TECHVFY
Empower your digital innovation

QUY TRÌNH

BẢO MẬT THÔNG TIN

Mã tài liệu	**01v-QT/ISM/HDCV**
Phiên bản	**1.0**
Ngày sửa đổi	**15/04/2021**

LỊCH SỬ THAY ĐỔI					
Ngày cập nhật	**Phiên bản**	**Nội dung cập nhật**	**Người phê duyệt**	**Người đánh giá**	**Người cập nhật**
15/04/2021	1.0	Tạo mới	Hieu Nguyen	Lou Nguyen	Nguyen Duc Linh
15/07/2024	1.0	Cập	Hieu Nguyen	Nguyen Duc Linh	Nguyen Duc Linh

Mục Lục

1. MỤC ĐÍCH

Quy trình 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

Quy trình này dành cho đối tượng là toàn bộ nhân viên của công ty.

3. ĐỊNH NGHĨA THUẬT NGỮ

Định nghĩa thuật ngữ thì tuân theo "**ISO 27001: 2013**"

Định nghĩa thuật ngữ chính như sau:

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 bảo mật thông tin	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.
Tổ chức	Công ty Cổ phần TECHVIFY Việt Nam
Nhân viên	Người lao động của công ty TECHVIFY

4. CẤU TRÚC CỦA TÀI LIỆU NÀY

Bản quy trình này được xây dựng dựa vào thể chế của **"ISO 27001: 2013 - Phụ lục A"**.

5. CHÍNH SÁCH BẢO MẬT THÔNG TIN

5.1 PHƯƠNG HƯỚNG CỦA ĐỘI NGŨ QUẢN LÝ TRONG BẢO MẬT THÔNG TIN

5.1.1 CHÍNH SÁCH BẢO MẬT THÔNG TIN

a) Ban bảo mật thông tin sẽ định nghĩa Chính sách liên quan đến bảo mật thông tin trong **"Chính sách bảo mật thông tin"** và lấy chấp thuận của Tổng Giám đốc.

Ngoài ra, Ban bảo mật thông tin sẽ công bố Chính sách bảo mật thông tin đến toàn thể nhân viên là đối tượng, phạm vi áp dụng Chính sách này. **"Chính sách bảo mật thông tin"** của công ty cũng sẽ được công bố với các cơ quan liên quan ở bên ngoài.

b) Bên cạnh **"Chính sách bảo mật thông tin",** ban bảo mật thông tin sẽ quy định những Chính sách để bảo mật thông tin khác tại bản quy trình này. Bao gồm:

1) Chính sách sử dụng thiết bị di động
2) Chính sách làm việc tại nhà
3) Chính sách kiểm soát đăng nhập.
4) Chính sách sử dụng kiểm soát mã hóa.
5) Chính sách màn hình/bàn làm việc gọn gàng
6) Chính sách (và quy trình) chuyển tiếp thông tin
7) Chính sách phát triển đảm bảo đến bảo mật
8) Chính sách bảo mật thông tin liên quan đến nhà cung cấp.

5.1.2 XEM XÉT NHỮNG CHÍNH SÁCH ĐỂ BẢO MẬT THÔNG TIN

Ban bảo mật thông tin sẽ xem xét lại Chính sách liên quan đến bảo mật thông tin như "Chính sách bảo mật thông tin",v.v…1 năm 1 lần, hoặc khi phát sinh thay đổi nghiêm trọng. Trường hợp đã thực hiện chỉnh sửa Chính sách liên quan đến bảo mật thông tin chẳng hạn như **"Chính sách bảo mật thông tin"** thì sẽ phải nhận được đồng thuận của Tổng Giám đốc.

6. TỔ CHỨC ĐỂ BẢO MẬT THÔNG TIN

6.1 TỔ CHỨC NỘI BỘ

6.1.1 VAI TRÒ VÀ TRÁCH NHIỆM CỦA BẢO MẬT THÔNG TIN

Lãnh đạo cấp cao nhất sẽ phân trách nhiệm và quyền hạn liên quan đến bảo mật thông tin cho ban ISMS, cho người chịu trách nhiệm đánh giá nội bộ, như sau.

Ngoài ra, Lãnh đạo cấp cao nhất sẽ truyền đạt những vai trò, trách nhiệm và quyền hạn này cho các nhân viên trong công ty.

Khi vận hành ISMS, lãnh đạo cấp cao nhất sẽ lập ra và điều hành hội đồng ISMS. Sơ đồ tổ chức được trình bày trong văn bản "***Sơ đồ tổ chức***".

Vai trò của các thành viên trong ban ISMS như sau:

a) Lập kế hoạch ứng phó rủi ro ISMS
b) Xây dựng ban để thực hiện ISMS
c) Thực hiện chính sách quản lý đã lập.
d) Đào tạo/ huấn luyện

e) Quản lý việc vận hành

f) Quản lý tài nguyên kinh doanh

g) Quản lý sự kiện/ sự cố bảo mật thông tin

h) Liên lạc với các cơ quan liên quan (cảnh sát, cơ quan kiểm tra, công ty tư vấn, đối tác, nơi ủy thác v.v.)

1) Thành viên ban ISMS

Chức vụ	**Vai trò**
Ban điều hành (CEO)	CEO xem xét, phê duyệt các chính sách, hỗ trợ ban ISM trong việc vận hành và triển khai các hệ thống, hoạt động liên quan đến bảo mật thông tin trong doanh nghiệp.
Trưởng ban ISM	Quản lý bao quát từ thực hiện, vận hành hệ thống quản lý ISMS. Lên kế hoạch triển khai các hoạt động liên quan đến bảo mật thông tin trong công ty.
Người chịu trách nhiệm đào tạo ISMS	Lập kế hoạch đào tạo ISMS và thực hiện triển khai. Báo cáo kết quả với trưởng phòng khi được yêu cầu (có thể làm việc vs bộ phận đào tạo để quản lý việc đào tạo trong công ty). ISM sẽ chịu trách nhiệm lập kế hoạch đào tạo về ISM và phòng đào tạo của công ty sẽ thực hiện triển khai kế hoạch đào tạo từ phòng ISM đến nhân viên.
Người chịu trách nhiệm hệ thống thông tin	Là người quản lý hệ thống thông tin, tuân theo các quy trình/ quy tắc liên quan đến quản lý hệ thống thông tin, thực hiện các đối sách quản lý an toàn để duy trì hệ thống quản lý ISM.
Người chịu trách nhiệm xử lý các sự cố ISMS	Là người quản lý và chịu trách nhiệm xử lý các sự cố Bảo mật thông tin theo quy định của công ty. Việc xử lý phải đảm bảo nhanh chóng, hạn chế tối đa các thiệt hại cho tổ chức và các bên liên quan.
Người chịu trách nhiệm quản lý tài liệu	Quản lý, duy trì các tài liệu và ghi chép lại các bản ghi liên quan tới hệ thống quản lý ISMS.

2) Người chịu trách nhiệm đánh giá nội bộ ISMS

Chịu trách nhiệm báo cáo với trưởng ban về kết quả kiểm soát (Đánh giá nội bộ) đối với tất cả các nhóm trực thuộc công ty.

6.1.2 PHÂN CÔNG NHIỆM VỤ

a) Công ty sẽ phân tách giữa người chịu trách nhiệm khởi tạo, người thực hiện và người phê duyệt.
b) Trường hợp buộc phải kiêm nhiệm do giới hạn về mặt thành viên, thì có thể kiêm nhiệm với điều kiện là phải được giám sát.

6.1.3 LIÊN LẠC VỚI CÁC TỔ CHỨC CÓ THẨM QUYỀN

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

6.1.4 LIÊN LẠC VỚI TỔ CHỨC CÓ CHUYÊN MÔN

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

6.1.5 BẢO MẬT THÔNG TIN TRONG QUẢN LÝ DỰ ÁN

a) Người quản lý dự án sẽ xác định kiểm soát cần thiết cho dự án.
b) Kiểm soát cần thiết cho dự án cũng sẽ được cân nhắc cả sau khi kết thúc dự án.
c) Người quản lý dự án sẽ bổ nhiệm người chịu trách nhiệm về bảo mật thông tin.

