



QUY ĐỊNH AN TOÀN THÔNG TIN

Mã tài liệu: REG
Lần ban hành: 5.0
Ngày ban hành: 17/08/2022

THEO DÕI SỬA ĐỔI TÀI LIỆU

STT	Lần sửa đổi	Vị trí sửa đổi	Tóm tắt nội dung sửa đổi
1	2.0	Toàn bộ	<ul style="list-style-type: none">- Chia rõ các quy định cho từng phòng ban- Lược bỏ vài thông tin đang bị trùng lặp với các hồ sơ biểu mẫu- Thay đổi NVKT, NVTB thành NVIT
2	3.0	Toàn bộ	<ul style="list-style-type: none">- Chuyển 1 số quy định vào quy trình tương ứng- Rút gọn quy định
3	4.0	Phương án xử lý khi bị virus tấn công	<ul style="list-style-type: none">- Thay đổi các bước xử lý để đảm bảo linh động và đáp ứng thực tế công việc
4	4.1	Sự cố	<ul style="list-style-type: none">- Chỉnh sửa biểu mẫu ghi nhận sự cố thành biểu mẫu mới được tích hợp trong QT <i>QP18 xác định rủi ro BM04 Risks and Issue Management</i>
5	5.0	Bổ sung mục 8.	8. Quy định về các thông tin liên quan đến Dự án

TÀI LIỆU NÀY ĐƯỢC BAN HÀNH CHO ĐƠN VỊ

	QUY ĐỊNH AN TOÀN THÔNG TIN	Mã tài liệu: REG Lần ban hành: 5.0 Ngày ban hành: 17/08/2022
---	---------------------------------------	--

STT	Tên đơn vị	Ký hiệu
1	Ban lãnh đạo	BAP
2	Khối sản xuất	PR
3	Khối hỗ trợ	SP

Người viết	Người kiểm tra	Người phê duyệt
-------------------	-----------------------	------------------------



QUY ĐỊNH AN TOÀN THÔNG TIN

Mã tài liệu: REG
Lần ban hành: 5.0
Ngày ban hành: 17/08/2022

I/ Mục đích

Quy định và các bước thực hiện nhằm bảo mật và an toàn thông tin, dữ liệu của Công ty của tất cả nhân viên thuộc phòng ban trong quá trình làm việc tại Công ty.

II/ Phạm vi áp dụng

Áp dụng đối với tất cả phòng ban công ty.

III/ Tài liệu viện dẫn

Theo danh mục tài liệu được quy định trong ***QP01 Quy trình kiểm soát thông tin dạng văn bản***
Điều khoản A15 - Tiêu chuẩn ISO/IEC 27001:2013.

IV/ Thuật ngữ và định nghĩa

- | | |
|---|---|
| <ul style="list-style-type: none">● ATTT: An toàn thông tin● GD: Giám đốc● CBNV: Cán bộ nhân viên● TBP: Trưởng bộ phận● QLDA: Quản lý dự án● TN: Trưởng nhóm● TV: Thành viên● KH: Khách hàng● DA: Dự án | <ul style="list-style-type: none">● Phòng HCNS: Phòng hành chính nhân sự● HCNS: Hành chính nhân sự● nhân viên: Nhân viên● NVHCNS: Nhân viên hành chính nhân sự● NVIT: Nhân viên phòng IT● PCCC: Phòng cháy chữa cháy |
|---|---|



