QUY ĐỊNH BẢO MẬT THÔNG TIN

MÃ VĂN BẢN: 04/2018/QĐ-ISMS/VTI
PHIÊN BẢN: 1.4
NGÀY HIỆU LỰC:25/08/2020

NGƯỜI LẬP: NGÔ THỊ THU HIỀN
NGƯỜI KIỂM TRA: NGUYỄN THÚY HẰNG
NGƯỜI DUYỆT: ĐÀO THỊ THU HIỀN

Lịch sử cập nhật

*A – Thêm mới; M – Sửa; D – Xoá

Ngày hiệu lực	Mục thay đổi	A* M, D	Mô tả nội dung thay đổi	Lí do thay đổi	Phiên bản
12/2/2018		A	Tạo mới		1.0
16/4/2018	3.4.5, Điều 10, Chương V – mục 5	M, D	**3.4.5**: Update tên bộ phận Hành chính – Nhân sự (GA) **Điều 10**: Bỏ mục 10.2. Truy cập bằng mã truy cập cá nhân **Chương V**: Bổ xung trường hợp 5. Hành vi vi phạm phải áp dụng xử lý/truy tố theo quy định của Pháp luật…	Update theo yêu cầu của bộ phận GA và các quản lý	1.1
1/5/2018	All	M	Update lại font chữ Arial, và font size, dãn cách dòng	Format xấu, không theo chuẩn	1.2
1/10/2018	4.4, Chương V – Điều 4, mục 5	M	Bổ sung điều khoản cấm “Không được sao chép thông tin cá nhân…” và điều khoản phạt khi “Sao chép thông tin cá nhân…”	Bổ sung rõ thêm ràng buộc về sử dụng thông tin cá nhân theo yêu cầu KH	1.3
25/8/2020	Chương V - Điều 5: Mang tài sản, thông tin ra ngoài	M	Bổ sung 5. 4 & 5.5	Mô tả chi tiết hơn về yêu cầu	1.4

Tài liệu liên quan

STT	Mã hiệu	Tên tài liệu
1	07-CS/ISM/VTI	Chính sách Bảo mật Vật lý và Môi trường
2	02-QT/ISM/VTI	Quy trình Xử lý sự cố Bảo mật thông tin
3	04-CS/ISM/VTI	Chính sách Quản lý tài sản

Mục lục

CHƯƠNG I. QUY ĐỊNH CHUNG

Điều 1: Phạm vi và đối tượng áp dụng

1.1. **Phạm vi áp dụng:** "Quy định Bảo mật thông tin" đưa ra quy định cơ bản trong Bảo mật thông tin ở Công ty Cổ phần VTI (sau đây gọi tắt là Công ty).

1.2. **Đối tượng áp dụng:** Đối tượng áp dụng là các cán bộ nhân viên của Công ty (sau đây viết tắt là CBNV) là người lao động ký Hợp đồng thử việc, Hợp đồng đào tạo, Hợp đồng đào tạo thực nghiệm, Hợp đồng lao động theo thời vụ hoặc theo công việc nhất định có thời gian dưới 12 tháng, Hợp đồng lao động xác định thời hạn từ 12 tháng đến 36 tháng, Hợp đồng lao động không xác định thời hạn 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, tri thức về tài sản không được công khai, hoặc bất kì 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; hoặc của khách hàng/đối tác được trao đổi trong quá trình giao dịch kinh doanh với 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 hàng/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 dựng phần mềm như cơ sở dữ liệu, ngôn ngữ lập trình, chương trình dịch, chương trình hỗ 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 hàng/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 cookies, 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, vv.. hoặc khi kết hợp với các thông tin khác có thể nhận dạng được cá nhân cụ thể.

2.8. **Khu vực bảo mật**: là các trung tâm Phát triển phần mềm (ODC), các trung tâm Dữ liệu, các phòng thiết bị mạng, các phòng máy chủ, các hệ thống đa người dùng khác như các phòng thí nghiệm 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 giám sát.

2.9. **Ban Giám đốc (BOD)**: Giám đốc Điều hành và Giám đốc Sản xuất.

2.10. **Cán bộ quản lý (BOM)**: Giám đốc Điều hành, Giám đốc Sản xuất, Trưởng/phó các đơn vị sản xuất (DL/Vice DL), Trưởng/phó các phòng ban chức năng (GA, AF, Solution, QA, Tester, Comtor, ISMS, IT...)

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 (ISMS)**:

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

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

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

3.2. **Nhiệm vụ của bộ phận Công nghệ thông tin (IT)**:

3.2.1. Xây dựng, phát triển, vận hành, quản lý và đảm bảo hạ tầng mạng và hệ thống thông 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 Ban ISMS để áp dụng các chính sách BMTT liên quan đến thiết bị công nghệ thông tin, mạng nội bộ, hệ thống thông tin, máy chủ và kết nối internet.

3.3. **Nhiệm vụ của bộ phận Hành chính – Nhân sự (GA)**:

3.3.1. Chịu trách nhiệm bảo mật về mặt vật lý và môi trường làm việc, bao 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 vân tay-cửa từ và quyền truy cập, hệ thống camera và quyền truy cập.

3.3.4. Theo dõi, quản lý khách/đối tác/nhà thầu ra – vào văn phòng công ty.

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

3.3.6. Chịu trách nhiệm bảo mật về thông tin cá nhân của CBNV.

3.3.7. Đảm bảo toàn bộ CBNV được kí Cam kết BMTT ngay giai đoạn kí Hợp đồng lao động (các loại ngắn hạn và dài hạn, hợp đồng thời vụ) và được tham gia đào tạo đầy đủ kiến thức về BMTT từ Ban ISMS.

3.3.8. Đảm bảo CBNV hiểu được trách nhiệm của mình và có kiến thức/kỹ năng phù hợp với vai trò mà họ đang nắm giữ.

3.3.9. Đảm bảo việc kiểm tra kiến thức, trình độ và kinh nghiệm của tất cả các ứng viên được tiến hành theo đúng các luật định, chế định và nội quy liên quan, và tương ứng với các yêu cầu kinh doanh, với đúng phân loại thông tin được truy cập và với các rủi ro về nhận thức.

3.3.10. Phối hợp với bộ phận ISMS thực hiện các hình thức xử lý kỷ luật chính thức và công khai với CBNV vi phạm quy định về BMTT của Công ty.

3.3.11. Đảm bảo CBNV phải được truyền đạt về trách nhiệm và nhiệm vụ BMTT theo Cam kết BMTT đã kí sau khi kết thúc hoặc thay đổi công việc. Các cam kết BMTT cần được đảm bảo có hiệu lực. Trong trường hợp cần thiết phải tiến hành các biện pháp bảo vệ quyền lợi của tổ chức, có thể bao gồm cả tố tụng, theo đúng quy định/quy trình BMTT của Công ty và Pháp luật sở tại.