6.2 THIẾT BỊ DI ĐỘNG VÀ LÀM VIỆC TỪ XA

6.2.1 CHÍNH SÁCH SỬ DỤNG THIẾT BỊ DI ĐỘNG

a) Trường hợp mang thiết bị di động ra ngoài công ty thì nguyên tắc là không được phép lưu file chứa thông tin mật, thông tin cá nhân, v. v... vào thiết bị di động. Trường hợp bắt buộc phải lưu thì bảo vệ thiết bị di động và tài liệu bằng mật khẩu.
b) Trường hợp kết nối thiết bị di động với internet thì sử dụng thiết bị kết nối mượn từ công ty. Không được kết nối đến điểm phát Wifi miễn phí mà không bị giới hạn người sử dụng.

6.2.2 LÀM VIỆC TỪ XA

a) Làm việc tại nhà có thể thực hiện chỉ khi đã có sự phê duyệt của trưởng ban bảo mật thông tin.
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.

c) Máy tính sử dụng cho làm việc tại nhà phải cài đặt phần mềm diệt virus, và thiết lập theo 12.2.1.

d) Không được cài đặt phần mềm không cho phép được định nghĩa trọng tài liệu "**Standard_Whitelist-Blacklist_Software**".

7. AN TOÀN NGUỒN NHÂN LỰC

7.1 TRƯỚC KHI TUYỂN DỤNG

7.1.1 THẨM TRA

Thực hiện quy trình tìm kiếm ứng viên, tuyển dụng sau khi cân nhắc những điểm dưới đây.

a) Đánh giá độ thích hợp với các mục yêu cầu về mặt nghiệp vụ từ hồ sơ lý lịch, rồi tiến hành tuyển chọn.

b) Đánh giá quan điểm đạo đức từ thái độ, cách dùng từ ngữ… khi phỏng vấn và tiến hành tuyển chọn.

c) Khi tuyển dụng cấp quản lý hay giám đốc, với sự đồng thuận của bản thân người đó, sẽ thực hiện điều tra chi tiết hơn như thông tin tín dụng trong quá khứ…

7.1.2 ĐIỀU KIỆN TUYỂN DỤNG

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.

7.2 TRONG THỜI GIAN TUYỂN DỤNG

7.2.1 TRÁCH NHIỆM CỦA BAN QUẢN LÝ

Tổng Giám đốc sẽ yêu cầu toàn bộ nhân viên trong phạm vi áp dụng tuân thủ các mục yêu cầu về Chính sách bảo mật thông tin, quy trình bảo mật thông tin và các yêu cầu khác liên quan về bảo mật thông tin.

7.2.2 NÂNG CAO Ý THỨC, ĐÀO TẠO VÀ HUẤN LUYỆN VỀ BẢO MẬT THÔNG TIN

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

b) Việc nâng cao ý thức về bảo mật thông tin, huấn luyện và đào tạo được quy định trong **Điều 7 – Quy định_Bảo mật thông tin**

7.2.3 HÌNH THỨC KHIỂN TRÁCH

Trường hợp người lao động vô tình hoặc cố ý làm rò rỉ thông tin, hoặc trường hợp vi phạm các mục tuân thủ bảo mật thông tin, thì chiếu theo quy tắc lao động, sẽ bị coi là đối tượng khiển trách.

Các hình thức khiển trách được quy định cụ thể tại tài liệu **"Quy định_Bảo mật thông tin".**

7.3 CHẤM DỨT VÀ THUYÊN CHUYỂN CÔNG VIỆC

7.3.1 TRÁCH NHIỆM VỀ CHẤM DỨT VÀ THUYÊN CHUYỂN CÔNG VIỆC

Trong cam kết bảo mật thông tin cần có điều khoản quy định nghĩa vụ bảo mật thông tin trong một thời gian nhất định sau khi kết thúc hợp đồng lao động hoặc thay đổi công việc.

8. QUẢN LÝ TÀI SẢN

8.1 TRÁCH NHIỆM ĐỐI VỚI TÀI SẢN

8.1.1 DANH MỤC TÀI SẢN

Ban bảo mật thông tin sẽ lập Danh mục tài sản để nhận biết tài sản quan trọng trong công ty. Ngoài ra, sẽ xem xét lại Danh mục tài sản dựa vào Bảng kế hoạch ISMS trong năm ít nhất 1 năm 1 lần.

8.1.2 TRÁCH NHIỆM QUẢN LÝ TÀI SẢN

Đối với tài sản đặc thù đã xác định tại **Danh mục tài sản**, ban bảo mật thông tin sẽ làm rõ trách nhiệm quản lý bằng cách ghi chú người chịu trách nhiệm quản lý trên cùng danh mục.

8.1.3 PHẠM VI CHO PHÉP SỬ DỤNG TÀI SẢN

Mặt khác, sẽ làm rõ phạm vi cho phép sử dụng của tài sản thông tin trong phần thiết llập quyền truy cập.

8.1.4 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.

a) Thu hồi danh thiếp, thẻ nhân viên, ID card

b) Thu hồi máy tính cá nhân và điện thoại di động mà công ty đã cấp.

c) Thu hồi hoặc hủy hồ sơ lưu trên giấy.

8.2 PHÂN LOẠI THÔNG TIN

8.2.1 PHÂN LOẠI THÔNG TIN

Thông tin thì phân chia thành thông tin công khai (Public), thông tin sử dụng nội bộ (Internal Use), thông tin bảo mật (Confidential) và thông tin tối mất (Top Secret). Ban bảo mật thông tin sẽ xem lại phân loại của thông tin ít nhất 1 lần 1 năm.

STT	Phân loại	Nội dung
1	Public	Trừ những trường hợp dưới đây
2	Internal Use/Nội Bộ	Là những mục ngoài thông tin mật của những người liên quan, thông tin mật, và chỉ cho phép công khai đối với nhân viên của công ty (loại trừ những thông tin cần phải công khai cho khách hàng). Hoặc quy định, quy trình.
3	Confidential/ Mât	Là những thông tin mà khi bị rò rỉ sẽ có rủi ro khiến công ty bị thiệt hại lớn, hoặc là có thể chịu những bất lợi, là những thông tin chỉ được phép công khai với người có liên quan. Trường hợp chưa quyết định rõ ràng người có liên quan, thì người có liên quan là những người trực tiếp tiếp nhận thông tin.
4	Top Secret/Tuyêt Mật	Là những thông tin mà việc tiết lộ hoặc công bố sai đối tượng hoặc không đúng thẩm quyền sẽ làm ảnh hưởng đặc biệt nghiêm trọng đến tài chính, pháp lý hoặc hình ảnh của Công ty.

8.2.2 GẮN NHÃN THÔNG TIN

Người lao động phải nhận biết xem thông tin sử dụng có tương ứng với cái nào trong số các phân loại Public (Thông tin thường), Internal use/Nôi bộ ((Thông tin sử dụng nội bộ), Confidential/Mât (Thông tin bảo mật-chỉ dành cho những người liên quan), Top secret/Tuyêt mât(Thông tin chỉ do CEO chỉ định người được truy câp). Trường hợp không thể nhận biết được một cách dễ dàng, thì yêu cầu ban ISMS hỗ trợ.

8.2.3 XỬ LÝ THÔNG TIN

Dưới đây là những quy tắc khi xử lý đối với mỗi loại thông tin.