QUY ĐỊNH AN TOÀN THÔNG TIN

Mã tài liệu: REG
Lần ban hành: 5.0
Ngày ban hành: 17/08/2022


V/ Nội dung

1. Mật khẩu

- Để đảm bảo tính bảo mật và toàn vẹn đối với các tài sản thông tin trong việc truy cập các hệ thống nội bộ và các hệ thống trong hoạt động sản xuất, nhân viên phải tuân thủ các quy định sau:
 - + **KHÔNG** chia sẻ mật khẩu cá nhân với bất kỳ ai
 - + **KHÔNG** ghi lại mật khẩu dưới dạng văn bản cứng và để ở trong phạm vi công ty
 - + **KHÔNG** đính kèm mật khẩu vào email, thiết bị cá nhân/ máy tính hoặc các phương tiện trực tuyến
 - + **KHÔNG** tái sử dụng 5 mật khẩu gần nhất
- Tất cả mật khẩu **PHẢI** tuân thủ các yêu cầu sau:
 - + Thay đổi ngay sau lần đầu tiên đăng nhập
 - + Vòng đời của mật khẩu: **03 tháng**
 - + Độ dài mật khẩu: từ 8 ký tự trở lên, bao gồm: ký tự số, ký tự chữ từ a đến z và từ A đến Z, ít nhất một ký tự viết hoa, và một ký tự đặc biệt (?, !, @, #, %)
- **Cách xử lý khi phát hiện mật khẩu bị xâm phạm**
 - + **B1:** Thông báo cho phòng IT
 - + **B2:** Phòng IT thay đổi mật khẩu lập tức
 - + **B3:** Tìm nguyên nhân mật khẩu bị xâm phạm và có phương án khắc phục.

2. Quy định về email

- Mỗi nhân viên khi mới vào công ty sẽ được cấp 1 email sử dụng cho mục đích công việc. Nhân viên phải tuân thủ các quy định sau:
 - + **KHÔNG** sử dụng email của công ty để đăng ký các dịch vụ trực tuyến
 - + **KHÔNG** sử dụng email để trao đổi ra bên ngoài cho mục đích cá nhân
- Các trường hợp ngoại lệ: tạo group email, gửi email ra bên ngoài..., **PHẢI** thực hiện theo trình tự các bước sau:
 - + **B1:** Gửi yêu cầu đến phòng IT, cc TPB qua email
 - + **B2:** Phòng IT check với TBP/GĐ để xét duyệt

	QUY ĐỊNH AN TOÀN THÔNG TIN	Mã tài liệu: REG Lần ban hành: 5.0 Ngày ban hành: 17/08/2022
---	---------------------------------------	--

- + **B3:** NVIT cấp quyền gửi email ra bên ngoài theo đúng thời gian phía nhân viên yêu cầu

3. Quy định truy cập mạng

- Chia theo loại hình mạng:
- + Sử dụng mạng không dây
- + Sử dụng mạng có dây
- Đối với từng loại hình sẽ có những thiết lập mạng khác nhau, tùy theo mục đích sử dụng
- **Bảng thông mạng sẽ được phòng IT chia theo các mức: Thấp, Trung bình, Cao**
- **Đối với mạng không dây**
- Chia theo mục đích sử dụng với các SSID cố định như sau:

WIFI	Đối tượng sử dụng	Hình thức	Bảng thông
BAP_OFFICE	Thiết bị làm việc của nhân viên	Đăng ký địa chỉ MAC với phòng IT	Trung bình
BAP_MEETING	Thiết bị làm việc của PM, PL, TBP, BOM	Đăng ký địa chỉ MAC với phòng IT	Cao
BAP_RELAX	Thiết bị cá nhân của nhân viên	Nhập password hoặc scan ở các khu vực có dán thông tin	Thấp
BAP_GUEST	Khách hàng	N/A	Cao

- **Đối với mạng có dây**

Đối tượng sử dụng	Bảng thông
Máy tính bàn của Nhân viên	Trung bình



QUY ĐỊNH AN TOÀN THÔNG TIN

Mã tài liệu: REG
Lần ban hành: 5.0
Ngày ban hành: 17/08/2022

- **Những trường hợp ngoại lệ**
- + Sử dụng các thiết bị cá nhân cho mục đích công việc (laptop, macbook, mobile devices, ...etc) cần truy cập mạng nội bộ.
- + Những thiết bị của bên thứ 3, nhà cung cấp, khách hàng...etc cần truy cập mạng nội bộ của công ty để phục vụ cho mục đích công việc, sửa chữa, dịch vụ.
- + **B1:** Gửi yêu cầu đến **Phòng IT**, cc TPB để request quyền truy cập cho các thiết bị thuộc trường hợp ngoại lệ. Nội dung email bao gồm:
 - Tên người sử dụng thiết bị
 - Loại thiết bị
 - Thời hạn sử dụng (Ngày bắt đầu, ngày kết thúc)
 - Người chịu trách nhiệm liên hệ
 - Địa chỉ MAC NIC của devices (LAN port, Wireless).
- + **B2:** Phòng IT để xem xét yêu cầu và thông báo lại cho nhân viên biết thời gian thực hiện và thời gian hoàn thành kèm các thông tin khác nếu có.
- + **Lưu ý:** Phòng IT có quyền không chấp nhận nếu xét thấy các trường hợp yêu cầu không thuộc phạm vi cho phép hoặc không phù hợp với mục đích sử dụng.

