TECHVFY
Empower your digital innovation

QUY ĐỊNH

BẢO MẬT THÔNG TIN

Mã tài liệu	**02v-QD/ISM/HDCV**
Phiên bản	**1.0**
Ngày hiệu lực	**15/04/2021**

LỊCH SỬ THAY ĐỔI

Số	Ngày cập nhật	Phiên bản	Nội dung cập nhật	Lý do cập nhật	Người khởi tạo	Người phê duyệt
1	15/04/2021	1.0	Tạo mới	Tạo mới	Nguyen Duc Linh	Hieu Nguyen
2						

MỤC LỤC

CHƯƠNG I. QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

Quy định này áp dụng cho Công ty cổ phần TECHVIFY Việt Nam (sau đây gọi tắt là Công ty).

Đối tượng áp dụng là CBNV của Công ty (sau đây viết tắt là CBNV) là người lao động ký Hợp đồng thử việc, Hợp đồng lao động với Công ty.

Điều 2. Định nghĩa và giải thích từ ngữ.

2.1. **"Thông tin bảo mật"** là tất cả thông tin, dữ liệu, tin tức, sự kiện, sự việc, ý tưởng, phán đoán, trí thức về tài sản không được công khai, hoặc bất kỳ thông tin nào dưới mọi hình thức mang bản chất tương tự, có liên quan đến hoạt động sản xuất kinh doanh của Công ty. Phạm vi áp dụng bao gồm và không hạn chế ở:

2.1.1. Các sản phẩm phần mềm của Công ty và của khách hang/đối tác, bao gồm:

a) Tài liệu khảo sát, phân tích thiết kế bước đầu,

b) Tài liệu thiết kế, module sản phẩm

c) Cơ sở dữ liệu, các chương trình máy tính bao gồm mã nguồn, mã đối tượng,

d) Các phương tiện xây dụng phần mềm như cơ sở dữ liệu, ngôn ngữ lập trình, chương trình dịch, chương trình bổ trợ …

e) Sản phẩm phần mềm trọn gói, hướng dẫn sử dụng,

f) Nguyên bản các giao diện của sản phẩm phần mềm, bao gồm cả các trang web của Công ty và của Công ty thiết kế cho khách hang/đối tác…

2.1.2. Các thiết kế/giải pháp, các quy trình cài đặt/triển khai cho từng dòng sản phẩm Công nghệ thông tin (CNTT) hoặc cho từng khách hàng/đối tác và các tài liệu liên quan.
2.1.3. Các giải pháp tích hợp hệ thống thông tin, giải pháp công nghệ triển khai cho Công ty, khách hàng/đối tác.
2.1.4. Các tài liệu báo cáo hoặc tổng kết về giải pháp/ thiết kế do Công ty nghiên cứu, phát triển.
2.1.5. Các thông tin bảo mật về thị trường, khách hàng, tài chính … đã được Công ty phân tích, khai thác và phát triển mang tính đặc thù.
2.1.6. Các thông tin cá nhân của khách hàng, khách hàng của khách hàng và các thông tin cá nhân

khác, nếu có, được khách hàng ủy thác để thực hiện công việc.

2.1.7. Các thông tin cá nhân của CBNV bao gồm, nhưng không giới hạn, tên, ngày tháng năm sinh, nơi sinh, số chứng minh nhân dân, số sổ bảo hiểm, số nhận dạng cá nhân, tài khoản, mã số thuế, địa chỉ email, địa chỉ IP, web cookie, địa chỉ nhà riêng, số điện thoại, lương thưởng, vị trí công việc, trình độ học vấn, lịch sử đào tạo, sơ yếu lý lịch, con cái, bố mẹ.

2.1.8. Các quy trình sản xuất bao gồm tất cả các tài liệu cấu thành như Mô tả quá trình, Mô tả sản phẩm, Biểu mẫu …

2.1.9. Các thông tin, được thể hiện bằng văn bản giấy tờ hoặc văn bản điện tử được đánh dấu là "Tài liệu mật" hoặc "Sử dụng nội bộ" hoặc một hình thức tương đương.

2.2. **Đối tác của Công ty**: Là những cá nhân, tập thể, tổ chức có hoạt động sản xuất kinh doanh các sản phẩm/ dịch vụ giống hoặc tương tự với sản phẩm của Công ty, cùng hướng tới đối tượng khách hàng, đối tác như của Công ty, và chia sẻ lợi ích với Công ty.

2.3. **Đối thủ cạnh tranh**: Là những cá nhân, tập thể, tổ chức có hoạt động sản xuất kinh doanh các sản phẩm/ dịch vụ giống hoặc tương tự với sản phẩm của Công ty, cùng hướng tới đối tượng khách hàng, đối tác như của Công ty, nhưng không chia sẻ lợi ích với Công ty.

2.4. **Khách hàng của Công ty**: Là những cá nhân, tập thể, tổ chức mua sản phẩm/ dịch vụ của Công ty.

2.5. **Bên thứ ba**: Là bất kỳ một cá nhân, tập thể, tổ chức nào, ngoài Công ty và bản thân CBNV nắm giữ Thông tin bảo mật.

2.6. **Thiết bị di động**: Là bất cứ thiết bị cầm tay hoặc thiết bị có hình dáng nhỏ gọn cho phép người sử dụng có thể lưu trữ thông tin, xử lý thông tin, gửi thông tin, kết nối với internet từ bất cứ nơi nào, bao gồm nhưng không giới hạn: máy tính xách tay, máy tính bảng, điện thoại, thiết bị nhớ ngoài như ổ USB, thẻ nhớ hoặc các thiết bị khác có tính năng hoặc chức năng tương tự.

2.7. **Thông tin cá nhân**: Là thông tin có thể được sử dụng để phân biệt hoặc theo dõi danh tính của một cá nhân chẳng hạn như tên, số chứng minh nhân dân, số sổ bảo hiểm, hồ sơ sinh trắc học, v.v hoặc khi kết hợp với các thông tin khác có thể nhận dạng được cá nhân cụ thể.

2.8. **Khu vực bảo mật**: Các trung tâm Phát triển phần mềm (ODC), các trung tâm dữ liệu, các phòng máy chủ và các phòng có chứa thông tin bảo mật, các phòng chứa thiết bị. Chỉ có nhân viên được phân quyền mới được ra vào khu vực này, những người khác khi ra vào vì lý do công việc, phải được sự phê duyệt của người có thẩm quyền và có giám sát.

2.9. **Cán bộ quản lý**: Cán bộ có quyết định bổ nhiệm vào vị trí quản lý của Công ty, bao gồm nhưng không giới hạn: Tổng giám đốc, Trưởng/Phó giám đốc các đơn vị sản xuất phần mềm (BU), Trưởng/phó phòng ban chức năng (BA).

Điều 3. Nhiệm vụ của các phòng ban chức năng, cán bộ quản lý và CBNV.

3.1. Nhiệm vụ của bộ phận Bảo mật thông tin (sau đây viết tắt là BMTT)

3.1.1. Tổ chức xây dựng, triển khai và kiểm soát hệ thống BMTT của Công ty, đảm bảo quản lý được rủi ro và chịu trách nhệm được đến mức độ dự án.

3.1.2. Kiểm tra, đánh giá sự tuân thủ với hệ thống quản lý BMTT của các bộ phận, CBNV và đưa

ra biện pháp xử lý triệt để cho các trường hợp có vi phạm và đề xuất dự phòng cho tương lai.

3.1.3. Tổ chức chuẩn bị các chương trình và tài liệu đào tạo về BMTT.

3.1.4. Làm việc với các tổ chức bên ngoài về các vấn đề liên quan đến BMTT của Công ty.

3.1.5. Định kỳ hàng năm, xem xét và cập nhật Quy định này.

3.2. Nhiệm vụ của bộ phận CNTT

3.2.1. Xây dựng, phát triển, vận hành, quản lý và bảo đảm hạ tầng mạng và hệ thống thôn tin của Công ty.

3.2.2. Xây dựng, triển khai, báo cáo về hệ thống giám sát, kiểm soát việc truy cập hệ thống thông tin, nhằm ngăn ngừa việc truy cập bất hợp pháp vào máy tính, hệ thống thông tin, và các dịch vụ mạng của Công ty.