[Trường hợp văn bản, thiết bị lưu trữ]

STT	Phân Loại quản lý	Thông tin tuyệt mật	Thông tin mật	Thông tin lưu hành nội bộ	Thông tin công khai
1	Nhãn hiển thị	Ủy thác cho người chịu trách nhiệm	Ủy thác cho người chịu trách nhiệm	Ủy thác cho người chịu trách nhiệm	Không cần thiết
2	Người sử dụng	Giới hạn cán bộ quản lý/ lãnh đạo	Nhân viên trực thuộc bộ phận/dự án liên quan	Người lao động của tổ chức này	Ai cũng có thể
3	Phân phối lại	Giới hạn cán bộ quản lý/ lãnh đạo	Giới hạn trong bộ phận/dự án liên quan	Giới hạn trong nội bộ công ty	Không cần cân nhắc đặc biệt
4	Nơi bảo quản	Nơi đã được khóa	Nơi đã được khóa	Ủy thác cho người chịu trách nhiệm	
5	Sử dụng máy copy	Chỉ những người cần thiết	Chỉ những người cần thiết	Giới hạn trong nội bộ công ty	
6	Gửi Fax	Cấm	Giới hạn trong bộ phận/dự án liên quan	Giới hạn trong nội bộ công ty	
7	Sử dụng mặt sau (Ghi chú 1)	Cấm	Cấm	Cấm	
8	Chuyển ra ngoài công ty	Xử lý sao cho không thể nhìn xuyên được nội dung (Ghi chú 2)			
9	Mang ra ngoài công ty	Chỉ người đã được phép của người chịu trách nhiệm (Ghi chú 3)			
10	Hủy bỏ văn bản (Ghi chú 4)	Một trong những biện pháp như hủy tài liệu, đốt, tan chảy	Một trong những biện pháp như hủy tài liệu, đốt, tan chảy	Ủy thác cho người chịu trách nhiệm	
11	Xử lý hủy bỏ (Thiết bị lưu trữ)	Hủy bỏ nội dung trước khi hủy bỏ, tái sử dụng			

Ghi chú 1: Không sử dụng lại tài liệu có ghi thông tin cá nhân

Ghi chú 2: Để giảm nguy cơ làm mất, gửi nhầm xuống mức tối thiểu, thì khi gửi những thông tin cá nhân được ghi trên giấy hay thẻ nhớ bằng đường bưu điện hay gửi về nhà, cần phải chọn những phương thức vận chuyển như thùng thư có khóa, xác nhận giao nhận.

Ghi chú 3: Khi mang thông tin cá nhân ra bên ngoài, phải chú ý không được bỏ trên xe, không rời khỏi tay, không đến những địa điểm khác ngoài nơi phải đến để chuyển giao thông tin.

Ghi chú 4: Việc hủy bỏ thông tin cá nhân được ghi trong giấy phải được xử lý bằng máy hủy giấy hay làm tan chảy. Ngoài ra, để phòng tránh làm mất hay mất trộm từ nơi lưu tạm thời trước khi hủy bỏ thì tài liệu quan trọng sẽ cần được hủy bỏ ngay lập tức.

[Thông tin trong hệ thống]

STT	Phân loại quản lý	Top secret	Confidential	Internal Use	Public
1	Kiểm soát truy cập	Giới hạn truy cập cho Lãnh đạo, cán bộ quản lý được ủy thác	Kiểm soát truy cập mỗi cá nhân, hoặc nhóm	Ủy thác cho người chịu trách nhiệm	Không cần cân nhắc
2	Lưu vào máy tính cá nhân	Ủy thác cho người chịu trách nhiệm	Ủy thác cho người chịu trách nhiệm	Ủy thác cho người chịu trách nhiệm	
3	Lưu trữ vào server	Giới hạn truy cập	Giới hạn truy cập	Ủy thác cho người chịu trách nhiệm	
4	Copy (Ghi chú 1)	Giới hạn sao chép	Quản lý sao chép	Ủy thác cho người chịu trách nhiệm	
5	Thư điện tử	Cài mật khẩu vào file đính kèm (Ghi chép 2)			

Ghi chú 1: Việc copy phải được hạn chế ở mức tối thiểu, chỉ để khi nghiệp vụ yêu cầu.
Ghi chú 2: Trường hợp cần sự đồng ý của khách hàng thì tuân theo cách hủy mà khách hàng đã đồng ý đó.

8.3 QUẢN LÝ PHƯƠNG TIỆN TRUYỀN THÔNG

8.3.1 QUẢN LÝ PHƯƠNG TIỆN TRUYỀN THÔNG DI ĐỘNG

a) Việc mang ra/mang vào thẻ nhớ gắn ngoài chỉ được phép thực hiện, sau khi đã được sự cho phép trước. Ngoài ra, khi không sử dụng thì phải bảo quản trong tủ có khóa.
b) Không được lưu thông tin khách hàng, thông tin cá nhân, thông tin quan trọng của công ty một cách thiếu chú ý vào thiết bị lưu trữ ngoài.
c) Không được để thiết bị lưu trữ ngoại vi trên bàn hay trên kệ.
d) Trường hợp mang thiết bị lưu trữ ngoại vi của cá nhân vào công ty, hoặc trường hợp mang thiết bị lưu trữ ngoại vi của công ty ra ngoài, thì phải có sự cho phép của ban bảo mật thông tin và trưởng bộ phận của người đó.
e) Trường hợp lưu trữ, truyền tải dữ liệu vào thiết bị lưu trữ ngoài, phải sử dụng biện pháp truyền nhận sao cho có thể đảm bảo được tính bảo mật ứng với nội dung của dữ liệu.

f) Trường hợp cất giữ thẻ nhớ, thiết bị lưu trữ của khách hàng, nhất định phải quét bằng phần mềm diệt virus trước khi sử dụng.

8.3.2 XỬ LÝ PHƯƠNG TIỆN TRUYỀN THÔNG

Trường hợp không sử dụng thiết bị lưu trữ nữa, thì tuân theo quy tắc 8.2.3.

8.3.3 CHUYỂN GIAO PHƯƠNG TIỆN VẬT LÝ

Trường hợp vận chuyển thiết bị lưu trữ, phải bảo vệ bằng cách đóng gói thích hợp, và tuân theo 8.2.3.

9. KIỂM SOÁT TRUY CẬP

9.1 YÊU CẦU VỀ NGHIỆP VỤ ĐỐI VỚI KIỂM SOÁT TRUY CẬP

9.1.1 CHÍNH SÁCH KIỂM SOÁT TRUY CẬP

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.

9.1.2 TRUY CẬP VÀO MẠNG VÀ DỊCH VỤ MẠNG

a) Chỉ những thiết bị, nhân viên đã được phê chuẩn bởi người quản lý hệ thống thông tin mới được quyền kết nối vào mạng nội bộ công ty.
b) Việc truy cập từ bên ngoài vào nội bộ công ty sẽ bị hạn chế thông qua tường lửa.

9.2 QUẢN LÝ TRUY CẬP CỦA NGƯỜI SỬ DỤNG

9.2.1 ĐĂNG KÝ VÀ HỦY ĐĂNG KÝ NGƯỜI SỬ DỤNG

a) Khi đăng ký và hủy đăng ký của người sử dụng hệ thống thông tin thì trưởng bộ phận Hành chính nhân sự sẽ gửi yêu cầu tới cán bộ quản lý thông tin để xác nhận.
b) Người quản lý hệ thống thông tin sẽ thực hiện yêu cầu cho người làm việc trong phạm vi công việc cần thiết.

9.2.2 CUNG CẤP QUYỀN TRUY CẬP CHO NGƯỜI SỬ DỤNG

Đối với thông tin quan trọng, người quản lý hệ thống thông tin sẽ xem xét và thực hiện thiết lập quyền truy cập của người sử dụng, ở mức độ truy cập cần thiết tối thiểu.

9.2.3 QUẢN LÝ ĐẶC QUYỀN

ID đặc quyền sẽ gán cho người được chỉ định, làm rõ hệ thống được quản lý là gì, và người sở hữu đặc quyền đó là ai.

9.2.4 QUẢN LÝ THÔNG TIN CHỨNG THỰC BÍ MẬT CỦA NGƯỜI SỬ DỤNG

a) Người quản lý hệ thống thông tin, khi cấp mật khẩu tạm thời cho người sử dụng thì phải thông báo bằng phương pháp chỉ có bản thân người sử dụng mới biết.
b) Người quản lý hệ thống thông tin phải yêu cầu người sử dụng thay đổi ngay mật khẩu tạm thời.

9.2.5 XEM XÉT LẠI QUYỀN TRUY CẬP CỦA NGƯỜI SỬ DỤNG

Người quản lý hệ thống thông tin sẽ thực hiện kiểm kê và xem xét lại quyền truy cập định kỳ (ít nhất 1 lần 1 năm) hoặc khi cần thiết.

