cải tiến các quy định, quy trình, đào tạo nhận thức ATBMTT.
 - Đánh giá tính hiệu quả của các công nghệ bảo mật thông tin đã triển khai

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH AN TOÀN BẢO MẬT THÔNG TIN	Lần ban hành: 01 Ngày hiệu lực: 26/09/2024

V.16.7 Thu thập bằng chứng

- Bằng chứng thu thập trong quá trình điều tra sự cố phải được bảo vệ an toàn tránh bị truy cập hoặc sửa xóa trái phép, đảm bảo chứng đáng tin cậy để có thể sử dụng trong việc xử lý kỷ luật.
- Bằng chứng chỉ có thể được thu thập bởi những cá nhân được Giám đốc Ban CNTT chỉ định.

V.17 ATBMTT trong quản lý hoạt động liên tục của hệ thống CNTT

V.17.1 ATBMTT liên tục

a) Kế hoạch cho ATBMTT liên tục

- Các yêu cầu về ATBMTT cần phải được xác định khi xây dựng kế hoạch cho hoạt động liên tục hệ thống CNTT và phục hồi sau thảm họa.

b) Thực hiện ATBMTT liên tục

- Ban CNTT có trách nhiệm xây dựng, thực hiện và duy trì các quy trình, kiểm soát ATBMTT trong hoạt động phục hồi sau thảm họa nhằm đáp ứng yêu cầu ATBMTT liên tục cho những tình huống không mong muốn xảy ra.
- Phải triển khai các kiểm soát bổ sung cho những kiểm soát ATBMTT đã bị ảnh hưởng không thể duy trì sau khi xảy ra các tình huống bất lợi.

c) Xác minh, rà soát và đánh giá ATBMTT liên tục

- Ban CNTT phải định kỳ tối thiểu mỗi năm một lần thực hiện diễn tập theo các quy trình ATBMTT liên tục đã ban hành.

V.17.2 Dự phòng

- Hệ thống CNTT phải được triển khai với mức độ dự phòng đủ đáp ứng các yêu cầu về tính sẵn sàng.
- Ban CNTT phải làm việc với các đơn vị nghiệp vụ để xác định các yêu cầu cho tính sẵn của hệ thống CNTT.
- Nếu kiến trúc hệ thống hiện có không đảm bảo được tính sẵn sàng theo yêu cầu, thì các thành phần hoặc kiến trúc dự phòng phải được xem xét để triển khai.

V.18 Tuân thủ

V.18.1 Tuân thủ các yêu cầu của pháp luật và các hợp đồng đã ký

a) Xác định các quy định pháp luật và các cam kết đã ký mà PDH & CTTV cần tuân thủ

- Ban CNTT có trách nhiệm đảm bảo các quy định, chính sách, yêu cầu hợp đồng của mỗi hệ thống CNTT phải được nhận diện và tài liệu hóa trước khi bắt đầu công việc phát triển hay cải tiến.

b) Quyền sở hữu trí tuệ

- Phải thiết lập các kiểm soát để đảm bảo tuân thủ các yêu cầu pháp luật, các cam kết hợp đồng đã ký liên quan đến quyền sở hữu trí tuệ hay giấy phép sử dụng phần mềm.
- Chỉ được mua phần mềm từ các nhà cung cấp uy tín.
- Tất cả bằng chứng về quyền sử dụng hoặc quyền sở hữu phải được bảo quản và duy trì.

 PHAT DAT HOLDINGS	CÔNG TY TNHH PHÁT ĐẠT HOLDINGS	Mã số: PDH-CNTT-CS01
	CHÍNH SÁCH	Lần ban hành: 01
	AN TOÀN BẢO MẬT THÔNG TIN	Ngày hiệu lực: 26/03/2024

- Phải triển khai các kiểm soát để đảm bảo không bị vượt quá số lượng người dùng được phép sử dụng sản phẩm theo giấy phép đã cấp cho PDH & CTTV.
- Phải thực hiện kiểm soát để đảm bảo chỉ có những phần mềm có giấy phép sử dụng mới được cài đặt vào các máy tính của PDH & CTTV.

c) Bảo vệ hồ sơ

- Các đơn vị được phân công quản lý hồ sơ của PDH & CTTV phải có trách nhiệm bảo vệ tránh thất lạc, phá hủy, truy cập trái phép vào các hồ sơ này. Đảm bảo tuân thủ các thỏa thuận hợp đồng đã ký.

d) Bảo vệ thông tin và dữ liệu cá nhân

- Bảo vệ dữ liệu và tính riêng tư của các thông tin cá nhân cần phải tuân thủ các yêu cầu quy định trong luật định, quy định của các cơ quan Nhà nước, và các điều khoản trong các hợp đồng mà PDH & CTTV đã ký kết với nhân viên, khách hàng và đối tác.
- Tất cả cán bộ nhân viên của PDH & CTTV làm việc liên quan đến thông tin cá nhân cần phải nắm rõ các yêu cầu về bảo vệ dữ liệu của PDH & CTTV, và đảm bảo thực hiện các yêu cầu của Chính sách ATBMTT.

V.18.2 Rà soát công tác ATBMTT

a) Kiểm soát đánh giá về công tác ATBMTT

- Công tác kiểm toán nội bộ về CNTT phải được thực hiện tối thiểu mỗi năm 01 lần.
- Giám đốc Ban CNTT có trách nhiệm chính để giải quyết các điểm yếu, và các kiểm soát chưa tuân thủ được nêu ra trong các báo cáo kiểm toán nội bộ CNTT.

b) Tuân thủ các chính sách, quy định ATBMTT

- Các Trưởng đơn vị có trách nhiệm rà soát, kiểm tra đảm bảo các quy trình ATBMTT liên quan đến công việc của mình phải tuân thủ các quy định ATBMTT đã ban hành.
- Trong quá trình kiểm tra, đánh giá phát hiện chưa tuân thủ, Ban CNTT phải thực hiện:
 - Xác định nguyên nhân.
 - Đánh giá các mối đe dọa và rủi ro đối với các nội dung chưa tuân thủ.
 - Thực hiện hành động khắc phục.

c) Rà soát tuân thủ mặt kỹ thuật

- Ban CNTT phải thực hiện kiểm tra kỹ thuật định kỳ tối thiểu 06 tháng một lần bằng cách thực hiện các công việc sau:
 - Rà quét phát hiện xâm nhập hệ thống mạng.
 - Đánh giá lỗ hổng bảo mật và thực hiện xâm nhập thử (penetration testing) vào hệ thống.
 - Kiểm tra nhằm đảm bảo các biện pháp kiểm soát kỹ thuật đã triển khai đang hoạt động đúng chức năng.
- Ban CNTT có trách nhiệm thực hiện khắc phục các lỗ hổng được phát hiện trong quá trình kiểm tra rà soát.

Nơi nhận :

- Email: Toàn thể nhân viên PDH, Chủ tịch/TGD CTTV.
- Lưu trữ: Bản gốc (Ban CNTT), file scan (sharepoint)