3.2.3. Xây dựng, triển khai, báo cáo về hệ thống thông tin, hệ thống mạng, hệ thống sao lưu dữ liệu, ghi nhật ký hệ thống và truy nhập, theo dõi đường truyền, bảo vệ tấn công hệ thống mạng và hệ thống thông tin.

3.2.4. Đề xuất và áp dụng các giải pháp kỹ thuật trong BMTT.

3.2.5. Phối hợp với bộ phận BMTT để áp dụng các chính sách BMTT liên quan đến thiết bị CNTT, mạng nội bộ, hệ thống thống tin, máy chủ và kết nối internet.

3.3. Nhiệm vụ của bộ phận Hành chính – Tài sản

3.3.1. Chịu trách nhiệm bảo mật về mặt vật lý và môi trường làm việc, gồm cả hệ thống điện, điều hòa, phòng cháy chữa cháy.

3.3.2. Quản lý và báo cáo tài sản vật lý, trang thiết bị văn phòng trong Công ty.

3.3.3. Quản lý và báo cáo hệ thống cửa từ và quyền truy cập, hệ thống camera và quyền truy cập.

3.3.4. Quản lý các nhà cung cấp dịch vụ khi truy cập vào khu vực làm việc của Công ty và đảm bảo họ hiểu và tuân thủ quy định BMTT của Công ty.

3.4. Nhiệm vụ của bộ phận Nhân sự

3.4.1. Tổ chức ký Cam kết BMTT cho CBNV và quản lý hồ sơ này.

3.4.2. Đưa ra yêu cầu tạo các tài khoản truy nhập hệ thống thông tin cho CBNV mới, sau khi ký cam kết BMTT và hợp đồng lao động.

3.4.3. Đưa ra yêu cầu cắt hay cập nhật tài khoản của CBNV ngày khi CBNV chấm dứt, tạm dừng hay thay đổi hợp đồng lao động, thay đổi vị trí công tác.

3.4.4. Duy trì và xem xét danh sách tài khoản nhân viên của Công ty.

3.5. Nhiệm vụ của bộ phận Tuyển dụng và Đào tạo

3.5.1. Tổ chức đào tạo BMTT cho CBNV ở cấp Công ty.

3.6. Nhiệm vụ của bộ phận Đảm bảo chất lượng (PQA)

3.6.1. Đánh giá nội bộ và kiểm soát việc tuân thủ các yêu cầu BMTT ở mực dự án.

3.6.2. Lập danh sách các dự án quan trọng, phối hợp với bộ phận BMTT xem xét đánh giá yêu cầu BMTT của dự án.

3.7. Nhiệm vụ của bộ phận quản lý ở mỗi cấp đơn vị

3.7.1. Đánh giá rủi ro trước khi phê duyệt các yêu cầu đặc biệt về việc sử dụng thông tin, tài sản, quyền truy cập thông tin quyền truy cập hệ thống thông tin.

3.7.2. Phổ biến, nâng cao nhận thức của CBNV trong đơn vị mình về BMTT.

3.7.3. Chịu trách nhiệm cao nhất về BMTT tại đơn vị mình phụ trách, đảm bảo CBNV mà mình

quản lý tuân thủ các trách nhiệm của họ được quy định trong Quy định này.

3.7.4. Phối hợp với bộ phận BMTT xử lý sự cố nếu có.

3.8. Nhiệm vụ của CBNV

3.8.1. CBNV phải nắm được các yêu cầu về BMTT được quy định tại các tài liệu về BMTT như: chính sách BMTT, Quy định BMTT, mô tả quy trình, mô tả công việc (nếu có), hướng dẫn công việc (nếu có), Biểu mẫu và các tài liệu được khách hàng cung cấp …

3.8.2. CBNV phải hiểu đầy đủ và tuân thủ các yêu cầu này.

CHƯƠNG II. QUY ĐỊNH BẢO MẬT THÔNG TIN

Điều 4. Sử dụng thông tin bảo mật

4.1. Chỉ được sử dụng thông tin bảo mật cho đúng người cần truy cập và cho mục đích công việc liên quan đếm hoạt động sản xuất kinh doanh của Công ty.

4.2. Không được tiết lộ cho bất kỳ bên thứ ba nào những thông tin bảo mật mà CBNV được biết một cách chính thức hoặc không chính thức.

4.3. Không được sử dụng thông tin bảo mật cho bất kỳ mục đích cá nhân nào (lập hồ sơ xin việc, chia sẻ thông tin với bạn be, người thân).

4.4. Chỉ được sử dụng thông tin cá nhân cho công việc ở mức tối thiểu cần thiết. Không được cung cấp thông tin cá nhân của khách hàng, đối tác hoặc CBNV ra bên ngoài Công ty hoặc cho những người không liên quan đến công việc mà không được người có thẩm quyền của Công ty phê duyệt.

4.5. Tuyệt đối không được tải lên hoặc lưu trữ thông tin bảo mật của Công ty trên website, ổ lưu trữ internet công cộng hay cá nhân.

4.6. Tuyệt đối không được tải lên hoặc lưu trữ các tài sản thông tin của khách hàng, Công ty lên môi trường Internet công cộng bao gồm nhưng không giới hạn: Google drive.

4.7. Phải lưu thông tin quan trọng, thông tin bảo mật trên server hoặc hệ thống lưu trữ của Công ty, không được lưu trữ trên ổ lưu trữ cục bộ hay các thiết bị di động.

4.8. Khi kết thúc công việc trong một dự án, các thông tin liên quan đến dự án phải được lưu trên server của dự án, không được lưu các thông tin này tại máy tính hoặc các thiết bị di động.

4.9. Tùy theo yêu cầu của dự án, khi kết thúc dư án, các thông tin liên quan đến dự án có thể phải xóa bỏ khỏi máy tính, email và các nơi lưu trữ khác theo yêu cầu của người có thẩm quyền của dự án hoặc Công ty.

4.10. Công ty được toàn quyền sử dụng, truy cập vào thông tin, dữ liệu, máy tính, hệ thống thông tin, mang, ứng dụng, phần mềm, email, trang web và dữ liệu có liên quan đến địa điểm làm việc, khu vực làm việc của Công ty. Theo đó, tất cả CBNV đồng ý với việc thu thập, truy cập, sử dụng và theo dõi giám sát đó.

Điều 5. Mang tài sản, thông tin ra ngoài

5.1. Không được mang tài sản, thông tin của khách hàng hoặc Công ty ra ngoài khu vực làm việc.

5.2. Phải xin phép và được sự phê duyệt của người có thẩm quyền và chỉ mang ra các tài sản, thông tin cần thiết đã được phê duyệt, khi cần thiết phải mang tài sản, thông tin cả Công ty hoặc khách hàng ra ngoài.

5.3. Khi mang tài sản, thông tin của khách hàng hoặc Công ty ra ngoài phải áp dụng các biện pháp

bảo mật phù hợp.

Điều 6. Làm việc từ xa và thiết bị di động

6.1. Nhu cầu làm việc từ xa, làm việc ở nhà phải xin phép và được sự phê duyệt của Trưởng/Phó giám đốc các đơn vị sản xuất phần mềm (BU), Trưởng/phó phòng ban chức năng (BA). Khi làm việc từ xa, làm việc ở nhà, CBNV phải chịu trách nhiệm trong việc bảo mật, bảo vệ thông tin như khi làm việc tại Công ty.

6.2. Phải tuân thủ hướng dẫn, quy trình của bộ phận ISMS về việc cài đặt, sử dụng đối với các thiết bị di động, kết nối từ xa tới hệ thống thông tin của Công ty. Nghiêm cấm việc thiết lập kết nối từ xa, từ nhà vào máy tính tại Công ty nếu chưa được sự kiểm soát tự bộ phận ISMS.

Điều 7. Cam kết và đào tạo về bảo mật thông tin

7.1. CBNV phải tuân thủ cam kết BMTT ghi trong hợp đồng lao động với Công ty hoặc phải ký thêm cam kết BMTT khi được yêu cầu.