9.2.6 XÓA HOẶC CHỈNH SỬA QUYỀN TRUY CẬP

a) Khi phát sinh nghỉ việc thì phải điều chỉnh sao cho không có gây trở ngại trong nghiệp vụ, và nhanh chóng xóa tài khoản tương ứng. Về quyền truy cập:
    1) Trưởng bộ phận của người đó phải yêu cầu tới người quản lý hệ thống thông tin để xóa quyền truy cập.
    2) Bộ phận nhân sự sẽ yêu cầu cán bộ quản lý tại TECHVIFY vô hiệu hóa tài khoản
b) Khi phát sinh luân chuyển đến bộ phận khác thì sẽ xóa theo quy trình a)1). Ngoài ra, về quyền truy cập mới thì trưởng bộ phận mà người đó sẽ chuyển tới thì phải yêu cầu xin quyền truy cập mới, đăng ký theo quy trình 9.2.1.

9.3 TRÁCH NHIỆM CỦA NGƯỜI SỬ DỤNG

9.3.1 SỬ DỤNG THÔNG TIN CHỨNG THỰC BÍ MẬT

a) 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 khác (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 ISMS để được hỗ trợ.

b) Người sử dụng phải thay đổi mật khẩu trong vòng 90 ngày và khi cần thiết.

c) Mật khẩu của tài khoản quản trị hệ thống thì phải được quản lý nghiêm ngặt bởi người quản lý hệ thống thông tin.

d) Người sử dụng hoặc người quản lý hệ thống thông tin có thể sử dụng phương thức chứng thực bằng các thiết bị như là máy quét vân tay, máy quét thẻ IC, v.v... để thay thế hoặc củng cố cho mật khẩu.

9.4 KIỂM SOÁT TRUY CẬP HỆ THỐNG VÀ ỨNG DỤNG

9.4.1 KIỂM SOÁT TRUY CẬP VÀO THÔNG TIN

Người quản lý hệ thống thông tin hoặc người được chỉ định phải thiết lập sao cho chỉ những người cần thiết mới có quyền truy cập các hệ thống thông tin.

9.4.2 QUY TRÌNH ĐĂNG NHẬP BẢO MẬT

Mật khẩu được nhập trên màn hình đăng nhập phải để ở chế độ không hiển thị chuỗi ký tự.

Sử dụng phương thức MFA.

9.4.3 HỆ THỐNG QUẢN LÝ MẬT KHẨU

a) Nhập mật khẩu phải là tương tác

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

9.4.4 SỬ DỤNG TIỆN ÍCH HỆ THỐNG ĐẶC QUYỀN

Về việc sử dụng tiện ích hệ thống, trên nguyên tắc thì chỉ cho phép chức năng tiêu chuẩn hệ điều hành. Trường hợp cần tiện ích khác thì trước khi sử dụng phải có sự cho phép của người quản lý hệ thống thông tin.

Không được cài đặt phần mềm không cho phép được định nghĩa trọng tài liệu "**Standard_Whitelist-Blacklist_Software**".

9.4.5 KIỂM SOÁT TRUY CẬP VÀO MÃ NGUỒN CHƯƠNG TRÌNH

Mã nguồn chương trình thì phải được lưu vào tập tin, tập tin được lưu ở nơi mà được quản lý bằng quyền truy cập. Ngoài ra, thiết bị lưu trữ ngoài đã sao chép mã nguồn chương trình thì phải bảo quản theo mức độ bảo mật.

10. MÃ HÓA

10.1 KIỂM SOÁT MÃ HÓA

Chính sách sử dụng kiểm soát mã hóa

A) **SSL**

Thông tin nhận từ form đầu vào của trang chủ công ty sẽ được mã hóa dựa vào SSL.

B) LAN KHÔNG DÂY

Việc truyền thông tin qua LAN không dây sẽ được mã hóa, bằng phương pháp an toàn.

10.1.1 QUẢN LÝ KHÓA

A) **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.

B) 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.

11. BẢO MẬT VẬT LÝ VÀ MÔI TRƯỜNG

11.1 KHU VỰC NÊN ĐẢM BẢO BẢO MẬT

11.1.1 GIỚI HẠN BẢO MẬT VẬT LÝ

a) Công ty quy định phạm vi hạn chế việc ra vào, và sẽ giới hạn những ai không có quyền ra vào.

11.1.2 KIỂM SOÁT RA VÀO VẬT LÝ.

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 thẻ khách hoặc nhận diện khuôn mặt
   3) Tuyệt đối không sử dụng nhận diện của mình để mở cửa hộ người khác
b) Lịch sử ra vào
   1) Khi ra vào, ứng dụng mobile MyTechvify sẽ lưu lại toàn bộ thời gian ra vào của nhân viên
   2) Khi người ngoài đến thăm công ty, cần lưu lại thông tin trên sổ Visitor logs. Bộ phận Hành chính sẽ quản lý và có thể cấp thẻ ra vào cho khách.

11.1.3 BẢO MẬT VĂN PHÒNG, PHÒNG LÀM VIỆC VÀ CƠ SỞ VẬT CHẤT

a) Các khu vực làm việc thì luôn trang bị khóa, và cấm người không có quyền ra vào. Ở các khu vực mà không thể khóa được, thì những thông tin quan trọng cần quản lý nghiêm ngặt bằng cách lưu trữ vào các tủ khóa được.
b) Về nguyên tắc, nhân viên là người thực hiện khóa, mở khóa.
c) Đối với người ngoài đã được cho phép ra vào, về nguyên tắc phải đi theo nhân viên và không được phép ra vào các khu vực ngoài quyền hạn.

11.1.4 NGĂN CHẶN CÁC MỐI ĐE DỌA TỪ MÔI TRƯỜNG BÊN NGOÀI

a) Bố trí bình cứu hỏa ở các tầng dưới sự quản lý của tòa nhà.
b) Xác định vị trí cài đặt thiết bị để tránh máy chủ bị rơi. Ngăn chặn máy chủ bị va đập bằng cách sử dụng tủ rack.

11.1.5 LÀM VIỆC TẠI KHU VỰC CẦN BẢO MẬT

a) Khu vực cần đảm bảo bảo mật của tổ chức là phòng máy chủ và phòng quản lý tài sản.
b) Tại khu vực cần bảo mật, nguyên tắc là cấm kết nối thiết bị cá nhân (PC, điện thoại di động, thiết bị mạng v. v...) vào những thiết bị liệt kê dưới đây:
   1) PC và server
   2) Thiết bị ngoại vi
   3) Mạng trong công ty

   Ngoài ra, trường hợp cần kết nối theo yêu cầu công việc thì cần sự phê duyệt của

11.1.6 NƠI GIAO NHẬN

Về việc tiếp nhận hàng hóa, nguyên tắc là tuân theo khu vực giới hạn bảo mật vật lý và được giám sát bởi nhân viên thuộc bộ phận Hành chính.

11.2 THIẾT BỊ

11.2.1 THIẾT LẬP VÀ BẢO VỆ THIẾT BỊ

a) Công tắc, điểm truy cập LAN không dây nên thiết lập tại nơi ít người qua lại
b) Điều chỉnh góc độ để không nhìn thấy được màn hình, giao diện của PC từ lối vào.
c) Máy chủ sẽ được quản lý trong phòng máy chủ, cách ly với phòng làm việc. Trường hợp thiết lập ở nơi chưa được cách ly thì sẽ chứa vào tủ có khóa.

11.2.2 TIỆN ÍCH HỖ TRỢ

a) Người quản lý hệ thống thông tin sẽ thiết lập UPS cho các thiết bị mạng, server để đáp ứng yêu cầu quản lý và vận hành khi cần thiết.
b) Người quản lý hệ thống thông tin cần xác nhận kịp thời xem khu vực (nơi lắp đặt thiết bị) có được đảm bảo với nhiệt độ thích hợp hay không.

11.2.3 BẢO VỆ DÂY CÁP

Dây cáp được lắp ở những nơi mà có người hay qua lại phải được bảo vệ bằng đường dây ngầm dưới sàn hoặc nẹp lại, hay vỏ bảo vệ dây cáp. Ngoài ra, cố gắng buộc dây cáp thành một bó.