4. Kiểm soát về phát triển và duy trì hệ thống

- Khi phát sinh yêu cầu cần phát triển và duy trì hệ thống của công ty hoặc yêu cầu từ các bên liên quan phù hợp với nhu cầu của công ty, phòng IT trình phiếu **BM01_ Phiếu yêu cầu phát triển và duy trì hệ thống** lên ban lãnh đạo xem xét.
- Sau khi phát triển xong hệ thống, căn cứ vào các hồ sơ thiết kế về việc phát triển hệ thống và các hồ sơ khác liên quan. Phòng IT phối hợp với các Phòng ban liên quan và Ban ISO, triển khai đánh giá các hạng mục chất lượng và ATTT của quá trình nâng cấp, phát triển hệ thống.
- Kết quả quá trình phát triển và duy trì hệ thống được ghi chép đầy đủ vào **BM02_ Biên bản đánh giá kết quả phát triển và duy trì hệ thống**.
- Nếu đạt yêu cầu các phòng ban liên quan và Phòng IT tiến hành nghiệm thu hệ thống nâng cấp hoặc phát triển hệ thống, nếu không đạt thực hiện theo **QP03 Quy trình hành động khắc phục** để tìm nguyên nhân và biện pháp xử lý.



QUY ĐỊNH AN TOÀN THÔNG TIN

Mã tài liệu: REG
Lần ban hành: 5.0
Ngày ban hành: 17/08/2022

5. Di dời thiết bị và vị trí đặt các thiết bị

- Cấm di dời thiết bị khi chưa được phép: Không được di dời thiết bị văn phòng (máy tính để bàn, máy fax, server mạng LAN, hub, vv) khi chưa được phê duyệt của TBP và GD.
- Các thông tin được phân loại và các thông tin bảo mật khi được in ra cần phải xóa bỏ khỏi máy in ngay lập tức. Không được để bất kỳ tài liệu nào trên máy in.

6. Quy định phần mềm

- Các quy định liên quan đến phần mềm được phép và không được phép truy cập, nhân viên tuân thủ danh mục tại **BM03_Danh sách phần mềm được phép cài đặt** đã được phê duyệt.

7. Quy định mã hóa

- Mã hoá là cần thiết cho các trường hợp sau:
 - + Truyền tải files (SFTP, SCP, or VPN...các phương thức mã hoá kết nối trong trường hợp files không được mã hoá).
 - + Truy cập dữ liệu thông tin nhạy cảm qua môi trường web, ứng dụng web, ứng dụng mobile (HTTPS).
 - + Tất cả kết nối từ xa vào các môi trường ảo. (SSL)
 - + Truyền thông dữ liệu nhạy cảm đối với truy vấn dữ liệu trong database, web service call. (SSL)
 - + Truy cập hệ thống mạng hoặc máy chủ cho mục đích quản lý. (SSH Key)
- Mã hoá email:
 - + Các dữ liệu, thông tin nhạy cảm được đính kèm theo email cần được mã hoá.
 - + Các phương thức mã hoá được tích hợp sẵn có trong ứng dụng email.