3.4. **Nhiệm vụ của bộ phận Đảm bảo chất lượng (QA)**:

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

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

3.5. **Nhiệm vụ của Cán bộ quản lý ở mỗi cấp đơn vị**:

3.5.1. 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.

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

3.5.3. Chịu trách nhiệm cao nhất về BMTT tại đơn vị mình phụ trách.

3.5.4. Phối hợp với Ban ISMS xử lý sự cố nếu có.

3.6. **Nhiệm vụ của CBNV**:

3.6.1. CBNV phải nắm được các yêu cầu về BMTT được quy định tại các tài liệu về BMTT như: Chính sách BMTT, Quy định Bảo mật thông tin, mô tả quá trình, mô tả công việc, hướng dẫn công việc, biểu mẫu và các tài liệu được khách hàng cung cấp…

3.6.2. CBNV phải hiểu đầy đủ, tuân thủ các yêu cầu này.

3.6.3. CBNV cần phải hoàn thành việc ký Cam kết BMTT trước khi tham gia các hoạt động tại Công ty, và đảm bảo rằng việc tuân thủ Cam kết BMTT vẫn được thực hiện theo đúng nguyên tắc và thời gian quy định ở Cam kết BMTT với Công ty.

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 **đúng mục đích công việc** liên quan đến 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 bè, 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. Không

được sao chép thông tin cá nhân khi chưa được người có thẩm quyền của Công ty, hoặc chủ sở hữu của thông tin phê duyệt.

4.5. Tuyệt đối không được tải lên hoặc lưu trữ thông tin của Công ty có mức bảo mật từ Medium (M) hoặc "Internal Use", hoặc "Nội bộ" trở lên trên các website, mạng xã hội, ổ lưu trữ công cộng hay cá nhân trên internet.

4.6. Phải lưu thông tin quan trọng, thông tin bảo mật có mức bảo mật từ High (H), hoặc ""Confidential", hoặc "Bảo mật" trở lên trên file-server hoặc hệ thống lưu trữ nội bộ của Công ty, không được phép lưu trên ổ cứng máy tính hay thiết bị di động, trên các website, mạng xã hội, ổ lưu trữ công cộng hay cá nhân trên internet.

4.7. Khi kết thúc công việc trong một dự án, các thông tin liên quan đến dự án phải được lưu trên file-server của dự án, không được phép lưu các thông tin này tại máy tính.

4.8. Tùy theo yêu cầu của dự án, khi kết thúc dự 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.

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 phải mang tài sản, thông tin của 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 cho tài sản, thông tin đó.

5.4. Cán bộ mang tài sản thông tin ra ngoài chịu trách nhiệm về tính toàn vẹn, tính bảo mật của tài sản thông tin và chỉ được sử dụng đúng mục đích công việc.

5.5. Trong trường hợp có yêu cầu tiêu hủy tài sản, thông tin từ Khách hàng, người có thẩm quyền, … thực hiện theo 04-CS-ISM-VTI-Chinh sach Quan ly tai san/ 5.8. Tiêu hủy tài sản.

Điều 6: Làm việc từ xa, ở nhà

6.1. Không được làm việc từ xa, làm việc ở nhà.

6.2. Trong trường hợp có nhu cầu làm việc từ xa, làm việc ở nhà, phải xin phép và được sự phê duyệt của Giám đốc trung tâm sản xuất/Trưởng ban chức năng và đại diện Ban ISMS. 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.

6.3. Phải tuân thủ các yêu cầu về cài đặt, sử dụng đối với các kết nối từ xa tới hệ thống thông tin của Công ty theo hướng dẫn của phòng IT. Nghiêm cấm việc thiết lập kết nối từ xa, từ nhà vào máy tính tại Công ty nếu chưa được sự kiểm soát từ phòng IT.

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

7.1. CBNV phải ký và tuân thủ Cam kết BMTT khi ký Hợp đồng lao động với Công ty.

7.2. CBNV có thể phải ký và tuân thủ Cam kết BMTT với khách hàng như là yêu cầu bảo mật thông tin của khách hàng.

7.3. CBNV phải tham gia các khóa đào tạo về BMTT do Công ty tổ chức trước khi ký hợp đồng lao động và các khóa đào tạo lại định kỳ hàng năm, các khóa đào tạo hướng đối tượng như cho cán bộ quản lý, quản trị dự án, lập trình viên, CBNV đi Onsite, CBNV khối đảm bảo kinh doanh, CBNV làm việc trong các Khu vực bảo mật ODC (Offshore Development Center)…

7.4. Cán bộ quản lý đơn vị, khi thuê nhân lực từ bên ngoài phải có trách nhiệm ký Cam kết BMTT và phối hợp với ban ISMS đào tạo BMTT 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 cho 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.

8.2. Khi có như cầu sử dụng tài sản sở hữu cá nhân vào mục đích công việc, CBNV phải xin phép và được sự phê duyệt của người có thẩm quyền (như Giám đốc trung tâm sản xuất/Trưởng ban chức năng hoặc Quản trị dự án) và đại diện của Ban ISMS trước khi sử dụng.

8.3. Các tài sản sở hữu cá nhân, có kết nối với hệ thống thông tin của Công ty, trước khi sử dụng phải được phòng IT xem xét, kiểm tra, cấu hình, và cài đặt các phần mềm, biện pháp bảo vệ phù hợp.

Điều 9: Quản lý tài khoản, mật khẩu

9.1. 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.

9.2. 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 khách hàng hoặc bên thứ ba.

9.3. Tài khoản sử dụng tại Công ty phải là độc nhất, xác định được người dùng và chỉ được sử dụng bởi người đã được chỉ định.

9.4. CBNV phải sử dụng tài khoản Công ty mà không có quyền quản trị cho hoạt động thường ngày (bao gồm cả việc truy cập internet và email) và sử dụng tài khoản cục bộ riêng biệt có quyền quản trị cho các hoạt động yêu cầu đặc quyền cao.

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

9.6. Không cho người khác sử dụng tài khoản hoặc tiết lộ mật khẩu của 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.

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

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

9.9. Không cố tình tìm kiếm hay dò mật khẩu của người khác.

Điều 10: Ra vào địa điểm làm việc *(Chi tiết tại Chính sách Bảo mật Vật lý và Môi trường)*

10.1. **Truy nhập bằng vân tay**:

10.1.1. Mỗi CBNV được cấp tối thiểu 02 mã vân tay và tối đa 10 mã vân tay để có thể truy cập vào hệ thống vân tay-cửa từ để ra vào khu vực làm việc.

10.1.2. Mã vân tay đại diện duy nhất cho mỗi cá nhân CBNV, thể hiện sự hiện diện và trách nhiệm của cá nhân đó tại khu vực làm việc.