11.2.4 BẢO TRÌ THIẾT BỊ

Về máy chủ, thiết bị mạng (switch, router...), các thiết bị bảo mật khác, tham khảo hướng dẫn đã được cung cấp từ nhà sản xuất, và thực hiện bảo trì với tần suất mà nhà sản xuất khuyến cáo. Trường hợp cần có chuyên môn để bảo trì thì ủy thác việc bảo trì cho tổ chức bên ngoài.

11.2.5 DI CHUYỂN TÀI SẢN

a) Không được di dời nơi cài đặt của máy chủ, thiết bị mạng (switch, router…) mà

không được sự phê duyệt của phòng BMTT.

b) Nghiêm cấm việc mang tài sản có chứa thông tin mật của công ty và tài sản khách hàng mà không có phê duyệt của trưởng bộ phận và phòng BMTT.

11.2.6 BẢO MẬT THIẾT BỊ VÀ TÀI SẢN Ở BÊN NGOÀI

a) Trường hợp mang laptop ra bên ngoài thì nhất định phải thiết lập bảo mật thông tin theo quy định của ban ISMS. Ngoài ra, cần hạn chế mang thông tin quan trọng mang ra ngoài. Nếu bắt buộc phải mang ra ngoài thì phải thiết lập mật khẩu cho file chứa thông tin quan trọng.

b) Cần đưa ra các điều khoản khi thuê dịch vụ đối với nhà cung cấp để đảm bảo bảo mật thiết bị và tài sản ở bên ngoài theo điều 15.

11.2.7 BẢO MẬT TRONG VIỆC LOẠI BỎ HOẶC TÁI SỬ DỤNG THIẾT BỊ

a) Trường hợp cần xử lý laptop/PC, nhân viên sẽ không tự xử lý mà cần thông báo cho người quản lý tài sản và người quản lý hệ thống thông tin để tiến hành xử lý theo quy trình của công ty.

b) Trường hợp xác định là cần xử lý theo phương pháp khác a) thì cần phải có phê duyệt của phòng bảo mật thông tin.

c) Người quản lý hệ thống thông tin, trong trường hợp tái sử dụng thiết bị, sẽ xóa hoàn toàn những thông tin không cần thiết và phần mềm được cấp bản quyền.

11.2.8 THIẾT BỊ CỦA NGƯỜI DÙNG TRONG TRẠNG THÁI KHÔNG SỬ DỤNG

a) Người sử dụng phải thiết lập mật khẩu screen saver cho PC. Thời gian cài đặt screen saver là trong vòng 3 phút.

b) Để phòng chống trộm cắp máy tính cá nhân, cần thực hiện một trong những đối sách dưới đây:
   1) Cố định bằng khóa dây.
   2) Bảo quản trong tủ khóa khi không sử dụng.

c) Khi gửi nhận FAX, photocopy hoặc in ấn và scan thì cần chú ý lấy ngay tài liệu, không để tại máy.

11.2.9 CHÍNH SÁCH MÀN HÌNH/BÀN LÀM VIỆC GỌN GÀNG

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 5 phút trở lên thì thực hiện khóa laptop hoặc tắt nguồn điện của màn hình. Ngoài ra, khi về nhà 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

12. BẢO MẬT VẬN HÀNH

12.1 QUY TRÌNH VÀ TRÁCH NHIỆM VẬN HÀNH

12.1.1 THỦ TỤC VẬN HÀNH ĐƯỢC VĂN BẢN HÓA

Người sử dụng phải tham khảo quy trình khi cần thiết để xác thực được tính chính xác và đảm bảo tính bảo mật của các thiết bị xử lý thông tin.

12.1.2 QUẢN LÝ THAY ĐỔI

Người quản lý hệ thống thông tin phải thu thập thông tin và xác nhận không có vấn đề trước khi thực hiện kết nối thiết bị ngoại vi với máy chủ hoặc trước khi áp dụng gói dịch vụ. Ngoài ra, trường hợp phát sinh vấn đề sau khi áp dụng thì cần thực hiện giải quyết vấn đề ngay lập tức bằng cách cài đặt lại.

12.1.3 QUẢN LÝ DUNG LƯỢNG

a) Người quản lý hệ thống thông tin cần dựa vào thời gian truy cập cũng như trạng thái của hệ thống mạng để xác định xem có vấn đề gì hay không. Trong trường hợp phát hiện vấn đề, người quản lý hệ thống thông tin phải nhanh chóng thực hiện điều tra nguyên nhân và báo cáo cho ban bảo mật thông tin. Ban bảo mật thông tin sẽ chỉ thị cách xử lý cho người quản lý hệ thống thông tin, và báo cáo cho đội ngũ quản lý nếu cần thiết.

b) Người quản lý hệ thống thông tin sẽ xem xét về tình trạng hoạt động của hệ thống trong các khoảng thời gian (trung bình hoặc dài hạn) để ước tính khả năng đáp ứng của hệ thống trong tương lai và báo cáo cho Tổng Giám đốc nếu cần thiết.

12.1.4 PHÂN TÁCH MÔI TRƯỜNG PHÁT TRIỂN, MÔI TRƯỜNG KIỂM THỬ VÀ MÔI TRƯỜNG VẬN HÀNH

Khi phát triển hệ thống thông tin thì phân chia về mặt vật lý, hoặc về mặt logic đối với môi trường phát triển, môi trường kiểm thử và môi trường vận hành.

12.2 BẢO VỆ CHỐNG MALWARE

12.2.1 KIỂM SOÁT CHỐNG MALWARE

a) Tất cả các máy tính hoặc máy chủ kết nối với mạng cần cài đặt phần mềm diệt virus bởi người quản lý hệ thống thông tin.
b) Thiết lập phần mềm diệt virus trong trạng thái sẵn sàng và tự động quét khi nhận được email hay truy cập vào file.
c) Không chỉ scan bình thường, mà định kỳ thực hiện scan đối với toàn bộ file, trong khoảng thời gian mà người quản lý hệ thống thông tin chỉ định, 3 tháng 1 lần.
d) Thiết lập sao cho việc cập nhật các bản vá lỗi theo hình thức tự động.
e) Người quản lý hệ thống thông tin sẽ thiết lập mức độ bảo mật của trình duyệt Web ở mức trung bình - cao.
f) Đối với email có mục tiêu lừa đảo:
    1) 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.
    2) 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).

12.3 SAO LƯU

12.3.1 SAO LƯU THÔNG TIN

a) Sử dụng chức năng sao lưu thông tin có sẵn theo tiện ích/ dịch vụ đang sử dụng (Git, AWS, Sharepoint, Microsoft…)
b) Người quản lý hệ thống thông tin sẽ thực hiện sao lưu dữ liệu từ hệ thống theo định kỳ để phòng tránh các dữ liệu quan trọng được lưu trong máy chủ bị làm giả, phá hủy, truy cập bất chính...
c) Người quản lý hệ thống thông tin phải kiểm tra định kỳ xem việc sao lưu có được thực hiện chính xác, và có thể khôi phục khi bị lỗi hay không.

12.4 LẤY VÀ GIÁM SÁT LOG

12.4.1 LẤY LOG SỰ KIỆN

a) Người quản lý hệ thống thông tin phải tiến hành lấy log khi cần thiết để phòng tránh các dữ liệu quan trọng được lưu trong máy chủ bị làm giả, phá hủy, truy cập bất chính.
b) Người quản lý hệ thống thông tin phải thực hiện kiểm tra log định kỳ nếu cần thiết.

12.4.2 BẢO VỆ THÔNG TIN LOG

Chỉ người quản lý hệ thống thông tin hoặc những người được chỉ định có thể truy cập vào log.

12.4.3 Log công việc của người quản lý nghiệp vụ và người phụ trách vận hành Người quản lý hệ thống thông tin sẽ xác nhận công việc mà người phụ trách vận hành tham gia vào server. Xác nhận dựa vào việc xem log công việc, hoặc báo cáo lịch sử các thao tác trên server.