7.2. CBNV có thể phải ký và tuân thủ cam kết BMTT với khách hàng như là yêu cầu BMTT của khách hàng.

7.3. CBNV phải tham gia các khóa đào tạo về BMTT do Công ty tổ chức. Tùy thuộc vào tình hình thực tế, Tổng Giám đốc có thể quyết định tần suất đào tạo về BMTT, nhưng ít nhất 1 năm 1 lần.

7.4. Cán bộ quản lý đơn vị, khi thuê nhân lực từ bên ngoài, phải có trách nhiệm ký cam kết bảo mật thông tin và đảm bảo bảo mật thông tin cho nhân lực được thuê.

7.5. CBNV phải tuân thủ nguyên tắc làm việc, nguyên tắc BMTT tại nơi làm việc của khách hàng.

Điều 8. Sử dụng tài sản sở hữu cá nhân có công việc

8.1. Không được tự ý sử dụng tài sản sở hữu cá nhân (thiết bị di động, máy tính và thiết bị mạng) cho mục đích công việc. Khi có nhu cầu sử dụng thiết bị trên, CBNV phải xin phép sử dụng và được phê duyệt của người có thẩm quyền trước khi sử dụng.

8.2. Tài sản sở hữu cá nhân, có kết nối với hệ thống thông tin của Công ty, trước khi sử dụng phải được bộ phận ISMS xem xét, kiểm tra, cấu hình, cài đặt phần mềm anti-virus và kiểm soát máy tính phù hợp.

Điều 9. Quản lý tài khoản mật khẩu

9.1. Tài khoản Công ty phải là độc nhất, không dùng chung hay phổ biến, xác định được người dùng và chỉ được sử dụng bởi người đã được chỉ định. Tài khoản phải được cập nhật quyền truy cập ngay khi CBNV thay đổi vị trí và trách nhiệm.

9.2. Danh sách CBNV Công ty, nhà cung cấp, đối tác kinh doanh, có quyền truy cập vào thông tin bảo mật của Công ty được duy trì và xem xét định kỳ ít nhất ít nhất 1 năm 1 lần.

9.3. CBNV phải sử dụng tài khoản Công ty mà không có quyền quản trị cho hoạt động thường ngày

(bao gồm truy cập internet và email) và sử dụng tài khoản cục bộ riêng biệt có quyền quản trị các hoạt động yêu cầu tạm quyền cao.

9.4. Không cho người khác sử dụng tài khoản Công ty truy cập hệ thống thông tin của Công ty và không được tiết lộ bất kỳ mật khẩu cá nhân nào.

9.5. Không cho người khác sử dụng tài khoản hoặc tiết lộ mật khẩu khách hàng hoặc bên thứ ba cung cấp cho mình quản lý để truy cập vào hệ thống thông tin của khách hàng hoặc bên thứ ba.

9.6. Không được sử dụng hay truy nhập vào hệ thống thông tin của Công ty bằng tài khoản người khác.

9.7. Không được sử dụng hay khi nhập vào hệ thống thông tin của khách hàng hoặc của bên thứ ba bằng bằng tài khoản người khác

9.8. Phải tuân thủ chính sách về thiết lập và đổi mật khẩu của Công ty. Không đặt và sử dụng mật khẩu quá đơn giản, dễ suy đoán.

9.9. Phải tuân thủ chính sách về thiết lập và đổi mật khẩu của khách hàng hoặc bên thứ ba khi tài khoản và mật khẩu được cung cấp bởi hoặc bên thứ ba.

9.10. Không vô tình tìm kiếm hay dò mật khẩu của người khác.

Điều 10. Ra vào địa điểm làm việc

10.1. Mỗi CBNV được cấp một thẻ từ có ảnh ra vào khu làm việc. CBNV phải có trách nhiệm giữ gìn bảo quản thẻ từ của mình. Không được phép mượn thẻ từ của người khác hoặc cho người khác hoặc cho người khác sử dụng thẻ từ của mình để ra vào nơi làm việc.

10.2. CBNV phải luôn đeo thẻ tại địa điểm làm việc.

10.3. Khi quên thẻ, mất thẻ CBNV phải thông báo với cán bộ quản lý thẻ trong vòng 2 giờ để xử lý và làm thủ tục mượn thẻ tạm tại bộ phận hành chính. CBNV phải trả lại thẻ tạm đã mượn trong vòng 7 ngày làm việc. Cán bộ quản lý thẻ cho mượn thẻ có trách nhiệm ghi nhận lại thời gian mượn, trả thẻ.

10.4. Tuân thủ các biển báo cấm, biển chỉ dẫn tại địa điểm làm việc. Trong khu làm việc có một số khu vực bảo mật, ODC, chỉ dành cho những người được giao nhiệm vụ làm việc trong khu vực này. CBNV nếu không được phép ra vào khu vực bảo mật, tuyệt đối không được mượn thẻ hoặc tìm cách để vào khu vực này vì bất kỳ lý do gì

10.5. Người chịu trách nhiệm của bộ phận hành chính văn phòng có trách nhiệm bố trí sổ theo dõi khách ra vào ở những nơi có hệ thống thẻ từ riêng.

Điều 11. Sử dụng các thiết bị ghi hình, ghi âm, chụp ảnh

11.1. Không được tự ý sử dụng các thiết bị ghi hình, ghi âm (bao gồm nhưng không giới hạn: máy ảnh, máy quay phim, máy ghi âm, điện thoại hay thiết bị cầm tay có chức năng chụp ảnh, quay phim hoặc các loại máy thiết bị khác có tính năng hoặc chức năng tương tự) tại khu vực có dấu hiệu cấm chụp ảnh, quay phim, ghi âm như các khu vực bảo mật, ODC hoặc khu vực có

thông tin khách hàng tại địa điểm của Công ty hoặc khách hàng.

11.2. Phải xin phép và được sự đồng ý của người có thẩm quyền khi chụp ảnh, ghi hình, ghi âm ở các khu vực nnêu ở mục 11.1 trên.

Điều 12. Sử dụng máy in, máy hủy giấy

12.1. Tất cả máy in trong Công ty chỉ phân quyền in cho cá nhân hay nhóm người xác định.

12.2. Không được sử dụng máy in của Công ty để in tài liệu không cần thiết cho công việc.

12.3. Khi cần hủy vật liệu hoặc hồ sơ bảo mật phải sử dụng máy hủy giấy.

Điều 13. Sử dụng máy fax

13.1. Không được fax hồ sơ mà không có sự cho phép của người có thẩm quyền.

13.2. Không được gửi thông tin bảo mật bằng máy fax.

Điều 14. Bảo bảo quản tài liệu hồ sơ bản cứng

14.1. Không được để tài liệu, hồ sơ bảo mật bừa bãi ở các nơi công cộng như máy in, máy photocopy, phòng họp, bàn làm việc, trong tủ không khóa.

14.2. Phải phân loại, sắp xếp, bảo quản và lưu trữ tài liệu, hồ sơ bản cứng cần bảo mật trong tủ có khóa và đảm bảo người khác không thể tiếp cận được.

Điều 15. Vận chuyển thông tin

15.1. Khi gửi tài liệu, thiết bị có chứa thông tin mật phải sử dụng dịch vụ vận chuyển có uy tín và có đảm bảo trừ trường hợp khẩn cấp. Phải xác nhận với người nhận về nội dung tài liệu và thời gian nhận tài liệu.

15.2. Khi vận chuyển tài liệu hay thiết bị có chứa thông tin mật, CBNV phải luôn mang theo bên mình và thực hiện các biện pháp bảo mật phù hợp.

Điều 16. Sử dụng máy tính và thiết bị CNTT

16.1. Chỉ được sử dụng máy tính và thiết bị CNTT cho Công ty cấp vào mục đích công việc và tuân thủ theo các yêu cầu của Công ty về cài đặt, sử dụng và bảo quản.

16.2. Không được tự ý tháo lắp máy tính và các thiết bị CNTT, trong trường hợp cần cài đặt hay sửa chữa, phải liên hệ với bộ phận ISMS để nhận được sự trợ giúp.