10.1.3. CBNV phải trung thực trong việc đăng ký mã vân tay của mình. Nghiêm cấm việc sử dụng mã vân tay giả để đăng ký vân tay cá nhân. Nghiêm cấm sử dụng mã vân tay giả để giả mạo vân tay của người khác để ra vào khu vực làm việc.

10.1.4. Trong trường hợp có sự cố bất khả kháng, CBNV không thể sử dụng vân tay cũ đã đăng ký để ra vào khu vực làm việc, cần thông báo với cán bộ chuyên trách quản lý Vân tay-Thẻ từ để được hỗ trợ áp dụng phương pháp truy nhập khác.

10.2. **Truy nhập bằng thẻ từ dành cho khách**:

10.2.1. Công ty sử dụng thẻ từ dành cho khách để kiểm soát truy cập vào các khu vực giới hạn, ngăn ngừa các truy cập trái phép. Thẻ từ chỉ được cấp dành cho các đối tượng khách hàng/đối tác/nhà thầu hoặc CBNV thuộc chi nhánh khác đến làm việc tại Công ty có nhu cầu ra vào nhiều lần. Mỗi cá nhân kể trên sẽ chỉ được cấp 01 thẻ từ để ra vào khu vực làm việc hoặc khu vực chung của Công ty.

10.2.2. Khách hàng/đối tác/nhà thầu hoặc CBNV phải xuất trình giấy tờ tùy thân để cán bộ quản lý thẻ ghi lại/sao chụp trước khi tiến hành cho mượn thẻ.

10.2.3. Khách hàng/đối tác/nhà thầu hoặc CBNV được cấp thẻ 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 sử dụng thẻ từ của mình để ra vào khu vực làm việc.

10.2.4. Khách hàng/đối tác/nhà thầu hoặc CBNV phải luôn đeo thẻ tại khu vực làm việc.

10.2.5. Khi quên thẻ, mất thẻ, người được cấp thẻ phải thông báo với cán bộ quản lý thẻ khách để xử lý theo quy định và làm thủ tục mượn thẻ khác.

10.2.6. Khách hàng/đối tác/nhà thầu hoặc CBNV phải trả lại thẻ từ đã mượn trong vòng 05 ngày làm việc tính từ thời hạn cuối cùng trong đăng ký mượn thẻ hoặc ngày cuối cùng làm việc tại Công ty (tùy thời hạn nào đến trước).

10.2.7. Cán bộ quản lý thẻ khách có trách nhiệm ghi nhận lại thời gian mượn - trả thẻ vào Sổ theo dõi mượn – trả thẻ; xử lý vi phạm về việc sử dụng thẻ từ, mất thẻ theo quy định.

10.3. CBNV, khách hàng/đối tác cần tuân thủ các biển báo cấm, biển chỉ dẫn tại địa điểm làm việc. Trong khu vực làm việc có một số khu vực bảo mật (như phòng ODC, phòng server,…), chỉ dành cho những người được giao nhiệm vụ làm việc trong khu vực này. CBNV, khách hàng/đối tác nếu không được phép ra vào khu vực bảo mật, tuyệt đối không được giả mạo vân tay, sử dụng mã truy cập của người khác, hoặc mượn/đánh cắp thẻ để tìm cách vào khu vực này vì bất cứ lý do gì.

10.4. Người chịu trách nhiệm quản lý tiếp đón khách có trách nhiệm bố trí sổ theo dõi khách ra vào văn phòng Công ty, và khu vực bảo mật.

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 và thiết bị khác có chức năng tương tự) tại khu vực có dấu hiệu cấm quay phim, chụp ảnh, ghi âm như trong 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 trước khi chụp ảnh, ghi hình, ghi âm ở các khu vực đã nêu tại mục 11.1 trên.

Điều 12: Sử dụng máy in, máy hủy giấy

12.1. Máy in sử dụng trong Công ty phải được cài đặt phần mềm ghi log, hoặc có chức năng ghi log, 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 tài liệu hoặc hồ sơ có mức độ bảo mật “Credentical”, “Bảo mật” hoặc từ mức Cao (High) trở lên, phải sử dụng máy hủy giấy.

Điều 13: Sử dụng máy scan, máy photocopy

13.1. Không được sử dụng máy scan, máy photocopy để scan, photo tài liệu không cần thiết cho công việc.

13.2. Không được bỏ quên tài liệu tại khay sao chụp của máy scan, máy photocopy, đặc biệt là các tài liệu, hồ sơ bản cứng cần bảo mật.

13.3. Trong trường hợp phát hiện tài liệu bảo mật bị bỏ quên trong khay sao chụp của máy scan, máy photocopy, CBNV cần có trách nhiệm báo cáo và chuyển lại ngay cho Ban ISMS hoặc bộ phận sở hữu tài liệu bảo mật. Nghiêm cấm CBNV sử dụng hoặc chia sẻ, phát tán khi bản thân không được phép hoặc cho những người khác không được phép sử dụng tài liệu bảo mật.

13.4. Khi cần hủy tài liệu bảo mật đã photocopy, phải sử dụng máy hủy giấy.

13.5. File dữ liệu scan, tài liệu photocopy (bản sao) của tài liệu bảo mật có mức độ bảo mật tương đương như tài liệu cần bảo mật bản gốc. Cần áp dụng cấp độ BMTT tương tự như tài liệu bảo mật bản cứng (bản gốc) cho file dữ liệu scan (bản sao).

Điều 14: Bảo quản tài liệu, hồ sơ bản cứng *(Chi tiết tại Chính sách Bảo mật Vật lý và Môi trường)*

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, phòng lab, bàn làm việc, trong tủ không khóa.

14.2. Phải phân loại, sắp xếp, bảo quản và lưu trữ các 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 *(Chi tiết tại Chính sách Bảo mật Vật lý và Môi trường)*

15.1. Khi gửi tài liệu, thiết bị có chứa thông tin mật phải sử dụng dịch vụ vận chuyển có uy tín và gửi 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, sự toàn vẹn của tài liệu.

15.2. Khi tự 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 Công nghệ thông tin

16.1. Chỉ được sử dụng máy tính và thiết bị CNTT do 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 phòng IT để nhận được sự trợ giúp.

16.3. Không được đặt tên chung chung, không xác định được cho máy tính và máy chủ. Phải tuân thủ theo nguyên tắc về đặt tên cho máy tính và máy chủ đã được quy định.

16.4. Phải cài đặt screen saver không quá 05 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 tính qua đêm vì lý do công việc thì phải đăng ký với bộ phận Hành chính – Nhân sự (GA) khi được sự chấp thuận từ cán bộ quản lý trực tiếp và phòng ban chức năng liên quan.