8. Quy định về các thông tin liên quan đến Dự án

- Mỗi Dự án sẽ được tạo một folder để lưu trữ các thông tin trên Google Driver, tool nội bộ của công ty
- Folder Dự án chỉ được share cho các thành viên liên quan của Dự án. Trong trường hợp Khách hàng, bên Thứ 3 muốn truy cập thì PM phải gửi yêu cầu đến IT, COO để được phê duyệt.
- Không được phép sử dụng mail cá nhân để truy cập vào các folder Dự án mà chưa có sự xét duyệt của người có thẩm quyền



QUY ĐỊNH AN TOÀN THÔNG TIN

Mã tài liệu: REG
Lần ban hành: 5.0
Ngày ban hành: 17/08/2022

- PM/PL cần phải có trách nhiệm trao việc quản lý và kiểm soát việc phân chia quyền truy cập chỉnh sửa ở các folder Dự án. Lưu ý, chỉ share quyền edit.modify ở folder Dự án tổng cho những người có thẩm quyền (BOD, PM, PL)
- Các thành viên trong Dự án đều phải có trách nhiệm trong việc bảo mật thông tin liên quan đến Dự án và tuyệt đối không được sử dụng các thông tin này cho mục đích cá nhân
- Những thông tin Dự án chỉ được thao tác làm việc và lưu trữ tại các tool nội bộ và server của Công ty. Trong trường hợp cần phải sử dụng các tool và server ngoài thì phải báo lên người có thẩm quyền để được xem xét và phê duyệt
- Không được thao tác và lưu trữ các thông tin Dự án ở máy local mà chưa có sự xét duyệt của người có thẩm quyền

9. Nhân sự

- **Thông tin ứng viên**
 - + Không được tiết lộ thông tin của ứng viên cho bên thứ 3 nếu ứng viên không đồng ý
 - + Khi ứng viên nhận việc, cần đảm bảo đủ hồ sơ yêu cầu để xác minh đầy đủ danh tính của nhân viên.
- **Thông tin nhân viên**
 - + Không tiết lộ thông tin cá nhân ra bên ngoài nhằm mục đích trục lợi.
 - + Chỉ sử dụng thông tin cá nhân cho các mục đích làm hồ sơ thủ tục cho nhân viên về pháp lý.
 - + Nhân viên có trách nhiệm cung cấp đầy đủ thông tin theo yêu cầu để đảm bảo công tác nhân sự thuận lợi.
 - + Không tiết lộ thông tin về hợp đồng, lương, đãi ngộ của nhân viên
 - + Nhân viên cũng không được tiết lộ thông tin về lương thưởng bao gồm cả những lần tăng lương.
- **Khi chấm dứt hoặc thay đổi công việc**
 - + Xác định rõ trách nhiệm của CBNV và các bên liên quan về hệ thống thông tin của Công ty.
 - + Phòng HCNS làm biên bản bàn giao tài sản với CBNV
 - + Trước khi chấm dứt hợp đồng lao động, phòng HCNS thông báo cho CBNV về các yêu cầu đã ký trong cam kết bảo mật trước đó.



QUY ĐỊNH AN TOÀN THÔNG TIN

Mã tài liệu: REG
Lần ban hành: 5.0
Ngày ban hành: 17/08/2022

- + Khi nhân sự nghỉ việc/ chuyển công tác, Phòng HCNS gửi email đề nghị hủy bỏ quyền truy cập hoặc đăng ký quyền truy cập mới cho nhân sự gửi về phòng IT.

11. Kế toán

- Phòng kế toán không được tiết lộ thông tin về tài chính ra bên ngoài và cho bên thứ 3 Phòng kế toán không được tiết lộ các thông tin về HĐ của khách hàng ra bên ngoài.
- Phòng kế toán phải tuân thủ các yêu cầu của luật định.

12. Sản xuất

- **Quyền truy cập**
 - + QLDA/TN có quyền tạo lập và phân quyền truy cập các thông tin dự án trên hệ thống lưu trữ và các hệ thống được cấp quyền.
 - + Sau khi dự án kết thúc hoặc nhân viên rời khỏi dự án, QLDA/TN cần xóa các quyền truy cập của TV. Nếu vẫn cần TV ở lại để thực hiện bảo hành cho phía KH thì giữ lại quyền cho TV đó tuy nhiên sau thời gian bảo hành 2-3 tháng tùy theo cam kết bảo hành trong hợp đồng, QLDA/TN phải xóa hết quyền của các TV tham gia dự án trong folder dự án.
- **Trao đổi thông tin/dữ liệu dự án**