16.3. Phải cài đặt screen saver không quá 5 phút. Phải khóa màn hình máy tính khi ra khỏi chỗ ngồi hoặc khi ra khỏi khu vực làm việc.

16.5. Phải tắt máy và các thiết bị trước khi ra về. Khi có nhu cầu bật máy qua đêm vì lý do công việc đăng ký với bộ phận hành chính và xin phép Hồng Vân năng liên quan.

16.6. Không được chia sẻ ổn lưu trữ cục bộ, thư mục, files trên máy tính qua mạng có dây, không

dây hay phần mềm.

16.7. Không sử dụng chung máy tính

16.8. Khi đơn vị có máy tính hay thiết bị CNTT dùng chung, cán bộ quản lý đơn vị phải phân công người quản lý và kiểm tra định kỳ.

Điều 17. Sử dụng phần mềm

17.1. Chỉ được sử dụng những phần mềm có trong danh mục phần mềm được phép sử dụng của Công ty.

17.2. Nghiêm cấm sử dụng các phần mềm trong danh sách bị cấm theo quy định của Công ty.

17.3. Nghiêm cấm sử dụng hoặc thử nghiệm bất kỳ dạng phần mềm thăm dò, theo dõi, tấn công, truy cập trái phép Công ty.

17.4. Nghêm cấm sử dụng các loại phần mềm sử dụng mạng ngang hàng peer-to-peer, các phần mềm chia sẻ dữ liệu, phần mềm chia sẻ màn hình.

17.5. Nghiêm cấm sử dụng phần mềm và website để vượt qua Proxy hoặc Firewall của Công ty bao gồm nhưng không giới hạn: Tor, FreeGate, UltraSurf, Proxifier, HotspotShield hoặc các phần mềm khác có tính năng hoặc chức năng tương tự dưới mọi hình thức, kể cả phục vụ mục đích công việc.

Điều 18. Sử dụng các thiết bị di động, thiết bị mạng và ngoại vi

18.1. Các thiết bị di động kết nối với hệ thống mạng hoặc các dịch vụ CNTT của Công ty phải đáp ứng các yêu cầu bảo mật của Công ty và hướng dẫn của bộ phận ISMS trong quá trình đăng ký sử dụng quá trình cài đặt các biện pháp bảo vệ như cài đặt mật khẩu chuyên nghiệp thiết bị mã hóa dữ liệu sử dụng khóa dây quá trình sử dụng quá trình hủy đăng ký

18.2. nghiêm cấm việc sử dụng các thiết bị có chức năng tạo kết nối mạng phát sóng wi-fi để làm tâm đối cho các thiết bị khác kết nối vào mạng của Công ty hay ra Internet

18.3. Cá nhân và đơn vị muốn sử dụng các thiết bị mạng khác đều phải đăng ký sử dụng trong Công ty và được cấu hình và quản lý bởi bộ phận ISMS.

Điều 19 Sử dụng email Công ty

19.1. Hệ thống Email là tài sản Công ty, được cung cấp để phục vụ cho việc vận hành và quản trị của Công ty.

19.2. 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 tại Công ty.

19.3. Các hệ thống email miễn phí như: Gmail, Hotmail,… bị cấm sử dụng, cấm gửi, cấm nhận tại Công ty.

19.4. Trước khi gửi mail phải kiểm tra địa chỉ người nhận (To, Cc, Bbcc), tiêu đề, nội dung email, file đính kèm và chữ ký. Phải quét virus files đính kèm trước khi gửi.

19.5. Không được sử dụng hệ thống email của Công ty để test; không được tự ý cài đặt email server;

nếu cần cho việc test thì phải xin phép cán bộ quản lý đơn vị và cán bộ quản lý bộ phận ISMS.

19.6. Không được sử dụng tài khoản email của người khác, không mượn hay cho mượn tài khoản email.

19.7. Không giả mạo email, bẻ khóa mật khẩu, xâm nhập, tấn công hoặc gửi email hàng loạt đến hệ thống email của Công ty hay hệ thống email khác.

19.8. Không được gửi email hoặc chuyển tiếp email có nội dung mang tính xúc phạm, công kích một cá nhân hay một tổ chức hoặc chống lại, đi ngược lại với truyền thống hoặc tập quán dân tộc, thông tin xâm phạm đến an ninh quốc gia.

19.9. Không được chuyển tiếp email cho cá nhân hay mailing list mà không được phép từ người gửi email lần đầu.

19.10. Không được chuyển tiếp thủ công hoặc tự động email của Công ty đến hệ thống email bên ngoài.

19.11. Không được sử dụng địa chỉ email của Công ty để đăng ký vào các diễn đàn hay mạng xã hội.

19.12. Không được gửi thông tin có mức độ bảo mật “Confidential” qua email. Nếu gửi thông tin có mức độ bảo mật “Confidential” qua email thì phải được phép của người có thẩm quyền và phải mã hóa thông tin hoặc zip và đặt mật khẩu. Mật khẩu giải mã phải được gửi bằng email hoặc bằng phương tiện khác.

19.13. Không mở email lừa đảo hoặc email có các dấu hiệu đáng ngờ như tên miền email không phải của Công ty đáng tin cậy. email không chỉ định một người nhận cụ thể, email có lỗi chính tả và ngữ pháp.

19.14. Không nhấp vào các liên kết trong các email lừa đảo hoặc email đáng ngờ; tuyệt đối không trả lời email lừa đảo hoặc đáng ngờ; hoặc cung cấp thông tin cá nhân, tên đăng nhập và mật khẩu.

19.15. Báo cáo cho bộ phận ISMS khi nhận được email lừa đảo hoặc email đáng ngờ.

19.16. Không được lợi dụng hệ thống email của Công ty. Những hành động được coi là lợi dụng bao gồm, nhưng không giới hạn: sử dụng email cho việc kinh doanh cá nhân, tìm kiếm cơ hội nghề nghiệp bên ngoài Công ty, tham gia vào các hoạt động kiếm tiền trên mạng, tham dự vào các hoạt động mang tính chính trị hoặc kêu gọi gây quỹ với lý do tôn giáo hoặc bất kỳ một hoạt động nào khác có tính chất tương tự.

19.17. CBNV muốn sử dụng thiết bị di động thông tin để truy cập hệ thống email của Công ty thì phải đăng ký với bộ phận ISMS và tuân thủ hướng dẫn của bộ phận ISMS về việc cài đặt mật khẩu thiết bị và mã hóa dữ liệu.

19.18. Khi thay đổi vị trí công việc CBNV phải bàn giao lại cho người có trách nhiệm mailing list và địa chỉ email đặc biệt do mình quản lý, nếu có.

Điều 20. Sử dụng mạng nội bộ, hệ thống thông tin, máy chủ và kết nối internet

20.1. Quyền truy cập vào hệ thống thông tin, ứng dụng, chức năng, dữ liệu được cung cấp, ủy quyền và kiểm soát dựa trên nguyên tắc “đúng vị trí”, “đủ để biết”, “đủ để sử dụng”. “đủ để làm việc” của CBNV. CBNV chỉ được truy cập vào những thông tin hay dữ liệu mà mình được phép thông qua việc phân quyền truy nhập của người có thẩm quyền của Công ty hoặc khách hàng.

20.2. Người có thẩm quyền phân quyền truy nhập hệ thống thông tin hoặc dữ liệu phải có trách

nhiệm đánh giá rủi ro trước khi thực hiện và kiểm tra lại sau khi thực hiện để đảm bảo việc phân quyền là đúng đối tượng, đúng phạm vi "đủ để làm việc".

20.3. Không được sử dụng nội bộ, hệ thống thông tin, máy chủ và đường truyền internet vào mục đích khác ngoài công việc.

20.4. Các máy chủ cung cấp dịch vụ ra internet phải được kiểm tra và quản lý bởi bộ phận ISMS.

20.5. Không được tự ý cài đặt các máy chủ công cụ cung cấp dịch vụ như Web, FPT, SVN, Proxy, Firewall, DC, DNS, DHCP…

20.6. Không tự ý cấu hình mạng, không tự ý thiết lập kết nối internet cho các máy tính trong mạng nội bộ Công ty.

20.7. Không được truy cập vào các website không liên quan đến mục đích công việc, không được sử dụng các trang proxy trung gian truy nhập Internet của Công ty hoặc khách hàng.