16.6. Không được phép chia sẻ thông tin từ máy tính Công ty.

16.7. Không được 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 trực tiếp và kiểm tra định kỳ.

Điều 17: Sử dụng phần mềm

17.1. Chỉ được phép sử dụng những phần mềm có trong danh mục phần mềm được phép sử dụng của Công ty. Các phần mềm không có trong danh sách cấm, nhưng cũng không nằm trong danh sách được phép sử dụng, có thể tạm thời được coi như được phép, nhưng vẫn khuyến khích CBNV tham khảo phòng IT về độ an toàn của phần mềm trước khi download, cài đặt trên máy tính và hệ thống mạng của Công ty.

17.2. Nghiêm cấm sử dụng các phần mềm trong danh sách bị cấm theo quy định của Công ty. Nghiêm cấm download, sử dụng, lưu trữ phần mềm không có bản quyền, hoặc không được phép sử dụng. Các hành động bẻ khóa (crack) phần mềm có bản quyền là bị cấm, cho dù phần mềm có thể/hoặc không nằm trong danh sách được phép sử dụng.

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

17.4. Nghiêm cấm sử dụng các loại phầm mềm sử dụng mạng ngang hàng peer-to-peer, các phần mềm chia sẻ dữ liệu, phần mềm chia sẻ màn hình ngoại trừ các phần mềm chia sẻ dữ liệu/màn hình trong danh sách được sử dụng của Công ty.

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

17.6. Trong trường hợp có nhu cầu sử dụng phần mềm có trong danh sách bị cấm nói trên vì mục đích công việc, cần phải được cho phép bởi cán bộ quản lý và đại diện của Ban ISMS.

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

18.1. Tất cả 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 phòng CNTT trong quá trình đăng ký sử dụng, quá trình cài đặt các biện pháp bảo vệ như: đặt mật khẩu truy nhập thiết bị, mã hóa dữ liệu, sử dụng khóa dây…, quá trình sử dụng, quá trình hủy đăng ký.

18.2. Nghiêm cấm sử dụng các thiết bị có chức năng tạo kết nối mạng, phát sóng Wifi hay các hình thức chia sẻ mạng khác để làm cầu nối 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 quản lý bởi phòng IT.

Điều 19: Sử dụng email Công ty

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

19.2. Chỉ được phép sử dụng email của Công ty hoặc email được công ty cho phép cho mục đích công việc.

19.3. Các hệ thống email miễn phí như: Gmail, Yahoo, Hotmal, Outlook,.. bị cấm sử dụng, cấm gửi, cấm nhận tại Công ty. Không được sử dụng bất kỳ email hay hệ thống email khác tại Công ty. Quy định này ngoại trừ các phòng ban có đặc biệt được Ban ISMS và phòng IT cho phép như HR, BOD...

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

19.5. CBNV phải sử dụng mẫu chữ ký mới nhất do bộ phận Truyền thông (PR/GA) của Công ty ban hành cho cả email gửi đi, email phản hồi và email chuyển tiếp.

19.6. 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 và được sự chấp thuận của cán bộ quản lý đơn vị và cán bộ quản lý phòng IT.

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

19.8. 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. Chỉ các CBNV được phân quyền mới được phép gửi email tới các nhóm email có số lượng email lớn hoặc cho cả Công ty.

19.9. 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, có thông tin xâm phạm đến an ninh quốc gia.

19.10. Không được phép 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 là “Confidential” hoặc “Bảo mật” hoặc mức Medium (M) hoặc các mức độ cao hơn qua email. Nếu gửi thông tin có mức độ bảo mật này qua email thì phải được phép của người có thẩm quyền và phải mã hóa thông tin hoặc nén “zip” file và đặt mật khẩu file nén. Mật khẩu giải mã phải được gửi bằng email khác hoặc bằng phương tiện liên lạc khác.

19.13. 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.

19.14. CBNV muốn sử dụng thiết bị thông tin di động để truy cập hệ thống email của Công ty thì phải đăng ký với phòng IT. Phải tuân thủ hướng dẫn của phòng IT về việc đặt mật khẩu thiết bị và mã hóa dữ liệu hoặc cài đặt các biện pháp bảo mật liên quan trên thiết bị.

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

19.16. Khi kết thúc Hợp đồng lao động với Công ty, tài khoản email của CBNV sẽ bị xóa.

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

20.1. CBNV chỉ được truy cập vào những thông tin hay dữ liệu mà mình được phép thông qua việc phân quyền truy cập 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 hạ tầng mạng, hệ thống thông tin, và tài nguyên (bao gồm cả đường truyền Internet) của Công ty vào mục đích khác 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 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,…

20.4. Các máy chủ cung cấp dịch vụ ra internet phải được kiểm tra và quản lý bởi phòng IT.

20.5. Không được tự ý cài đặt các máy chủ cung cấp dịch vụ như Web, FTP, 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 của 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 để truy nhập internet của Công ty hoặc của 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 phép sử dụng công cụ hoặc website do 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 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.

20.10. Việc sử dụng dịch vụ Điện toán đám mây cho mục đích công việc phải được cán bộ có thẩm quyền phê duyệt, có thể sự điều chỉnh, hỗ trợ thêm các nguyên tắc bảo mật từ phía bộ phận IT, ISMS.

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 phải 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 phòng IT. CBNV không được phép tắt hay xóa phần mềm này.

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

21.3. Khi nghi ngờ máy tính bị nhiễm virus thì ngay lập tức phải ngắt kết nối mạng (tháo dây mạng, tắt kết nối wifi,..), thông báo cho phòng IT và phối hợp thực hiện xử lý.

21.4. Không được phát tán các chương trình độc hại (như virus, sâu, trojan, bom thư, thư lừa đảo,..) từ máy tính 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 hàng

22.1. Tài sản của khách hàng cung cấp (hạ tầng, hệ thống thông tin, ứng dụng/phần mềm, kết nối mạng, máy chủ, internet, thiết bị, tài khoản/mật khẩu, email…) được coi là tài sản của khách hàng để phục vụ cho việc vận hành và quản trị hoặc hỗ trợ quá trình phát triển phần mềm, kiểm thử phần mềm của Công ty hoặc khách hàng.

22.2. Phải 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 trong trường hợp khách hàng không cung cấp. *(chi tiết tại Chính sách Quản lý tài sản)*

22.4. Không được phép mang tài sản của khách hàng ra khỏi khu vực Công ty hoặc khu vực của khách hàng mà không được phép. Khi cần thiết phải mang ra ngoài, cần phải được phê duyệt bởi người có thẩm quyền và áp dụng các biện pháp bảo vệ phù hợp khi tính tới rủi ro mất mát, để lộ thông tin (như đặt mật khẩu, mã hóa hoặc các biện pháp bảo vệ vật lý… tùy theo loại tài sản cần bảo vệ - *chi tiết tại Chính sách Quản lý tài sản*)

22.5. 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”.