Nội dung trao đổi	Quyền
Thông tin hợp đồng dự án hoặc thông tin tài chính liên quan đến dự án	BGD/QLDA
Xác nhận Yêu cầu/Chỉ dẫn kỹ thuật của khách hàng liên quan đến dự án	BGD/QLDA/TN/BrSE
Tài khoản hệ thống/Mã nguồn của khách hàng	BGD/QLDA/TN/BrSE/IT
Xác nhận các vấn đề nhân lực trong dự án	BGD/QLDA/TN/BrSE

	QUY ĐỊNH AN TOÀN THÔNG TIN	Mã tài liệu: REG Lần ban hành: 5.0 Ngày ban hành: 17/08/2022
---	---------------------------------------	--

Tài liệu/xác nhận các vấn đề kỹ thuật trong thực hiện dự án	BGĐ/QLDA/TN/TVDA
--	------------------

14. Ban ISO

- Liên hệ với cơ quan có thẩm quyền và hiệp hội ngành nghề
- + Công ty đảm bảo việc liên lạc với các cơ quan liên quan có thẩm quyền được tuân thủ theo quy định của tòa nhà cho thuê: luật thi hành, cơ quan quản lý, cơ quan giám sát, ứng cứu ATTT, đơn vị phòng cháy chữa cháy....
- + Ban ISO đảm bảo sự liên lạc phù hợp với các hiệp hội ngành nghề hoặc các diễn đàn các chuyên gia bảo mật khác và các hiệp hội chuyên ngành...
- + Định kỳ 01 năm/01 lần Ban ISO có trách nhiệm tổng hợp và cập nhật những thông tin liên lạc theo ***BM04_Danh sách hiệp hội, ngành nghề*** nhằm đảm bảo khi có các sự cố ATTT như tấn công trên Internet, tấn công hệ thống của Công ty.... mà năng lực hiện tại Công ty chưa thể ứng phó được thì Công ty sẽ có đầu mối để nhờ sự ứng phó từ các cơ quan có thẩm quyền tham gia nhằm đảm bảo xử lý các sự cố một cách kịp thời.
- Đào tạo về ATTT
- + Định kỳ hàng quý (3 tháng), Ban ISO sẽ tổ chức đào tạo về các quy định ATTT nhằm nâng cao ý thức trách nhiệm đảm bảo ATTT của từng cá nhân trong công ty.
- + Đào tạo cơ bản về ATTT phải nằm trong kế hoạch đào tạo chung của công ty, được Công ty phê duyệt hoặc thông qua.
- + **Đối tượng đào tạo:** Từng cá nhân trong công ty
- + **Hình thức đào tạo:** Ban ISO phối hợp với Phòng HCNS có trách nhiệm lập kế hoạch đào tạo kiến thức cơ bản về ATTT cho cán bộ nhân viên, trình lãnh đạo Công ty phê duyệt.
- + **Thời gian đào tạo:** phải đảm bảo phù hợp với nội dung đào tạo, đối tượng được đào tạo.
- + Việc đào tạo này phải được lưu trữ tại ***BM06_Danh sách tham dự đào tạo***, kèm theo các hồ sơ đào tạo khác như tài liệu đào tạo, bảng điểm, chứng chỉ liên quan (nếu có).

	QUY ĐỊNH AN TOÀN THÔNG TIN	Mã tài liệu: REG Lần ban hành: 5.0 Ngày ban hành: 17/08/2022
---	---------------------------------------	--

15. Sự cố

- Sự cố nhỏ: những sự cố xảy ra trong quá trình hoạt động với một khoảng thời gian ngắn, không gây ảnh hưởng nghiêm trọng đến hệ thống ATTT của Công ty mà phía BPPB đã có dự trù sẵn phương án thay thế hoặc có thể tự giải quyết.
- **Sự cố lớn:** những sự cố xảy ra với tần suất nhiều hoặc có thời gian xảy ra dài, có khả năng làm tổn hại đến các hoạt động của cơ quan tổ chức và ảnh hưởng nghiêm trọng đến hệ thống ATTT mà phía BPPB không thể nào giải quyết mà cần có ý kiến chỉ đạo của Ban ISO/ lãnh đạo.
- Hằng năm, Ban ISO có trách nhiệm phân cấp sự cố nhỏ và sự cố lớn nhằm đảm bảo NV có thể phân biệt rõ ràng các sự cố nhỏ và sự cố lớn cùng với các mức độ xử lý của các sự cố và sự kiện.