20.8. Không được dùng công cụ trực tuyến hoặc website công cộng để chuyển đổi ngôn ngữ có chứa thông tin bảo mật của Công ty. Chỉ được dùng công cụ hoặc website cho Công ty phát triển, cung cấp hoặc cho phép để dịch tài liệu có chứa thông tin bảo mật của Công ty.

20.9. Không được lợi dụng hạ tầng mạng, thiết bị và tài nguyên của Công ty cho mục đích ngoài công việc. Hành động lợi dụng bao gồm nhưng không giới hạn: kinh doanh cá nhân, tìm kiếm cơ hội nghề nghiệp bên ngoài Công ty, tham gia các hoạt động kiếm tiền trên mạng, tham dự vào các hoạt động mang tính chính trị, hoặc kêu gọi gây quỹ với lý do tôn giáo hoặc bất kỳ một hoạt động nào khác có tính chất tương tự.

20.10. Không được tấn công vào mạng hoặc máy chủ của Công ty; hoặc lợi dụng hạ tầng mạng, thiết bị và tài nguyên của Công ty để tấn công vào mạng hoặc máy chủ bên ngoài.

20.11. Việc sử dụng dịch vụ Điện toán đám mây cho mục đích công việc phải được trưởng bộ phận ISMS phê duyệt.

Điều 21. Phòng chống virus và cập nhật chương trình

21.1. Máy tính và các thiết bị CNTT khi sử dụng trong mạng Công ty và được cài đặt và cập nhật phần mềm phòng chống virus phiên bản mới nhất và thực hiện quét virus định kỳ theo hướng dẫn của bộ phận ISMS. CNBV không được phép tắt hay xóa phần mềm này.

21.2. Máy tính và các thiết bị CNTT khi sử dụng trong mạnh Công ty được cập nhật các bản vá lỗi hệ điều hành và phần mềm một cách tự động. CBNV phải có trách nhiệm kiểm tra việc này và báo cáo bộ phận ISMS khi có lỗi xảy ra.

21.3 Khi nhờ máy tính bị nhiễm virus thì ngay lập tức ngắt kết nối mạng (tháo dây mạng, tắt kết nối wi-fi), thông báo cho bộ phận ISMS và phối hợp thực hiện xử lý.

21.4. Không được phát tán các chương trình độc hại (như virus, sâu, trojan, bom thư …) từ máy tính bị và/hoặc thiết bị của Công ty hoặc vào mạng và/ hoặc máy chủ của Công ty.

Điều 22. Sử dụng tài sản của khách hành

22.1. Tài sản của khách hàng cung cấp (hạ tầng, hệ thống thông ti,n ứng dụng, phần mềm, kết nối mạng, máy chủ, internet, thiết bị, mật khẩu, email …) được coi là tài sản của khách hàng để

phục vụ cho việc vận hành và quản trị của Công ty hoặc khách hàng.

22.2. Tuân thủ chính sách hoặc hướng dẫn quản lý tài sản của khách hàng khi được cung cấp hoặc sử dụng.

22.3. Tuân thủ chính sách hoặc hướng dẫn quản lý tài sản của Công ty đối với tài sản của khách hàng nếu khách hàng không cung cấp

22.4. Sử dụng và bảo quản thiết bị, tài khoản, mật khẩu, email, quyền truy cập … được phân quyền sử dụng trên nguyên tắc "đủ để làm việc".

22.5. Không được lợi dụng tài sản của khách hàng. những hành động được coi là lợi dụng bao gồm, nhưng không giới hạn: sử dụng sai mục đích, kinh doanh cá nhân, tìm kiếm cơ hội nghề nghiệp bên ngoài Công ty, tham gia các hoạt động kiếm tiền trên mạng, tham dự vào các hoạt động mang tính chính trị, hoặc kêu gọi gây quỹ với lý do tôn giáo hoặc bất kỳ một hoạt động nào khác có tính chất tương tự.

22.6. Không được tấn công vào mạng hoặc máy chủ của khách hàng; hoặc lợi dụng tài sản của khách hàng cung cấp để tấn công vào mạng hoặc máy chủ bên ngoài.

22.7. Bàn giao tài sản của khách hàng, nếu có, cho người có trách nhiệm khi thay đổi vị trí công việc.

Điều 23. Sử dụng các phương tiện truyền thông xã hội

23.1. Không được đăng tải, chia sẻ hoặc tiết lộ thông tin hoặc hình ảnh cần bảo mật của Công ty hoặc khách hàng khi tham gia viết blog, tham gia vào các phương tiện truyền thông xã hội.

23.2. Không được đăng tải, chia sẻ hoặc tiết lộ thông tin cá nhân của khách hàng hoặc hình ảnh của họ trên các phương tiện truyền thông xã hội

23.3. Không được đăng tải, chia sẻ hoặc tiết lộ thông tin hoặc hình ảnh khu vực làm việc của khách hàng, khu vực bị cấm chụp ảnh, quay phim của Công ty trên các phương tiện truyền thông xã hội.

23.4. Không được đăng tải, chia sẻ hoặc tiết lộ thông tin về lịch trình làm việc, địa điểm làm việc, công việc của cá nhân hoặc cán bộ quản lý trên các phương tiện truyền thông xã hội.

Điều 24. Xử lý sự cố bảo mật thông tin

24.1. Khi phát hiện có hiện tượng hoặc sự cố về bảo mật thông tin CBNV có trách nhiệm thông báo ngay cho cán bộ quản lý cấp trên và trưởng Bộ phận BMTT trong vòng 2 giờ để tìm phương hướng giải quyết.

24.2. Tuân thủ yêu cầu khách hàng về báo cáo xử lý sự cố bảo mật thông tin nếu đã thống nhất phương thức xử lý với khách hàng trước đó.

24.3. CBNV phải có trách nhiệm hợp tác xử lý sự cố về BMTT khi được Công ty hoặc khách hàng yêu cầu.

CHƯƠNG III. XỬ LÝ VI PHẠM BẢO MẬT THÔNG TIN

Điều 25. Căn cứ xử lý vi phạm bảo mật thông tin

Việc xác định hình thức xử lý vi phạm BMTT phải dựa trên các căn cứ sau đây:

25.1. Hành vi vi phạm;

25.2. Mức độ nguy cơ, rủi ro: rò rỉ, mất mát thông tin;

25.3. Mức độ thiệt hại thực tế: thiệt hại vật chất và thiệt hại về uy tín, danh tiếng của Công ty;

25.4. Tính chất lỗi: lỗi cố ý, lỗi vô ý.

Điều 26. Các hình thức xử lý vi phạm bảo mật thông tin

CBNV vi phạm quy định bảo mật thông tin thì có thể bị xử lý theo một hay tất cả các hình thức sau đây:

26.1. Hình thức trừ thưởng hoặc phạt tiền

26.2. Tham gia lại các khóa đào tạo về BMTT theo yêu cầu của Công ty

26.3. Hành vi vi phạm sẽ là một trong những yếu tố để đánh giá mức độ hoàn thành nhiệm vụ.

26.4. Hình thức bồi thường thiệt hại theo pháp luật

26.5. CBNV vi phạm còn có thể bị xem xét xử lý kỷ luật theo các hành vì và hình thức xử lý kỷ luật lao động đươc quy định tại Nội quy lao động Công ty.

Điều 27. Xử lý vi phạm bảo mật thông tin

27.1. Trường hợp phát hiện hành vì vi phạm BMTT, bộ phận Bảo mật thông tin có trách nhiệm báo cáo cho cán bộ quản lý cấp trên hoặc Tổng Giám đốc Công ty để kịp thời xử lý

27.2. Quy trình xử lý vi phạm BMTT tuân thủ theo quy định về xử lý kỷ luật lao động tại Nội quy lao động của Công ty.

CHƯƠNG IV. CÁC ĐIỀU KHOẢN THI HÀNH

Điều 28. Trách nhiệm thi hành

28.1. Quy định bảo mật thông tin này có hiệu lực kể từ ngày ký

28.2. Bộ phận Bảo mật thông tin là đầu mối soạn thảo các quy trình thực hiện và hướng dẫn chi tiết, đôn đốc, theo dõi, kiểm tra và đánh giá việc tổ chức thực hiện Quy định này tại các đơn vị trong Công ty.