22.6. 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 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.

22.7. 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.

22.8. Phải 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, mạng xã hội và các kênh tương tự trên internet.

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 ghi âm/quay phim/chụp ảnh 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 BMTT, CBNV phải có trách nhiệm thông báo ngay cho cán bộ quản lý cấp trên và trưởng phòng ISMS trong vòng 02 giờ để tìm phương hướng giải quyết (chi tiết tại Quy trình Xử lý sự cố Bảo mật thông tin).

24.2. Tuân thủ yêu cầu của khách hàng về báo cáo xử lý sự cố BMTT 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 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 vô ý, lỗi cố ý.

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

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

26.1. Hình thức trừ thưởng (theo Phụ lục các mức trừ thưởng).

26.2. Hình thức bồi thường thiệt hại theo Pháp luật.

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

Điều 27: Xử lý vi phạm bảo mật thông tin

27.1. Trường hợp phát hiện hành vi vi phạm BMTT, ban ISMS có trách nhiệm báo cáo cho Lãnh đạo cấp trên hoặc Ban 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 BMTT này có hiệu lực kể từ ngày ký.

28.2. Ban ISMS 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. Lãnh đạo Công ty, lãnh đạo các Chi nhánh, Văn phòng đại diện, lãnh đạo các Công ty thành viên và tất cả các đơn vị 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, bổ xung 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 Giám đốc (BOD), Phòng Nhân sự (HR), Phòng IT, Phòng Đảm bảo chất lượng (QA) và được sự phê duyệt của Ban Giám đốc.

GIÁM ĐỐC

Trần Xuân Khôi

CHƯƠNG V. PHỤ LỤC CÁC MỨC TRỪ THƯỞNG / PHẠT TIỀN *(trong trường hợp không có thưởng)*

Các trường hợp vi phạm sau đây có thể bị áp dụng mức trừ thưởng / phạt tiền cao hơn so với mức tiền được quy định ở bảng bên dưới:

1. *Hành vi vi phạm do khách hàng phát hiện và yêu cầu Công ty xử lý.*
2. *Hành vi vi phạm phải có sự tham gia xử lý của thành viên Ban Tổng giám đốc.*
3. *Người có hành vi vi phạm là cán bộ quản lý.*
4. *Hành vi vi phạm phải áp dụng các mức xử lý/ truy tố theo quy định của Pháp luật của nước sở tại hoặc của quốc gia khác.*

Trong các trường hợp kể trên, quyết định trừ thưởng / phạt tiền hoặc áp dụng các mức xử phạt cao hơn tuân theo quyết định của Ban Tổng giám đốc hoặc luật pháp hiện hành.

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 / phạt tiền *(*) căn cứ vào phạm vi, mức độ thiệt hại do hành vi vi phạm gây ra, thái độ thành khẩn, tích cực khắc phục hậu quả của người có hành vi vi phạm.*				
		Từ 300.000 đến 1.000.000	*Từ 1.000.000 đến 3.000.000*	*Từ 3.000.000 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 hoặc yêu cầu truy cập thông tin cá nhân vượt quá mức cần thiết tối thiểu cho công việc.	I		II		
5	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. Sao chép thông tin cá nhân của khách hàng, đối tác hoặc CBNV mà không được người có thẩm quyền của Công ty, hoặc chủ sở hữu của thông tin phê duyệt.				I	II

Đơn vị tính: VNĐ

STT	Các hành vi vi phạm	Các mức trừ thưởng / phạt tiền *(*) căn cứ vào phạm vi, mức độ thiệt hại do hành vi vi phạm gây ra, thái độ thành khẩn, tích cực khắc phục hậu quả của người có hành vi vi phạm.*				
		Từ 300.000 đến 1.000.000	*Từ 1.000.000 đến 3.000.000*	*Từ 3.000.000 đến 5.000.000*	*Từ 5.000.000 đến 10.000.000*	*Từ 10.000.000 trở lên*
6	Tải lên hoặc lưu trữ thông tin của Công ty có mức bảo mật từ Medium (M) hoặc “Internal Use”, hoặc “Nội bộ” trở lên trên các website, ổ lưu trữ internet công cộng, ổ lưu trữ internet sở hữu cá nhân, thiết bị di động sở hữu của cá nhân.	I	II			
7	Lưu thông tin quan trọng, thông tin bảo mật có mức bảo mật từ High (H), hoặc “”Confidential”, hoặc “Bảo mật” trở lên ngoài file-server và hệ thống lưu trữ nội bộ của Công ty.		I		II	
8	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			
9	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		
	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, ở nhà					
14	Làm việc từ xa, làm việc ở nhà mà 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 kết nối từ xa tới hệ thống thông tin 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 phòng IT.		I		II	

Đơn vị tính: VNĐ

STT	Các hành vi vi phạm	Các mức trừ thưởng / phạt tiền *(*) căn cứ vào phạm vi, mức độ thiệt hại do hành vi vi phạm gây ra, thái độ thành khẩn, tích cực khắc phục hậu quả của người có hành vi vi phạm.*				
		Từ 300.000 đến 1.000.000	*Từ 1.000.000 đến 3.000.000*	*Từ 3.000.000 đến 5.000.000*	*Từ 5.000.000 đến 10.000.000*	*Từ 10.000.000 trở lên*
	Điều 7: Cam kết và đào tạo về bảo mật thông tin					
17	CBNV không ký Cam kết BMTT khi kí hợp đồng 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 lao động và các khóa đào tạo lại định kỳ hàng năm, các khóa đào tạo hướng đối tượng như cho cán bộ quản lý, quản trị dự án, lập trình viên, CBNV đi onsite, CBNV khối đảm bảo kinh doanh, CBNV làm việc trong các Khu vực bảo mật ODC (Offshore Development Center)…	I	II			
20	Cán bộ quản lý đơn vị, khi thuê nhân lực từ bên ngoài không ký Cam kết BMTT 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 phòng IT 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	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			
25	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		