12.4.4 ĐỒNG BỘ THỜI GIAN

Người quản lý hệ thống thông tin sẽ đồng bộ thời gian của toàn bộ máy tính và server.

12.5 QUẢN LÝ PHẦN MỀM VẬN HÀNH

12.5.1 CÀI ĐẶT PHẦN MỀM LIÊN QUAN ĐẾN HỆ THỐNG VẬN HÀNH

a) Hệ thống vận hành chỉ lưu mã nguồn thực thi, không lưu mã nguồn phát triển hoặc mã nguồn tổng hợp.
b) Phần mềm sử dụng tại máy tính, về nguyên tắc chỉ chấp nhận những gì được chỉ định bởi người quản lý hệ thống thông tin, và trường hợp sử dụng phần mềm khác thì sẽ phải xin phép trước.
c) Nghiêm cấm sử dụng các phần mềm có mức độ an toàn thấp (dễ bị nhiễm virus, hay truy cập bất chính như phần mềm chia sẻ file). Xem thêm tại tài liệu "**Standard_Whitelist-Blacklist_Software**".

12.6 QUẢN LÝ LỖ HỔNG BẢO MẬT

12.6.1 QUẢN LÝ LỖ HỔNG BẢO MẬT

a) Người quản lý bảo mật thông tin và ban bảo mật thông tin phải luôn nhận thức được các vấn đề về bảo mật, để ngăn ngừa những cuộc tấn công từ bên ngoài một cách hiệu quả, không mất thời gian.
b) Áp dụng bản vá bảo mật mới nhất cho hệ điều hành và các ứng dụng. Tuy nhiên, thông qua kết quả kiểm chứng, trường hợp được cho là có vấn đề về mặt bảo mật thì phải tiến hành các đối sách chống phần mềm độc hại bằng phương pháp an toàn thông tin.

12.6.2 GIỚI HẠN CÀI ĐẶT PHẦN MỀM

a) Người quản lý hệ thống thông tin, sẽ kiểm tra định kỳ các phần mềm mà người sử dụng được phép cài đặt.

b) Người sử dụng không được cài đặt các phần mềm chưa cho phép, trường hợp cần thiết cho nghiệp vụ thì phải có sự đồng thuận của người quản lý hệ thống thông tin trước khi cài đặt.

12.7 CÁC MỤC CÂN NHẮC ĐỐI VỚI GIÁM SÁT HỆ THỐNG THÔNG TIN

12.7.1 KIỂM SOÁT ĐỐI VỚI VIỆC GIÁM SÁT HỆ THỐNG THÔNG TIN

a) Việc giám sát hệ thống thông tin, theo nguyên tắc là sẽ cân nhắc đến rủi ro của việc dừng hệ thống, nên sẽ sử dụng thời gian ngoài giờ làm việc hoặc ngày nghỉ để thực hiện.

b) Trường hợp dừng hoạt động của hệ thống thông tin do bảo trì hệ thống, trên nguyên tắc là sẽ thực hiện theo phạm vi không gây ảnh hưởng đến nghiệp vụ hoặc là thực hiện theo từng khoảng thời gian.

13. BẢO MẬT KẾT NỐI

13.1 QUẢN LÝ BẢO MẬT MẠNG

13.1.1 KIỂM SOÁT MẠNG

a) Sử dụng mạng trong công ty

1) Việc kết nối đến mạng trong công ty phải tuân theo quy trình đã được chỉ thị, xác nhận của người quản lý hệ thống thông tin.
2) Người quản lý hệ thống thông tin sẽ thực hiện đối sách chống xâm nhập bất chính như thiết lập tường lửa ở ranh giới mạng lưới nội bộ với mạng bên ngoài.
3) Không được kết nối với mạng trong công ty bằng tài khoản, mật khẩu của người khác.
4) 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.
5) Trường hợp mang và sử dụng máy tính cá nhân thì không kết nối với mạng nội bộ trong công ty. Trường hợp bắt buộc phải kết nối thì thực hiện quét virus dựa vào phần mềm mà người quản lý hệ thống thông tin chỉ định.
6) Trường hợp sử dụng mạng LAN không dây, thì phải có sự đồng thuận của người quản lý hệ thống thông tin, và thực hiện chính sách an toàn đầy đủ như là mã hóa và chứng thực máy tính kết nối.

b) Sử dụng Internet

1) Trường hợp sử dụng internet phải tuân theo chỉ thị của người quản lý hệ thống

thông tin.

2) Về internet, phải nhận thức rằng có nhiều rủi ro hơn so với mạng nội bộ trong công ty, và sử dụng trong phạm vi giới hạn cần thiết về mặt nghiệp vụ.

13.1.2 BẢO MẬT CỦA 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.

13.1.3 PHÂN TÁCH MẠNG

a) Đặt tường lửa vào ranh giới giữa mạng ngoài và mạng nội bộ trong công ty.
b) Đường mạng của khối sản xuất được tách riêng khỏi mạng của khối backoffice
c) Các dự án yêu cầu bảo mật được tách V-Lan riêng

13.2 CHUYỂN TIẾP THÔNG TIN

13.2.1 CHÍNH SÁCH VÀ QUY TRÌNH CHUYỂN GIAO THÔNG TIN

a) Account được set quyền truy cập theo từng loại
b) Trường hợp cần gửi thông tin quan trọng ra bên ngoài bằng file đính kèm qua email phải mã hóa thông tin hoặc zip và đặt mật khẩu. Mật khẩu giải mã phải được gửi bằng email khác hoặc bằng phương tiện khác.
c) Trường hợp gửi thông tin quan trọng bằng FAX ra bên ngoài thì phải đối chiếu mã số đã nhập với danh thiếp, phiếu chuyển hàng, sau khi xác nhận không có nhầm lẫn mới bấm nút gửi. Ngoài ra, nếu địa chỉ nơi gửi đến là địa chỉ thường xuyên gửi thì đăng ký vào danh bạ.
d) 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.
e) Những thiết bị lưu trữ ngoài chứa thông tin quan trọng thì cần phải trao tận tay. Trường hợp bắt buộc phải gửi đi thì cần phải được đóng gói cẩn thận trước khi gửi.
f) Lịch sử tiếp nhận thông tin cá nhân
    1) Khi tiếp nhận thông tin cá nhân bằng giấy hoặc thiết bị lưu trữ, cần phải xác nhận bằng phiếu gửi hoặc hóa đơn.
    2) Khi thực hiện tiếp nhận thông tin cá nhân bằng mail điện tử, thì phải lưu lại lịch sử đã gửi, nhận mail.
g) Sử dụng Email
    1) Chỉ được sử dụng email của công ty hoặc email được công ty cho phép cho mục đích công việc, không được sử dụng bất kỳ email hay hệ thống email khác

13.2.2 THỎA THUẬN VỀ CHUYỂN GIAO THÔNG TIN

a) Trước khi chuyển giao thông tin thì phải có sự thỏa thuận của 2 bên về phương thức chuyển giao.
b) Trường hợp gửi thông tin quan trọng ra bên ngoài bằng mail đính kèm thì cần gọi điện thoại xác nhận trước và sau khi gửi khi cần thiết.
c) Trường hợp sử dụng giao hàng tận nhà thì sử dụng dịch vụ mà công ty chỉ định.

13.2.3 GỬI TIN NHẮN ĐIỆN TỬ

a) Việc gửi thông tin được nhập vào website của công ty được thực hiện thông qua SSL.
b) Trường hợp gửi dữ liệu điện tử có chứa thông tin cá nhân thông qua internet phải sử dụng biện pháp thiết lập mật khẩu hoặc mã hóa như SSL.

13.2.4 CAM KẾT BẢO MẬT/KHÔNG TIẾT LỘ

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.
c) Ban bảo mật thông tin sẽ đối chiếu 1 lần 1 năm về các mục yêu cầu bảo mật thông tin, và kiểm chứng tính hợp lệ của thỏa thuận bảo mật.