28.3. Giám đốc, Cán bộ quản lý và tất cả các đơn vị, phòng ban có trách nhiệm tổ chức triển khai thực hiện Quy định này

Điều 29. Sửa đổi, bổ sung Quy định

29.1. Quy định này sẽ được điều chỉnh, sửa đổi và bổ sung tùy thuộc vào tình hình hoạt động kinh doanh thực tế của Công ty và các nội dung sửa đổi, bổ sung của pháp luật về lao động.

29.2. Việc sửa đổi, bổ sung Quy định này phải có sự tham khảo ý kiến của Ban đảm bảo thông tin,

Ban Nhân sự và sự phê duyệt của Tổng Giám đốc

TỔNG GIÁM ĐỐC

NGUYỄN XUÂN HIẾU

CHƯƠNG V. CÁC MỨC TRỪ THƯỞNG HOẶC PHẠT TIỀN

Chú thích:

I: Hành vi vi phạm lần đầu

II: Hành vi vi phạm từ lần thứ 2 trở đi

Đơn vị tính: VNĐ

STT	***Các hành vi vi phạm***	***Các mức trừ thưởng hoặc phạt tiền***				
		Từ 500.000 đến 1.000.000	*Từ 1.000.000 đến 2.000.000*	*Từ 2.000.000 đến 5.000.000*	*Từ 5.000.000 đến 10.000.000*	*Từ 10.000.000 trở lên*
	Điều 4. Sử dụng thông tin và tài sản của Công ty					
1	Mang thông tin mật ra ngoài, tiết lộ thông tin mật cho người thứ ba mà gây thiệt hại hoặc ảnh hưởng đến hình ảnh, uy tín của Công ty.					I
2	Gửi nhầm thông tin bảo mật cho khách hàng.			I		II
3	Sử dụng thông tin bảo mật, tài sản thông tin cho mục đích cá nhân, mục đích ngoài công việc.		I		II	
4	Cung cấp thông tin cá nhân của khách hàng, đối tác hoặc CBNV ra bên ngoài Công ty hoặc cho người không liên quan đến công việc mà không được người có thẩm quyền của Công ty phê duyệt.				I	II
5	Tải lên hoặc lưu trữ thông tin của Công ty trên Website, ổ lưu trữ internet công cộng, cá nhân, thiết bị di động sở hữu của cá nhân.			I		II
6	Lưu thông tin quan trọng, thông tin bảo mật ngoài nơi lưu trữ của Công ty.		I		II	

7	Không xóa thông tin liên quan đến công việc/dự án ở máy tính hay thiết bị lưu trữ di động khi kết thúc công việc/dự án.	I		II		
8	Không xóa thông tin dự án ở máy tính, email, và các nơi lưu trữ khác nếu khách hàng đã có yêu cầu xóa các thông tin dự án khi kết thúc dự án		I		II	
9	Tải lên hoặc lưu trữ các tài sản thông tin của khách hàng, công ty lên môi trường internet công cộng bao gồm nhưng không giới hạn: google drive, …				I	II
	Điều 5. Mang tài sản, thông tin ra ngoài					
10	Mang tài sản, thông tin của công ty ra ngoài khu vực làm việc khi không xin phép, không được phê duyệt bởi người có thẩm quyền.			I		II
11	Mang tài sản, thông tin của khách hàng ra ngoài khu vực làm việc khi không xin phép, không được phê duyệt bởi người có thẩm quyền.				I	II
12	Không áp dụng các biện pháp bảo mật phù hợp khi mang thông tin, tài sản thông tin của Công ty ra ngoài.		I		II	
13	Không áp dụng các biện pháp bảo mật phù hợp khi mang thông tin, tài sản thông tin của khách hàng ra ngoài.			I		II
	Điều 6. Làm việc từ xa và thiết bị di động					
14	Làm việc từ xa, làm việc ở nhà không xin phép hoặc không được phê duyệt của người có thẩm quyền.		I		II	
15	Khi làm việc từ xa, làm việc ở nhà, không đảm bảo bảo mật, bảo vệ thông tin như khi làm việc tại công ty.		I		II	

16	Không tuân thủ các yêu cầu về cài đặt, sử dụng đối với các thiết bị di động, các kết nối từ xa tới hệ thống thông tin của công ty. Tự ý thiết lập kết nối từ xa, từ nhà vào máy tính tại công ty khi chưa được sự kiểm soát từ bộ phận ISMS		I		II	
	Điều 7. Cam kết và đào tạo về BMTT					
17	CBNV không ký cam kết BMTT khi ký hợp động lao động với công ty		I		II	
18	CBNV không ký cam kết BMTT với khách hàng như là một yêu cầu BMTT của khách hàng.		I		II	
19	Không tham gia các khóa đào tạo về BMTT do Công ty tổ chức trước khi ký hợp đồng và các khóa đào tạo lại định kỳ hàng năm, các khóa đào tạo hướng đối tượng, các khóa đào tạo hướng đặc thù theo yêu cầu của hợp đồng, dự án.		I		II	
20	Cán bộ quản lý đơn vị, khi thuê nhân lực từ bên ngoài không ký cam kết bảo mật thông tin và đào tạo BMTT cho nhân lực được thuê.		I		II	
21	Không tuân thủ nguyên tắc làm việc, nguyên tắc BMTT tại nơi làm việc của khách hàng.				I	II
	Điều 8. Sử dụng tài sản sở hữu cá nhân cho công việc					
22	Sử dụng tài sản sở hữu cá nhân (thiết bị di động, máy tính và thiết bị mạng …) cho mục đích công việc mà không xin phép, không được phê duyệt của người có thẩm quyền trước khi sử dụng.		I		II	
23	Các tài sản sở hữu cá nhân, có kết nối với hệ thống thông tin của Công ty, không được bộ phận ISMS xem xét, kiểm tra, cấu hình, cài đặt phần mềm bảo vệ phù hợp trước khi sử dụng.		I		II	
	Điều 9. Quản lý tài khoản, mật khẩu					

24	Cho người khác sử dụng tài khoản Công ty truy cập vào hệ thống thông tin của Công ty.		I		II	
25	Cho người khác sử dụng tài khoản hoặc tiết lộ mật khẩu truy cập để truy cập vào hệ thóng thông tin của khách hàng hoặc bên thứ ba cung cấp.			I		II
26	Sử dụng hay truy nhập vào hệ thống thông tin của Công ty bằng tài khoản của người khác.		I		II	
27	Sử dụng hay truy nhập vào hệ thống thông tin của khách hàng hoặc bên thứ ba cung cấp bằng tài khoản của người khác.			I		II
28	Không tuân thủ chính sách về thiết lập và đổi mật khẩu của Công ty. Không bảo mật mật khẩu, không đổi mật khẩu, hoặc đặt mật khẩu đơn giản, dễ đoán.	I		II		
29	Không tuân thủ chính sách về thiết lập và đổi mật khẩu của khách hàng hoặc bên thứ ba, trong trường hợp tài khoản và mật khẩu do khách hàng hoặc bên thứ ba cung cấp.		I		II	
30	Cố tình tìm kiếm hay dò mật khẩu của người khác.			I		II
	Điều 10. Ra vào địa điểm làm việc					
31	Mượn thẻ ra/vào của người khác hoặc cho người khác sử dụng thẻ từ của mình để ra vào nơi làm việc, bao gồm CBNV thực hiện việc quẹt thẻ hộ, hoặc CBNV nhờ quẹt thẻ hộ (mức phạt nhân với số lần vi phạm).	I		II		
32	Mở cửa hộ người khác trong Công ty hoặc người ngoài Công ty mà không có bảo lãnh.	I		II		
33	Không đeo thẻ tại địa điểm làm việc.	I		II		
34	Khi quên thẻ, mất thẻ, không thông báo với cán bộ quản lý thẻ trong vòng 2 giờ để xử lý.	I		II		
35	Khi quên thẻ, mất thẻ không mượn thẻ tạm tại bộ phận Hành chính.	I		II		