Đơn vị tính: VNĐ

STT	Các hành vi vi phạm	Các mức trừ thưởng / phạt tiền *(*) căn cứ vào phạm vi, mức độ thiệt hại do hành vi vi phạm gây ra, thái độ thành khẩn, tích cực khắc phục hậu quả của người có hành vi vi phạm.*				
		Từ 300.000 đến 1.000.000	*Từ 1.000.000 đến 3.000.000*	*Từ 3.000.000 đến 5.000.000*	*Từ 5.000.000 đến 10.000.000*	*Từ 10.000.000 trở lên*
26	Không sử dụng tài khoản cục bộ riêng biệt có quyền quản trị cho các hoạt động yêu cầu đặc quyền cao.		I		II	
27	Cho người khác sử dụng tài khoản Công ty truy cập vào hệ thống thông tin của Công ty.		I		II	
28	Cho người khác sử dụng tài khoản hoặc tiết lộ mật khẩu truy cập để truy cập vào hệ thống thông tin của khách hàng hoặc bên thứ ba cung cấp.			I		II
29	Sử dụng hay truy nhập vào hệ thống thông tin của Công ty bằng tài khoản của người khác.		I		II	
30	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
31	Cố tình tìm kiếm hay dò mật khẩu của người khác.			I		II
	Điều 10: Ra vào địa điểm làm việc					
32	Sử dụng vân tay giả để đăng ký vân tay cá nhân hoặc giả mạo vân tay của người khác để ra vào địa điểm làm việc.	I	II			
33	Chia sẻ cho người khác về mã số truy nhập cá nhân hoặc sử dụng mã số truy nhập cá nhân của người khác để ra vào khu vực làm việc.	I	II			
34	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 khách hàng/đối tác/CBNV thực hiện quẹt thẻ hộ, hoặc khách hàng/đối tác/CBNV nhờ quẹt thẻ hộ (đối với CBNV mức trừ thưởng nhân với số lần vi phạm).	I	II			
35	Mở cửa hộ người khác trong Công ty hoặc người ngoài Công ty mà không có bảo lãnh.	I	II			
36	Khách hàng/đối tác hoặc CBNV được cấp thẻ không đeo thẻ tại nơi làm việc.	I	II			
37	Khi phát hiện mã số truy cập cá nhân của mình có dấu hiệu bị lấy trộm hoặc sử dụng để truy nhập ra/vào trái phép mà không thông báo với cán bộ quản lý Vân tay-Thẻ từ trong vòng 02 giờ để xử lý.	I	II			

Đơn vị tính: VNĐ

STT	Các hành vi vi phạm	Các mức trừ thưởng / phạt tiền *(*) căn cứ vào phạm vi, mức độ thiệt hại do hành vi vi phạm gây ra, thái độ thành khẩn, tích cực khắc phục hậu quả của người có hành vi vi phạm.*				
		Từ 300.000 đến 1.000.000	*Từ 1.000.000 đến 3.000.000*	*Từ 3.000.000 đến 5.000.000*	*Từ 5.000.000 đến 10.000.000*	*Từ 10.000.000 trở lên*
38	Khi quên thẻ, mất thẻ mà không báo với cán bộ quản lý Vân tay-Thẻ từ để xử lý. Hoặc không trả lại thẻ cho cán bộ quản lý Vân tay-Thẻ từ trong vòng 7 ngày làm việc tính từ thời hạn cuối cùng trong đăng ký mượn thẻ hoặc ngày cuối cùng làm việc tại Công ty (tùy thời hạn nào đến trước).	I	II			
39	Cán bộ quản lý Vân tay-Thẻ từ không tuân thủ nguyên tắc cấp phát mã Vân tay/mã truy nhập cá nhân/Thẻ từ cho đúng loại đối tượng. Hoặc không ghi nhận lại thời gian giao mượn, trả thẻ từ.		I	II		
40	Không tuân thủ các biển báo cấm, biển chỉ dẫn tại địa điểm làm việc, các khu vực bảo mật của Công ty hoặc khách hàng.	I	II			
41	Ra/vào khu vực bảo mật khi không được phép, hoặc giả mạo vân tay, sử dụng mã truy cập của người khác, mượn/đánh cắp thẻ để ra vào khu vực này vì bất cứ lý do gì.		I	II		
42	Cán bộ chịu trách nhiệm quản lý Vân tay-Thẻ từ không bố trí sổ theo dõi khách ra/vào văn phòng Công ty, hoặc khu vực bảo mật	I	II			
	Điều 11: Sử dụng các thiết bị ghi hình, ghi âm, chụp ảnh					
43	Không xin phép hoặc không được sự đồng ý của người có thẩm quyền mà vẫn 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 và 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.		I	II		
	Điều 12: Sử dụng máy in, máy hủy giấy					
44	Không cài đặt phần mềm ghi log, phân quyền cho cá nhân hay nhóm người xác định cho máy in.	I	II			

Đơn vị tính: VNĐ

STT	Các hành vi vi phạm	Các mức trừ thưởng / phạt tiền (*) căn cứ vào phạm vi, mức độ thiệt hại do hành vi vi phạm gây ra, thái độ thành khẩn, tích cực khắc phục hậu quả của người có hành vi vi phạm.				
		Từ 300.000 đến 1.000.000	*Từ 1.000.000 đến 3.000.000*	*Từ 3.000.000 đến 5.000.000*	*Từ 5.000.000 đến 10.000.000*	*Từ 10.000.000 trở lên*
45	Sử dụng máy in của Công ty để in tài liệu không cần thiết cho công việc.	I	II			
46	Không sử dụng máy hủy giấy, khi cần hủy tài liệu, hồ sơ bảo mật.	I	II			
	Điều 13: Sử dụng máy scan, máy photocopy					
47	Sử dụng máy scan, máy photocopy để scan, photo các tài liệu không cần thiết cho công việc.	I	II			
48	Bỏ quên tài liệu tại khay sao chụp của máy scan, máy photocopy, đặc biệt là tài liệu bảo mật.	I	II			
49	Trong trường hợp phát hiện tài liệu bảo mật bị bỏ quên trong khay sao chụp của máy scan, máy photocopy, CBNV thay vì báo cáo và chuyển lại cho Ban ISMS hoặc bộ phận sở hữu tài liệu, lại sử dụng hoặc chia sẻ, phát tán khi bản thân không được phép hoặc cho những người khác không được phép sử dụng tài liệu bảo mật.		I		II	
50	Không áp dụng cấp độ bảo mật tương đương như bản gốc cho file dữ liệu scan, tài liệu photocopy (bản sao)		I		II	
	Điều 14: Bảo quản tài liệu, hồ sơ bản cứng					
49	Trong trường hợp phát hiện tài liệu bảo mật bị bỏ quên trong khay sao chụp của máy scan, máy photocopy, CBNV thay vì báo cáo và chuyển lại cho Ban ISMS hoặc bộ phận sở hữu tài liệu, lại sử dụng hoặc chia sẻ, phát tán khi bản thân không được phép hoặc cho những người khác không được phép sử dụng tài liệu bảo mật.		I		II	
50	Không áp dụng cấp độ bảo mật tương đương như bản gốc cho file dữ liệu scan, tài liệu photocopy (bản sao)		I		II	
51	Để tài liệu, hồ sơ cần được bảo mật bừa bãi ở các nơi công cộng như máy in, máy photocopy, phòng họp, lớp học, bàn làm việc, trong tủ không khóa.	I	II			
52	Không phân loại, sắp xếp, bảo quản và lưu giữ các tài liệu, hồ sơ bản cứng bảo mật trong tủ có khóa, người khác có thể dễ dàng tiếp cận được	I	II			