#	Các loại sự cố	Quy định phân loại	Trách nhiệm giải quyết	Mức độ khẩn cấp
I	Sự cố nhỏ			
1	Mất mạng	Nhỏ hơn 30p	Phòng IT	Thấp
2	Mất điện	Nhỏ hơn 30p	Phòng HCNS	Thấp
3	Phần mềm bị lỗi không chạy được	Tạm thời gián đoạn công việc nhưng có phương án dự phòng	Phòng IT	Thấp
4	Phần mềm không có bản bản quyền	Tạm thời gián đoạn công việc nhưng có phương án dự phòng	Phòng IT	Thấp
5	Hệ thống tool nội bộ gặp lỗi	Tạm thời gián đoạn công việc dưới 1h	Phòng IT	Thấp



QUY ĐỊNH AN TOÀN THÔNG TIN

Mã tài liệu: REG
Lần ban hành: 5.0
Ngày ban hành: 17/08/2022

II	Sự cố lớn			
1	Phần mềm bị hacker tấn công	Trên 24h	Phòng IT	Cao
2	Mạng bị các đối tượng khác sử dụng trái phép	Trên 24h	Phòng IT	Cao
3	Hỏng thiết bị	Trên 24h	Phòng IT	Cao
4	Điện lưới bị sự cố	Thời gian mất điện lớn hơn 30p	Phòng HCNS	Cao
5	Hệ thống mạng bị sập	Thời gian lớn hơn 30p	Phòng IT	Cao
6	Mất dữ liệu hệ thống nội bộ	Mất dữ liệu mà không khôi phục được hoàn toàn	Phòng IT	Cao

- Khi phát sinh sự cố nhỏ và lớn, TBP chịu trách nhiệm cập nhật thông tin vào **BM04 Risk and Issue Management** thuộc **QP18 Quy trình xác định bối cảnh và đánh giá rủi ro** của phòng ban mình dựa trên biện pháp xử lý sự kiện sự cố đã được đề xuất.
- **Định kì vào cuối năm thường là trước giai đoạn đánh giá nội bộ**, Ban ISO lập báo cáo tổng hợp về tình hình quản lý sự cố của công ty trong năm cụ thể: số lượng sự cố, phân loại sự cố, thời gian khắc phục sự cố; tổng hợp đánh giá, so sánh với số liệu năm trước theo **BM08_ Bảng báo cáo thống kê sự cố**
- **Hướng dẫn xử lý các sự cố có thể xảy ra:**
- + Rò rỉ thông tin:

#	Rủi ro thông tin/dữ liệu	Giải pháp	Ngoại lệ
---	--------------------------	-----------	----------



QUY ĐỊNH AN TOÀN THÔNG TIN

Mã tài liệu: REG
Lần ban hành: 5.0
Ngày ban hành: 17/08/2022

1	Nhân viên để lộ source code ra bên ngoài qua các kênh lưu trữ cá nhân.	Ký cam kết bảo mật thông tin với nhân viên trước khi vào làm việc. Chia nhỏ source code nếu có thể Vô hiệu quá các cổng USB/IO không sử dụng.	Trong trường hợp đã bị lộ ra bên ngoài thì Phòng IT và QLDA cần rà soát lại hệ thống phân quyền và đảm bảo các phần phát sinh thêm không bị ảnh hưởng.
2	Nhân viên chụp màn hình và đưa lên mạng xã hội trong quá trình làm việc và vô tình chứa thông tin nhạy cảm về khách hàng và dự án	Yêu cầu gỡ bỏ ngay lập tức hình ảnh đó. Đào tạo lại về ISMS trong dự án cho toàn bộ nhân viên của dự án. Nhắc nhở về cam kết bảo mật thông tin đã ký trước đó.	Trong trường hợp đã bị lộ ra bên ngoài thì QLDA/TBP cần rà soát và có phương án giải trình với khách hàng trong trường hợp xấu nhất.
3	Nhân viên mang các thiết bị có chứa thông tin dự án ra khỏi phạm vi công ty hoặc chuyển giao/thanh lý/sửa chữa thiết bị nhưng không xóa bỏ thông tin/dữ liệu dự án trước khi chuyển giao.	Nhân viên chỉ được mang các thiết bị ra khỏi phạm vi công ty khi đã được phê duyệt và đảm bảo các quy định ISMS của Công ty. Tất cả các thiết bị trước khi chuyển giao/thanh lý/sửa chữa cần được xóa bỏ các thông tin/dữ liệu theo chính sách thiết bị. Đảm bảo nhân viên đã ký cam kết bảo mật thông tin.	Trong trường hợp đã bị lộ ra bên ngoài thì QLDA/TBP cần rà soát và có phương án giải trình với khách hàng trong trường hợp xấu nhất.