	Hoặc không trả lại thẻ tạm tại bộ phận hành chính trong vòng 7 ngày làm việc.					
36	Cán bộ quản lý thẻ cho mượn thẻ mà không ghi nhận lại thời gian giao mượn, trả thẻ.	I		II		
37	Ra vào khu vực bảo mật mà không được phép, chưa xin phép. Không tuân thủ các biển báo cấm, biển chỉ dẫn tại địa điểm làm việc của Công ty hoặc khách hàng.		I		II	
38	Cán bộ có trách nhiệm thuộc bộ phận hành chính không bố trí sổ theo dõi ra/vào ở những nơi có hệ thống thẻ từ riêng.	I		II		
	Điều 11. Sử dụng các thiết bị ghi hình, ghi âm, chụp ảnh					
39	Tự ý sử dụng các thiết bị ghi hình, ghi âm tại khu vực có dấu hiệu cấm chụp ảnh, quay phim, ghi âm như các khu vực bảo mật, ODC hoặc khu vực có thông tin khách hàng tại địa điểm của Công ty hoặc khách hàng.		I		II	
40	Không xin phép và không được sự đồng ý của người có thẩm quyền khi chụp ảnh, ghi hình, ghi âm ở các khu vực nêu tại mục 11.1		I		II	
	Điều 12. Sử dụng máy in, máy hủy giấy					
41	Sử dụng máy in của Công ty để in tài liệu không cần thiết cho công việc	I		II		
42	Không sử dụng máy hủy giấy, phương pháp hủy triệt để khi cần hủy tài liệu, hồ sơ bảo mật.	I		II		
	Điều 13. Sử dụng máy fax					
43	Fax tài liệu, hồ sơ mà không có sự cho phép của người có thẩm quyền.	I		II		
44	Gửi thông tin bảo mật bằng máy fax	I		II		
	Điều 14. Bảo quản tài liệu hồ sơ bản cứng					
45	Để tài liệu, hồ sơ cần được bảo mật bừa bãi ở các nơi	I		II		

	công cộng như máy in, máy photocopy, phòng họp, bàn làm việc, trong tủ không khóa.					
46	Không phân loại, sắp xếp, bảo quản và lưu trữ các tài liệu, hồ sơ bản cứng bảo mật trong tủ có khóa và đảm bảo người khác không thể tiếp cận được.	I		II		
	Điều 15. Vận chuyển thông tin					
47	Không sử dụng dịch vụ vận chuyển có uy tín và có đảm bảo khi gửi tài liệu, thiết bị có chứa thông tin mật, trừ trường hợp khẩn cấp.	I		II		
48	Vận chuyển tài liệu hay tài sản có chứa thông tin mật không an toàn dẫn đến mất tài liệu, tài sản, lộ thông tin.			I		II
	Điều 16. Sử dụng máy tính và thiết bị CNTT					
49	Sử dụng máy tính và thiết bị CNTT do Công ty cấp vào mục đích ngoài công việc.	I		II		
50	Tự ý tháo lắp máy tính và các thiết bị CNTT, hoặc không tuân thủ theo các yêu cầu của công ty về cài đặt, sử dụng và bảo quản.	I		II		
51	Không cài đặt screen saver hoặc cài đặt screen saver trên 5 phút.	I		II		
52	Không khóa màn hình máy tính khi ra khỏi chỗ ngồi hoặc khi ra khỏi khu vực làm việc.	I		II		
53	Không tắt máy và các thiết bị trước khi ra về, trừ trường hợp phải để máy qua đêm.	I		II		
54	Bật máy qua đêm vì lý do công việc nhưng không đăng ký với Văn phòng công ty và xin phép phòng ban chức năng liên quan.	I		II		
55	Chia sẻ ổ lưu trữ cục bộ, thư mục, files trên máy tính qua mạng có dây, không dây hay phần mềm.	I		II		
56	Cho người khác mượn máy tính hoặc mượn máy tính của người khác. Sử dụng máy tính đứng tên người khác để làm việc.	I		II		
57	Làm mất laptop, thiết bị, tài sản do Công ty cấp hoặc thuộc sở hữu cá nhân, có chứa thông tin mật, thông tin			I		II

	của khách hàng, thông tin dự án.					
58	Cán bộ quản lý đơn vị không phân công người quản lý và kiểm tra định kỳ đối với máy tính hay thiết bị CNTT dung chung của đơn vị.	I		II		
	Điều 17. Sử dụng phần mềm					
59	Download, bẻ khóa (crack), sử dụng, lưu trữ phần mềm không có bản quyền hoặc không được phép.			I		II
60	Download, bẻ khóa, sử dụng, lưu trữ phần mềm không có bản quyền làm lây nhiễm virus sang mạng nội bộ, mạng của khách hàng hay nhiễm virus vào tài liệu gửi khách hàng hoặc làm ảnh hưởng đến tiến độ dự án.					I
61	Sử dụng các phần mềm trong danh sách bị cấm. Sử dụng hoặc thử nghiệm bất kỳ dạng phần mềm thăm dò, theo dõi, tấn công, truy nhập trái phép trong Công ty.					I
62	Sử dụng các loại phần mềm sử dụng mạng ngang hàng peer -to-peer, các loại phần mềm chia sẻ dữ liệu, phần mềm chia sẻ màn hình.					I
63	Sử dụng phần mềm, website đẻ vượt qua proxy hoặc firewall của Công ty dưới mọi hình thức.					I
	Điều 18. Sử dụng các thiết bị di độngm, thiết bị mạng và ngoại vi					
65	Thiết bị di động kết nối với hệ thống mạng hoặc các dịch vụ CNTT của Công ty không đáp ứng các yêu cầu đăng ký, sử dụng, cài đặt, bảo mật (mật khẩu truy cập, mã hóa dữ liệu ..) của công ty.		I		II	
66	Sử dụng các thiết bị có chức năng tạo kết nối mạng, phát song Wifi để làm cầu nối cho các thiết bị khác kết nối vào mạng của Công ty hay ra Internet.		I		II	
67	Sử dụng thiết bị mạng không được cấu hình và quản lý bởi bộ phận ISMS.		I		II	
	Điều 19. Sử dụng email của Công ty					
68	Sử dụng email của Công ty hoặc email được công ty cho phép cho mục đích ngoài công việc.		I		II	

69	Sử dụng email miễn phí, email cá nhân, email hay hệ thống email khác ngoài email của công ty, khách hàng cung cấp tại công ty.		I		II	
70	Gửi sai địa chỉ người nhận email, sai nội dung email, sai file đính kèm, có virus trong file đính kèm.		I		II	
71	Sử dụng hệ thống email của Công ty để test, tự ý cài đặt email servers.		I		II	
72	Sử dụng tài khoản email của người khác, mượn hay cho mượn tài khoản email.		I		II	
73	Giả mạo email, bẻ khóa mật khẩu, xâm nhập, tấn công đến hệ thống email của công ty hay ngoài công ty.					I
74	Gửi email hàng loạt (spam email) đến hệ thống email của công ty hay ngoài công ty.	I		II		
75	Gửi email hoặc chuyển tiếp email có nội dung mang tính xúc phạm, công kích một cá nhân hay một tổ chức hoặc chống lại, đi ngược lại với truyền thống hoặc tập quán dân tộc, thông tin xâm phạm đến an ninh quốc gia.		I		II	
76	Chuyển tiếp thủ công hoặc tự động email của Công ty đến hệ thống email bên ngoài.			I		II
77	Sử dụng địa chỉ email của Công ty để đăng ký vào các diễn đàn hay mạng xã hội.	I		II		
78	Gửi thông tin có mức độ bảo mật là “Confidential” qua email mà không đặt mật khẩu hoặc mã hóa.	I		II		
79	Mở hoặc nhấp vào các liên kết trong email lừa đảo hoặc đáng ngờ, trả lời các email lừa đảo hoặc đáng ngờ; hoặc cung cấp thông tin cá nhân, tên đăng nhập và mật khẩu. Không báo cáo cho bộ phận ISMS khi nhận được email lừa đảo hoặc đáng ngờ.		I		II	
80	Lợi dụng hệ thống email của công ty. Những hành động được coi là lợi dụng bao gồm, nhưng không giới hạn: sử dụng email cho việc kinh doanh cá nhân, tìm kiếm cơ hội nghề nghiệp bên ngoài Công ty, tham gia vào các hoạt động kiếm tiền trên mạng, tham dự vào các hoạt động mang tính chính trị hoặc kêu gọi gây quỹ với lý do tôn giáo hoặc bất kỳ một hoạt động nào khác có tính chất			I		II