Đơn vị tính: VNĐ

STT	Các hành vi vi phạm	Các mức trừ thưởng / phạt tiền *(*) căn cứ vào phạm vi, mức độ thiệt hại do hành vi vi phạm gây ra, thái độ thành khẩn, tích cực khắc phục hậu quả của người có hành vi vi phạm.*				
		Từ 300.000 đến 1.000.000	*Từ 1.000.000 đến 3.000.000*	*Từ 3.000.000 đến 5.000.000*	*Từ 5.000.000 đến 10.000.000*	*Từ 10.000.000 trở lên*
	Điều 15: Vận chuyển thông tin					
53	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		
54	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					
55	Sử dụng máy tính và thiết bị CNTT do Công ty cấp vào mục đích ngoài công việc.	I		II		
56	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		
57	Đặt tên chung chung, không xác định được cho máy tính và máy chủ. Hoặc không tuân thủ nguyên tắc về đặt tên cho máy tính và mày chủ đã được công ty quy định.	I, II				
58	Không cài đặt screen saver hoặc cài đặt screen saver trên 5 phút.	I, II				
59	Không khóa màn hình máy tính khi ra khỏi chỗ ngồi hoặc khi ra khỏi khu vực làm việc.	I, II				
60	Không tắt máy tính và các thiết bị trước khi ra về, trừ trường hợp phải để máy qua đêm.	I, II				
61	Bật máy tính qua đêm vì lý do công việc nhưng không đăng ký với bộ phận Hành chính – Nhân sự (GA) và xin sự chấp thuận từ cán bộ quản lý trực tiếp và phòng ban chức năng liên quan.	I, II				
62	Chia sẻ thông tin từ máy tính Công ty.	I	II			
63	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			
64	Làm mất laptop, thiết bị, tài sản do Công ty cấp hoặc thuộc sở hữu cá nhân, có chứa thông tin mật, thông tin của khách hàng, thông tin dự án.			I		II

Đơn vị tính: VNĐ

STT	Các hành vi vi phạm	Các mức trừ thưởng / phạt tiền *(*) căn cứ vào phạm vi, mức độ thiệt hại do hành vi vi phạm gây ra, thái độ thành khẩn, tích cực khắc phục hậu quả của người có hành vi vi phạm.*				
		Từ 300.000 đến 1.000.000	*Từ 1.000.000 đến 3.000.000*	*Từ 3.000.000 đến 5.000.000*	*Từ 5.000.000 đến 10.000.000*	*Từ 10.000.000 trở lên*
65	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 dùng chung của đơn vị.	I		II		
	Điều 17: Sử dụng phần mềm					
66	Download, sử dụng, lưu giữ phần mềm không có bản quyền hoặc không được phép sử dụng. Hoặc bẻ khóa (crack) phần mềm có bản quyền, cho dù phần mềm có thể/hoặc không nằm trong danh sách được phép sử dụng.		I	II		
68	Sử dụng hoặc thử nghiệm bất kỳ dạng phần mềm thăm dò, theo dõi, tấn công, truy nhập trái phép trong Công ty.					I
69	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 không nằm trong danh sách phần mềm được sử dụng trong Công ty.				I	II
70	Sử dụng phần mềm, website để vượt qua Proxy hoặc Firewall (ví dụ: Tor, FreeGate, UltraSurf, Proxifier, HotpotShield,..) của Công ty dưới mọi hình thức.				I	II
	Điều 18: Sử dụng các thiết bị di động, thiết bị mạng và ngoại vi					
71	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		
72	Sử dụng các thiết bị có chức năng tạo kết nối mạng, phát sóng Wifi để làm cầu nối cho các thiết bị khác kết nối vào mạng của Công ty hay ra Internet.		I	II		
73	Sử dụng thiết bị mạng không đăng ký hoặc không được cấu hình và quản lý bởi phòng IT		I		II	
	Điều 19: Sử dụng email Công ty					
74	Sử dụng email của Công ty hoặc email được Công ty cho phép dùng cho mục đích ngoài công việc.		I		II	
75	Sử dụng email miễn phí, email cá nhân, email hay hệ thống email khác ngoài email của Công ty hoặc khách hàng cung cấp tại Công ty.	I		II		

Đơn vị tính: VNĐ

STT	Các hành vi vi phạm	Các mức trừ thưởng / phạt tiền *(*) căn cứ vào phạm vi, mức độ thiệt hại do hành vi vi phạm gây ra, thái độ thành khẩn, tích cực khắc phục hậu quả của người có hành vi vi phạm.*				
		Từ 300.000 đến 1.000.000	*Từ 1.000.000 đến 3.000.000*	*Từ 3.000.000 đến 5.000.000*	*Từ 5.000.000 đến 10.000.000*	*Từ 10.000.000 trở lên*
76	Gửi sai địa chỉ người nhận email (To, Cc, Bcc) hoặc sai nội dung email, hoặc sai file đính kèm, hoặc có virus trong file đính kèm.		I		II	
77	Không sử dụng mẫu chữ ký mới nhất do bộ phận Truyền thông (PR/GA) của Công ty ban hành cho cả email gửi đi, email phản hồi và email chuyển tiếp.	I		II		
78	Sử dụng hệ thống email của Công ty để test; tự ý cài đặt email servers.	I		II		
79	Sử dụng tài khoản email của người khác, mượn hay cho mượn tài khoản email.		I		II	
80	Giả mạo email, hoặc bẻ khóa mật khẩu, hoặc xâm nhập, tấn công đến hệ thống email của Công ty hay ngoài Công ty.					I
81	Gửi email hàng loạt (spam email) đến hệ thống email của Công ty hay ngoài Công ty khi không nằm trong danh sách CBNV được phân quyền gửi email số lượng lớn hoặc cho cả Công ty.	I	II			
82	Gửi email hoặc chuyển tiếp email có nội dung mang tính xúc phạm, công kích một số 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	
83	Chuyển tiếp email cho cá nhân hay mailing list mà không được phép từ người gửi email ban đầu.		I		II	
84	Chuyển tiếp thủ công hay tự động email của Công ty đến hệ thống email bên ngoài.		I		II	
85	Sử dụng địa chỉ email của Công ty để đăng ký vào các diễn đàn hay mạng xã hội.	I		II		
86	Gửi thông tin có mức độ bảo mật là “Confidential” hoặc “Bảo mật” hoặc mức Medium (M) hoặc các mức độ cao hơn qua email mà không đặt mật khẩu hoặc mã hóa.	I		II		