QUY ĐỊNH AN TOÀN THÔNG TIN

Mã tài liệu: REG
Lần ban hành: 5.0
Ngày ban hành: 17/08/2022

4	Thông tin bị lộ ra ngoài khi hệ thống bị tấn công bởi hacker	Liên hệ với Phòng IT để được hướng dẫn xử lý.	Trong trường hợp thông tin đã bị lộ ra ngoài cần báo cáo cho khách hàng về nguyên nhân và giải pháp khắc phục.
5	Thông tin nhân viên bị lộ (Thông tin cá nhân, Thông tin lương, thưởng, đãi ngộ) do nhân viên vô tình thiết lộ	Phòng HCNS cần rà soát lại hệ thống cách lưu trữ, chuyển giao thông tin. Cần có những hoạt động truyền thông khéo léo để nhắc nhở nhân viên.	
6	Thông tin tài chính bị lộ	Phòng Kế toán cần rà soát lại hệ thống, cách lưu trữ và chuyển giao thông tin sau đó đưa ra các biện pháp để giải quyết.	

+ Phát hiện và bị virus tấn công:

Bước 1	Xác định nguyên nhân cốt lõi dẫn đến sự cố virus tấn công
Bước 2	Lập plan để xử lý sự cố và trình BGĐ/TB ISO phê duyệt theo <i>BM08_Kế hoạch khắc phục sự cố</i>
Bước 3	Xử lý theo kế hoạch đã phê duyệt
Bước 4	Báo cáo kết quả xử lý và BGĐ/TB ISO phê duyệt kết quả
Bước 5	Ghi chép sự cố và lưu lại phương án xử lý

	<p style="text-align: center;">QUY ĐỊNH AN TOÀN THÔNG TIN</p>	<p>Mã tài liệu: REG Lần ban hành: 5.0 Ngày ban hành: 17/08/2022</p>
---	--	---

<p>Bước 6</p>	<p>Đánh giá hiệu lực 2-3 tháng từ ngày đánh giá kết quả.</p>
---------------	--

	QUY ĐỊNH AN TOÀN THÔNG TIN	Mã tài liệu: REG Lần ban hành: 5.0 Ngày ban hành: 17/08/2022
---	---------------------------------------	--

+ Mất thiết bị lưu trữ thông tin

Bước 1	Sau khi nhận được báo cáo sự cố ATTT và xác định được sự cố thuộc loại mất thiết bị lưu trữ thông tin, thực hiện kiểm tra danh sách quản lý thiết bị để xác định nhân viên chịu trách nhiệm
Bước 2	Thực hiện các hoạt động để lần vết, tìm kiếm thiết bị lưu trữ bị mất: + Trường hợp tìm thấy thiết bị lưu trữ thông tin thực hiện bước 5 + Trường hợp không tìm thấy thiết bị lưu trữ thông tin thực hiện bước 3
Bước 3	Xác định thông tin lưu trữ trong thiết bị trước khi bị mất: + Trường hợp thiết bị không lưu trữ thông tin hoặc thông tin không quan trọng thực hiện bước 5 + Trường hợp thiết bị chứa thông tin quan trọng ảnh hưởng đến quá trình hoạt động nghiệp vụ của Công ty thực hiện bước 4
Bước 4	Báo cáo Lãnh đạo Công ty và thực hiện theo các chỉ đạo từ Lãnh đạo Công ty.
Bước 5	Xử lý vi phạm các đối tượng có liên quan theo quy định của Công ty (nếu có) hoặc theo chỉ đạo từ Lãnh đạo Công ty.