	tương tự.					
81	Không đăng ký với bộ phận ISMS trước khi CBNV sử dụng thiết bị di động để truy cập hệ thống email của Công ty và/hoặc không tuân thủ yêu cầu về việc đặt mật khẩu thiết bị và mã hóa dữ liệu.	I		II		
82	Không bàn giao lại cho người có trách nhiệm mailing list và địa chỉ email đặc biệt do mình quản lý, nếu có, khi thay đổi vị trí công việc.	I		II		
	Điều 20. Sử dụng mạng nội bộ, hệ thống thông tin, máy chủ và kết nối internet					
83	Truy cập vào những thông tin hay dữ liệu mà mình không được phép, không có thẩm quyền, không liên quan đến công việc được giao.		I		II	
84	Người có thẩm quyền phân quyền truy nhập hệ thống thông tin hoặc dữ liệu không đánh giá rủi ro trước khi thực hiện, không kiểm tra lại sau khi thực hiện dẫn đến phân quyền sai đối tượng, sai nguyên tắc “đủ để làm việc”.		I		II	
85	Sử dụng mạng nội bộ, hệ thống thông tin, máy chủ và đường truyền Internet vào mục đích khác ngoài công việc.		I		II	
86	Sử dụng máy chủ cung cấp dịch vụ ra internet không được kiểm tra và quản lý bởi bộ phận ISMS.		I		II	
87	Tự ý cài đặt các máy chủ cung cấp dịch vụ như Web, FTP, SVN, Proxy, Firewall, DC, DNS. DHCP …				I	II
88	Tự ý cấu hình mạng, tự ý thiết lập kết nối internet cho các máy trong mạng nội bộ của Công ty.			I		II
89	Truy cập vào các website không liên quan đến mục đích công việc, sử dụng các trang proxy trung gian truy nhập internet của Công ty hoặc khách hàng.		I		II	
90	Dùng công cụ trực tuyến hoặc website công cộng hoặc công cụ không được phép để dịch hoặc chuyển đổi ngôn ngữ có chứa thông tin bảo mật của Công ty.		I		II	
91	Lợi dụng hạ tầng mạng, thiết bị và tài nguyên của Công			I		II

	ty cho mục đích ngoài công việc bao gồm, nhưng không giới hạn: kinh doanh cá nhân, tìm kiếm cơ hội nghề nghiệp bên ngoài Công ty, tham gia vào các hoạt động kiếm tiền trên mạng, tham dự vào các hoạt động mang tính chính trị hoặc kêu gọi gây quỹ với lý do tôn giáo hoặc bất kỳ một hoạt động nào khác có tính chất tương tự.					
92	Tấn công vào mạng hoặc máy chủ của Công ty hoặc lợi dụng hạ tầng mạng, thiết bị và tài nguyên của Công ty để tấn công vào mạng hoặc máy chủ bên ngoài.					I
93	Sử dụng dịch vụ điện toán đám mây không được sự xem xét và phê duyệt của bộ phận ISMS.		I		II	
	Điều 21. Phòng chống virus và cập nhật chương trình					
94	Tải về, sao chép thông tin, tài liệu từ trên mạng, từ máy tính khác, thiết bị khác và bị lây nhiễm virus.			I		II
95	Máy tính và thiết bị CNTT khi sử dụng trong mạng Công ty không được cài đặt và cập nhật phần mềm phòng chống virus phiên bản mới nhất.		I		II	
96	Phát tán các chương trình độc hại vào mạng và máy chủ.			I		II
97	Tự ý tắt hay xóa chương trình phòng chống virus, cập nhật phiên bản định kỳ, quét virus định kỳ.		I		II	
98	Không kiểm tra việc cập nhật các bản vá lỗi hệ điều hành và phần mềm và báo cáo bộ phận ISMS khi có lỗi xảy ra.	I		II		
99	Không thông báo cho bộ phận ISMS, không ngắt kết nối mạng khi nghi ngờ máy tính bị nghiễm virus và không phối hợp thực hiện xử lý.	I		II		
	Điều 22. Sử dụng tài sản của khách hàng.					
100	Không tuân thủ chính sách hoặc hướng dẫn quản lý tài sản của khách hàng khi được cung cấp hoặc sử dụng. Không sử dụng tài sản của khách hàng theo đúng mục đích chỉ định ban đầu.			I		II

101	Không sử dụng và bảo quản thiết bị, tài khoản, mật khẩu, email, quyền truy cập tài sản của khách hàng được phân quyền sử dụng trên nguyên tắc “đủ để làm việc”.			I		II
102	Lợi dụng tài sản của khách hàng. Những hành động được coi là lợi dụng bao gồm, nhưng không giới hạn: kinh doanh cá nhân, tìm kiếm cơ hội nghề nghiệp bên ngoài Công ty, tham gia vào các hoạt động kiếm tiền trên mạng, tham dự vào các hoạt động mang tính chính trị hoặc kêu gọi gây quỹ với lý do tôn giáo hoặc bất kỳ một hoạt động nào khác có tính chất tương tự.			I		II
103	Tấn công vào mạng hoặc máy chủ của khách hàng hoặc lợi dụng tài sản của khách hàng để tấn cộng vào mạng hoặc máy chủ bên ngoài.					I
104	Không bàn giao tài sản của khách hàng, nếu có, cho người có trách nhiệm khi thay đổi vị trí cộng việc.			I		II
105	Làm mất tài sản khách hàng.				I	II
	Điều 23. Sử dụng các phương tiện truyền thông xã hội					
106	Đăng tải, chỉa sẻ hoặc tiết lộ thông tin hoặc hình ảnh cần bảo mật của Công ty hoặc khách hàng khi tham gia viết blog, tham gia vào các phương tiện truyền thông xã hội.			I		II
107	Đăng tải, chia sẻ hoặc tiết lộ trên phương tiện truyền thông xã hội thông tin cá nhận của khách hàng hoặc hình ảnh của họ.			I		II
108	Đăng tải, chia sẻ hoặc tiết lộ thông tin hoặc hình ảnh khu vực làm việc của khách hàng, khu vực làm việc bị cấm chụp ảnh, quay phim của Công ty trên các phương tiện truyền thông xã hội.		I		II	
109	Đăng tải, chia sẻ hoặc tiết lộ thông tin về lịch trình làm việc, địa điểm làm việc, công việc của cá nhân hoặc cán bộ quản lý trên các phương tiện truyền thông xã hội.		I		II	
	Điều 24. Xử lý sự cố bảo mật thông tin					
110	Không thông báo ngay cho cán bộ quản lý cấp tren hoặc trưởng bộ phận ISMS, trong vòng 2 giờ, khi phát hiện sự		I		II	

	mất mát, các hành vi trộm cắp và tiết lộ trái phép tài sản thông tin của công ty, các dấu hiệu vi phạm, sự cố bảo mật thông tin để tìm phương hướng giải quyết.					
111	Không tuân thủ yêu cầu của khách hàng về báo cáo sự cố bảo mật thông tin, nếu đã có thống nhất trước đó với khách hàng về cách thức xử lý khi có sự cố xảy ra.				I	II
112	Không hợp tác xử lý sự cố về BMTT khi được công ty hoặc khách hàng yêu cầu.		I		II	