Đơn vị tính: VNĐ

STT	Các hành vi vi phạm	Các mức trừ thưởng / phạt tiền *(*) căn cứ vào phạm vi, mức độ thiệt hại do hành vi vi phạm gây ra, thái độ thành khẩn, tích cực khắc phục hậu quả của người có hành vi vi phạm.*				
		Từ 300.000 đến 1.000.000	*Từ 1.000.000 đến 3.000.000*	*Từ 3.000.000 đến 5.000.000*	*Từ 5.000.000 đến 10.000.000*	*Từ 10.000.000 trở lên*
87	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 hoạt động nào tương tự.			I		II
88	Không đăng ký với phòng IT trước khi CBNV sử dụng thiết bị di động để truy cập hệ thống email của Công ty và/hoặc không tuân thủ hướng dẫn của phòng IT về việc đặt mật khẩu thiết bị và mã hóa dữ liệu.	I	II			
89	Không bàn giao lại cho người có trách nhiệm về các 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					
90	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	
91	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	
92	Sử dụng mạng nội bộ, hệ thống thông tin, máy chủ và đường truyền Internet vào mục đích khác ngoài công việc.		I		II	
93	Sử dụng máy chủ cung cấp dịch vụ ra internet không được kiểm tra và quản lý bởi phòng IT		I		II	
94	Tự ý cài đặt các máy chủ cung cấp dịch vụ như Web, FTP, SVN, Proxy, Firewall, DC, DNS, DHCP,…				I	II
95	Tự ý cấu hình mạng, tự ý thiết lập kết nối internet cho các máy trong mạng nội bộ của Công ty.			I		II

Đơn vị tính: VNĐ

STT	Các hành vi vi phạm	Các mức trừ thưởng / phạt tiền *(*) căn cứ vào phạm vi, mức độ thiệt hại do hành vi vi phạm gây ra, thái độ thành khẩn, tích cực khắc phục hậu quả của người có hành vi vi phạm.*				
		Từ 300.000 đến 1.000.000	*Từ 1.000.000 đến 3.000.000*	*Từ 3.000.000 đến 5.000.000*	*Từ 5.000.000 đến 10.000.000*	*Từ 10.000.000 trở lên*
96	Truy cập vào các website không kiên quan đến mục đích công việc, sử dụng các trang Proxy trung gian truy nhập internet của Công ty hoặc khách hàng.	I	II			
97	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		
98	Lợi dụng hạ tầng mạng, thiết bị và tài nguyên của Công 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 tương tự.		I		II	
99	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
100	Sử dụng dịch vụ điện toán đám mây không được sự xem xét và phê duyệt của phòng IT.		I		II	
	Điều 21: Phòng chống virus và cập nhật chương trình					
101	Tải về, sao chép thông tin, tài liệu từ trên mạng, từ máy tính khác, thiết bị khác và bị lây nhiễm các chương trình độc hại (như virus, sâu, trojan, bom thư, thư lừa đảo,..).		I		II	
102	Phát tán các chương trình độc hại (như virus, sâu, trojan, bom thư, thư lừa đảo,..) từ máy tính và/hoặc thiết bị của Công ty hoặc vào mạng và/hoặc máy chủ của Công ty.				I	II
103	Máy tính và các 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			
104	Phát tán các chương trình độc hại vào mạng và máy chủ (như virus, sâu, trojan, bom thư,…)			I		II

Đơn vị tính: VNĐ

STT	Các hành vi vi phạm	Các mức trừ thưởng / phạt tiền *(*) căn cứ vào phạm vi, mức độ thiệt hại do hành vi vi phạm gây ra, thái độ thành khẩn, tích cực khắc phục hậu quả của người có hành vi vi phạm.*				
		Từ 300.000 đến 1.000.000	*Từ 1.000.000 đến 3.000.000*	*Từ 3.000.000 đến 5.000.000*	*Từ 5.000.000 đến 10.000.000*	*Từ 10.000.000 trở lên*
105	Tự ý tắt hay xóa các chương trình phòng chống virus, các bản cập nhật định kì, không quét virus định kỳ	I	II			
106	Không kiểm tra việc cập nhật các bản vá lỗi hệ điều hành và phần mềm; không báo cáo phòng IT khi có lỗi xảy ra.	I	II			
107	Không thông báo cho phòng IT, không ngắt kết nối mạng khi nghi ngờ máy tính bị nhiễm virus và/hoặc không phối hợp thực hiện xử lý.	I		II		
	Điều 22: Sử dụng tài sản của khách hàng					
108	Không tuân thủ chính sách hoặc hướng dẫn quản lý tài sản của khách hàng khi được cung cấp hoặc sử dụng. Không tuân thủ chính sách hoặc hướng dẫn quản lý tài sản của Công ty đối với tài sản của khách hàng trong trường hợp không khách hàng không cung cấp hướng dẫn.			I		II
109	Không sử dụng và bảo quản thiết bị, tài khoản/mật khẩu, email, quyền truy cập… hoặc tài sản của khách hàng không được phân quyền sử dụng trên nguyên tắc “đủ để làm việc”.			I		II
110	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 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
111	Tấn công vào mạng hoặc máy chủ của khách hàng hoặc lợi dụng tài sản của khách hàng để tấn công vào mạng hoặc máy chủ bên ngoài.					I
112	Không bàn giao tài sản của khách hàng nếu có, cho người có trách nhiệm khi thay đổi vị trí công việc.			I		II
113	Làm mất tài sản của khách hàng.				I	II

Đơn vị tính: VNĐ

STT	Các hành vi vi phạm	Các mức trừ thưởng / phạt tiền *(*) căn cứ vào phạm vi, mức độ thiệt hại do hành vi vi phạm gây ra, thái độ thành khẩn, tích cực khắc phục hậu quả của người có hành vi vi phạm.*				
		Từ 300.000 đến 1.000.000	*Từ 1.000.000 đến 3.000.000*	*Từ 3.000.000 đến 5.000.000*	*Từ 5.000.000 đến 10.000.000*	*Từ 10.000.000 trở lên*
	Điều 23: Sử dụng các phương tiện truyền thông xã hội					
114	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, các phương tiện truyền thông xã hội.		I			II
115	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 quay phim, chụp ảnh của Công ty lên các phương tiện truyền thông xã hội.		I		II	
116	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 lên các phương tiện truyền thông xã hội.		I		II	
	Điều 24: Xử lý sự cố bảo mật thông tin					
117	Không thông báo ngay cho cán bộ quản lý cấp trên hoặc trưởng phòng ISMS trong vòng 02 giờ khi phát hiện sự 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 BMTT để tìm phương án giải quyết.		I		II	
118	Không tuân thủ yêu cầu của khách hàng về báo cáo sự cố BMTT, nếu đã có thống nhất trước đó với khách hàng về cách thức xử lý khi có sự cố xảy ra.				I	II
119	Không hợp tác xử lý sự cố về BMTT khi được Công ty hoặc khách hàng yêu cầu.		I		II	

GIÁM ĐỐC

Trần Xuân Khôi