14. XÂY DỰNG, PHÁT TRIỂN VÀ BẢO TRÌ HỆ THỐNG

14.1 NHỮNG MỤC YÊU CẦU BẢO MẬT CỦA HỆ THỐNG THÔNG TIN

14.1.1 PHÂN TÍCH VÀ THÔNG SỐ HÓA CÁC MỤC YÊU CẦU BẢO MẬT

Người quản lý hệ thống thông tin khi đưa vào sử dụng hoặc cải thiện hệ thống thông tin cho nghiệp vụ, nếu cần thiết thì sẽ văn bản hóa những yêu cầu của bảo mật thông tin. Sẽ gồm các hạng mục sau.

a) Mục liên quan đến nơi lắp đặt hệ thống thông tin (bao gồm cả chính sách và môi trường tiêu chuẩn).
b) Mục liên quan đến tiện ích hỗ trợ như thiết bị, hệ thống nguồn điện liên tục.
c) Mục liên quan đến hợp đồng bảo trì.
d) Mục liên quan đến dư thừa của dung lượng hệ thống.

e) Mục liên quan đến đối sách an toàn của đường truyền, dữ liệu.
f) Mục liên quan đến kiểm thử đầu vào.
g) Mục liên quan đến quyền truy cập.

14.1.2 BẢO MẬT CỦA DỊCH VỤ ỨNG DỤNG TRÊN MẠNG CÔNG CỘNG.

Khi cung cấp dịch vụ ứng dụng trên mạng công cộng như giao dịch online, phải tiến hành thực hiện cung cấp chức năng chứng thực thích hợp và mã hóa.

14.1.3 BẢO MẬT GIAO DỊCH CHO DỊCH VỤ ỨNG DỤNG

Giao dịch của dịch vụ ứng dụng sẽ được bảo vệ bằng việc mã hóa. Ngoài ra, sẽ xem xét về việc sử dụng ký tên điện tử nếu cần thiết.

14.2 BẢO MẬT TRONG TRONG QUÁ TRÌNH HỖ TRỢ VÀ PHÁT TRIỂN

14.2.1 CHÍNH SÁCH PHÁT TRIỂN ĐÃ CÂN NHẮC ĐẾN BẢO MẬT

Dưới đây là Chính sách phát triển đã cân nhắc đến bảo mật.

a) Phát triển hệ thống thông tin sử dụng trong công ty và hệ thống thông tin cung cấp cho bên ngoài.
   1) Môi trường phát triển: theo 14.2.6 a)
   2) Công đoạn: thiết lập yêu cầu rõ ràng trong công đoạn thiết kế (chỉ trường hợp phát triển nội bộ công ty), phát triển, kiểm thử và người quản lý sẽ xác nhận sau khi hoàn thành từng công đoạn.
   3) Tài liệu phát triển: tài liệu phát triển (bản thông số, bản thiết kế, thông số kiểm thử…), những gì cần thiết tối thiểu thì sẽ được phép truy cập.
b) Trong quá trình phát triển tại công ty hay ngồi tại công ty khách hàng thì cần tuân theo Chính sách, quy tắc bảo mật của khách hàng.

14.2.2 QUY TRÌNH QUẢN LÝ THAY ĐỔI HỆ THỐNG

a) Thực hiện quản lý thay đổi theo quy trình dưới đây.
   1) Khi có yêu cầu thay đổi thì người quản lý hệ thống thông tin, trưởng bộ phận trực thuộc của người đề xuất sẽ xác nhận.
   2) Người quản lý hệ thống thông tin lưu lại lịch sử thay đổi khi đã thay đổi hệ thống. Ngoài ra, thực hiện quản lý phiên bản của phần mềm, và xử lý sao cho phiên bản mới và phiên bản cũ không bị lẫn lộn.
b) Thực hiện sao chép dữ liệu và thông tin thiết lập của thiết bị, để có thể trở về trạng thái ban đầu trước khi thay đổi nếu phát sinh vấn đề.

14.2.3 XEM XÉT LẠI KĨ THUẬT CỦA ỨNG DỤNG SAU KHI THAY ĐỔI HỆ ĐIỀU HÀNH

Việc thay đổi hệ điều hành phải được thực hiện sau khi người quản lý thông tin đã kiểm chứng hoạt động của hệ thống thông tin hoạt động trên hệ điều hành bằng máy kiểm thử hay máy dự bị.

14.2.4 GIỚI HẠN ĐỐI VỚI THAY ĐỔI GÓI PHẦN MỀM

Về nguyên tắc thì không được tùy chỉnh gói phần mềm. Trường hợp bắt buộc phải điều chỉnh thì phải cân nhắc xem có ảnh hưởng đến hoạt động cũng như việc hỗ trợ trong tương lai từ nhà cung cấp hay không? Đồng thời phải được sự cho phép của người quản lý hệ thống thông tin thì mới được tùy chỉnh.

14.2.5 NGUYÊN TẮC XÂY DỰNG HỆ THỐNG ĐẢM BẢO BẢO MẬT.

Khi phát triển hệ thống thông tin sử dụng trong nội bộ công ty và hệ thống thông tin cung cấp cho bên ngoài thì cần làm rõ hạng mục bảo mật, và ghi chép lại.

14.2.6 MÔI TRƯỜNG PHÁT TRIỂN ĐẢM BẢO BẢO MẬT

a) Nhóm phát triển và nhóm vận hành cần được phân tách về khu vực làm việc cũng như các hệ thống làm việc. Ngoài ra, 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 thì chỉ những người liên quan mới được truy cập vào mã nguồn và file cài đặt.

14.2.7 PHÁT TRIỂN DỰA VÀO ỦY THÁC BÊN NGOÀI

Trình tự trong trường hợp ủy thác phát triển hệ thống thông tin cho bên ngoài như sau.

a) Đánh giá, chọn nơi ủy thác dựa vào **Phiếu đánh giá nhà cung cấp**, và giám sát tình trạng thực hiện hợp đồng, tái thẩm tra theo tần suất đã được quy định trước (ít nhất 1 năm 1 lần).
b) Ký kết hợp đồng với bên được ủy thác (trong hợp đồng phải bao gồm các mục yêu cầu bảo mật).
c) Thực hiện kiểm thử đầu vào theo quy định 14.2.9.

14.2.8 KIỂM THỬ BẢO MẬT HỆ THỐNG

Chức năng bảo mật của hệ thống thông tin được thực hiện trước khi chuyển sang môi trường vận hành.

14.2.9 KIỂM THỬ ĐẦU VÀO CỦA HỆ THỐNG

a) Khi cài đặt hoặc chỉnh sửa hệ thống thông tin thì tiến hành xác nhận hoạt động khi tiếp nhận.
b) Tạo bản thông số kiểm thử đầu vào, và xác nhận
c) Kết quả của kiểm thử đầu vào sẽ được xác nhận bởi người quản lý hệ thống thông tin và người quản lý của bộ phận tiếp nhận.

14.3 DỮ LIỆU KIỂM THỬ

14.3.1 BẢO VỆ DỮ LIỆU KIỂM THỬ

a) Cấm sử dụng thông tin cá nhân để làm dữ liệu kiểm thử.
b) Phân quyền việc truy cập dữ liệu kiểm thử.
c) Trường hợp sử dụng dữ liệu thực làm dữ liệu kiểm thử thì sẽ sử dụng sau khi nhận được đồng thuận của người quản lý hệ thống thông tin. Sau khi kết thúc kiểm thử thì sẽ xóa ngay dữ liệu thực tế, và báo cáo cho người quản lý hệ thống thông tin.

15. MỐI QUAN HỆ VỚI NHÀ CUNG CẤP

15.1 BẢO MẬT THÔNG TIN LIÊN QUAN ĐẾN NHÀ CUNG CẤP

15.1.1 Chính sách bảo mật thông tin trong mối quan hệ với nhà cung cấp

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

1) Nhà cung cấp ISP, dịch vụ điện thoại, v.v…
2) Ủy thác bên ngoài khi phát triển, bảo trì hệ thống thông tin.
3) Nhà cung cấp các dịch vụ chuyên môn như kế toán, thuế, pháp luật.
4) Server Cloud

b) Ban bảo mật thông tin sẽ cân nhắc đến rủi ro có thể phát sinh khi cho phép công ty ngoài truy cập vào khu vực văn phòng và hệ thống thông tin, sau đó cần làm rõ các mục yêu cầu về bảo mật thông tin.

15.1.2 XỬ LÝ BẢO MẬT VỚI SỰ ĐỒNG 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.

3) Ban bảo mật thông tin sẽ cân nhắc đến rủi ro có thể xảy ra tại 15.1.1a), và kí kết hợp đồng với bên thứ ba nếu cần thiết.

15.1.3 CHUỖI CUNG ỨNG ICT (INFORMATION & COMMUNICATION TECHNOLOGY)

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) Độ tin cậy, kết quả sử dụng thực tế của dịch vụ.
   2) Chức năng hỗ trợ người dùng
   3) Xử lý dữ liệu sau khi kết thúc sử dụng
   4) Tính sẵn sàng của dịch vụ
   5) Những biện pháp bảo mật (ví dụ như Mã hóa) đối với các kênh thông tin.

15.2 QUẢN LÝ CUNG CẤP DỊCH VỤ CỦA NHÀ CUNG CẤP

15.2.1 GIÁM SÁT VÀ XEM XÉT LẠI CUNG CẤP 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).

15.2.2 QUẢN LÝ ĐỐI VỚI THAY ĐỔI CUNG CẤP DỊCH VỤ CỦA NHÀ CUNG CẤP

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.

16. QUẢN LÝ SỰ CỐ BẢO MẬT THÔNG TIN

16.1 QUẢN LÝ VÀ CẢI THIỆN SỰ CỐ BẢO MẬT THÔNG TIN

16.1.1 TRÁCH NHIỆM VÀ QUY TRÌNH

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)

16.1.2 BÁO CÁO SỰ CỐ BẢO MẬT THÔNG TIN

Báo cáo sự cố bảo mật thông tin được mô tả trong tài liệu **"Quy trình_Quản lý sự cố"**.

16.1.3 BÁO CÁO ĐIỂM YẾU VỀ BẢO MẬT THÔNG TIN

Trường hợp đã nhận ra điểm yếu, mối đe dọa bảo mật thông tin hoặc trường hợp có nghi ngờ thì báo cáo cho ban bảo mật thông tin.

16.1.4 ĐÁNH GIÁ VÀ QUYẾT ĐỊNH SỰ CỐ BẢO MẬT THÔNG TIN

Đánh giá và quyết định sự cố bảo mật thông tin được mô tả trong tài liệu **"Quy trình_Quản lý sự cố"**

16.1.5 XỬ LÝ SỰ CỐ BẢO MẬT 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"**

16.1.6 BÀI HỌC TỪ SỰ CỐ BẢO MẬT THÔNG TIN

Ban bảo mật thông tin 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.

16.1.7 THU THẬP CHỨNG CỨ

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.

17. VẤN ĐỀ BẢO MẬT THÔNG TIN TRONG QUẢN TRỊ KINH DOANH LIÊN TỤC

17.1 BẢO MẬT THÔNG TIN LIÊN TỤC

17.1.1 KẾ HOẠCH BẢO MẬT THÔNG TIN LIÊN TỤC

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 ("tài sản quan trọng ") và có tính sẵn sàng (từ “3” trở lên).

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

d) 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.

e) 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.

17.1.2 THỰC HIỆN BẢO MẬT THÔNG TIN LIÊN TỤC

Đối với những mục được cho là có thứ tự ưu tiên cao ở 17.1.1D), lập **Kế hoạch kinh doanh liên tục**, và có sự xác nhận của Tổng Giám đốc. **Kế hoạch kinh doanh liên tục** có thể bao gồm nội dung (nếu cần) dưới đây.

a) Điều kiện bắt đầu thực hiện khi phát sinh rủi ro.

b) Quy trình xử lý khẩn cấp

c) Quy trình khôi phục.

d) Mục tiêu khôi phục (Quyết định thời gian mục tiêu nếu cần thiết).

e) Quy trình hoạt động lại (Quy trình theo dõi sau khi khôi phục).

f) Kiểm tra định kỳ.

17.1.3 KIỂM TRA VÀ ĐÁNH GIÁ LẠI BẢO MẬT THÔNG TIN LIÊN TỤC

a) Kiểm tra kế hoạch kinh doanh liên tục

Thực hiện kiểm tra về kế hoạch và thủ tục đã lập, cập nhật kế hoạch trong trường hợp phán đoán là cần kết quả kiểm tra. Thực hiện kiểm tra theo một trong những phương pháp dưới đây hoặc kết hợp.

1) Kiểm tra trong phòng thí nghiệm.
2) Kiểm tra giả định.
3) Kiểm tra khôi phục mang tính kỹ thuật.
4) Kiểm tra khôi phục ở cơ sở thay thế.
5) Kiểm tra dịch vụ và cở sở của nhà cung cấp.

b) Thực hiện kiểm tra liên tục

Ban bảo mật thông tin sẽ thực hiện liên tục ít nhất 1 lần 1 năm về việc kinh doanh liên tục.

17.2 DỰ PHÒNG

17.2.1 TÍNH SẴN SÀNG CỦA CƠ SỞ THIẾT BỊ XỬ LÝ THÔNG TIN

a) Hệ thống thông tin quan trọng cần làm rõ các mục yêu cầu về mặt nghiệp vụ liên quan đến tính sẵn sàng, và áp dụng phương pháp dự phòng (như làm thành 2 bản) nếu cần thiết.
b) Xác nhận độ chính xác khi hoán đổi giữa hệ thống chính và hệ thống dự phòng nếu cần thiết.

18. TUÂN THỦ

18.1 TUÂN THỦ CÁC MỤC YÊU CẦU TRÊN HỢP ĐỒNG VÀ PHÁP LUẬT

18.1.1 CHỈ ĐỊNH CÁC MỤC YÊU CẦU TRÊN HỢP ĐỒNG VÀ PHÁP LUẬT

a) Ban bảo mật thông tin 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 **Bảng quy định pháp lệnh liên quan đến hệ thống thông tin**. **Bảng quy định pháp lệnh liên quan đến hệ thống thông tin** sẽ xem lại ít nhất 1 lần 1 năm.
b) Ban bảo mật thông tin 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 thiết.

18.1.2 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.

18.1.3 BẢO VỆ 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.

Loại bản ghi	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 ■ 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,	10 năm

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)	
■ 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)	7 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	5 năm
■ Đơn đăng ký không đánh thuế tài sản hình thành tiết kiệm, đơn xin luân chuyển	5 năm
■ Tài liệu liên quan đến người được bảo hiểm bởi bảo hiểm tuyển dụng	4 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	5 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	5 năm

■ Tài liệu liên quan đến bảo hiểm lương hưu phúc lợi xã hội	
■ Tài liệu liên quan đến bảo hiểm tuyển dụng	

18.1.4 BẢO VỆ THÔNG TIN RIÊNG TƯ CÁ NHÂN

Thông tin cá nhân thì sẽ quản lý nghiêm ngặt theo các quy trình bảo mật thông tin hay pháp luật.

18.1.5 QUY CHẾ ĐỐI VỚI CHỨC NĂNG MÃ HÓA

Trường hợp mang thiết bị đã mã hóa ra ngoài công ty, hoặc mang ra nước ngoài thì phải tìm hiểu về pháp luật, quy chế liên quan, khi cần thiết.

18.2 XEM XÉT LẠI BẢO MẬT THÔNG TIN

18.2.1 XEM XÉT ĐỘC LẬP VỀ BẢO MẬT 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.

18.2.2 TUÂN THỦ CHÍNH SÁCH VÀ TIÊU CHUẨN BẢO MẬT 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 hoặc kiểm tra đột xuất.
b) Thành viên ban bảo mật thông tin sẽ yêu cầu bộ phận Hành chính lưu trữ các thông tin ra vào công ty. Định kỳ 3 tháng 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.

18.2.3 XEM XÉT VIỆC TUÂN THỦ MANG TÍNH KỸ THUẬT

Để chắc chắn các mục tuân thủ mang tính kỹ thuật đang được thực hiện đúng, thì người quản lý hệ thống thông tin sẽ kiểm tra theo 18.2.2.

Người phê duyệt	Người xem xét	Người lập