	QUY ĐỊNH AN TOÀN THÔNG TIN	Mã tài liệu: REG Lần ban hành: 5.0 Ngày ban hành: 17/08/2022
---	---------------------------------------	--

+ Phát hiện truy cập trái phép

Bước 1	Xác định loại truy cập trái phép: + Trường hợp truy cập mạng trái phép thực hiện bước 2,3,4 + Trường hợp truy cập vật lý trái phép thực hiện bước 5,6,7 + Trường hợp truy cập vào các loại tài liệu không được phép thực hiện bước 8,9
Bước 2	Chụp lại màn hình bao gồm link và thời gian của người truy cập trái phép.
Bước 3	Gửi email cảnh cáo cùng bằng chứng tới người truy cập trái phép. Yêu cầu chấm dứt hành động truy cập trái phép.
Bước 4	Xác định mức độ nghiêm trọng: + Trường hợp mức độ nghiêm trọng nhỏ, nhân viên lần đầu vi phạm. Thực hiện xử lý vi phạm theo quy định. + Trường hợp mức độ nghiêm trọng nhỏ, nhân viên đã từng vi phạm. Lập biên bản, thông báo lên Lãnh đạo Công ty thực hiện xử lý vi phạm theo quy định. + Trường hợp mức độ nghiêm trọng lớn. Thông báo lên Lãnh đạo Công ty thực hiện theo các chỉ đạo từ Lãnh đạo Công ty.
Bước 5	Thông báo đến người/Đơn vị chịu trách nhiệm: + Trường hợp là người trong Công ty: thông báo đến TBP của nhân viên + Trường hợp là khách/người bên ngoài Công ty: thông báo đến tổ bảo vệ, phòng hành chính
Bước 6	Thực hiện các hành động khắc phục tạm thời để ngăn chặn truy cập trái phép như: yêu cầu rời khỏi khu vực không được phép, cưỡng chế trong trường hợp không tuân theo...

	QUY ĐỊNH AN TOÀN THÔNG TIN	Mã tài liệu: REG Lần ban hành: 5.0 Ngày ban hành: 17/08/2022
---	---------------------------------------	--

Bước 7	Thu thập bằng chứng qua video, camera xác định mức độ nghiêm trọng. + Trường hợp mức độ nghiêm trọng nhỏ: xử lý vi phạm theo quy định. + Trường hợp mức độ nghiêm trọng lớn: Thông báo lên Lãnh đạo Công ty thực hiện theo các chỉ đạo từ Lãnh đạo Công ty.
Bước 8	Thực hiện các hành động khắc phục tạm thời để ngăn chặn truy cập trái phép:
Bước 9	Xác định mức độ nghiêm trọng: + Trường hợp mức độ nghiêm trọng nhỏ Xử lý vi phạm theo quy định. + Trường hợp mức độ nghiêm trọng lớn Thông báo lên Lãnh đạo Công ty. Thực hiện theo các chỉ đạo từ Lãnh đạo Công ty.

16. Vi phạm

- Đối với nhân viên đang làm việc tại công ty
- + Vi phạm nhẹ: quên đổi mật khẩu, quên đăng ký khi mang thiết bị ra ngoài, không đăng ký thiết bị cá nhân để làm việc thì xử phạt theo mức độ 1: Gửi văn bản cảnh báo vi phạm đến cá nhân nhân viên cc TN, QLDA, BGD
- + Vi phạm nặng: tiết lộ thông tin Khách hàng & Dự Án, thông tin lương; đánh cắp những tài sản thuộc sở hữu trí tuệ, những tài liệu mật, source code của Dự án;..Tùy theo thiệt hại mà sẽ bị xử phạt theo mức độ 2, 3 mà không cần chứng minh về thiệt hại, được quyết định bởi ban SSO
 - **Mức độ 2:** Gửi văn bản cảnh báo vi phạm đến toàn công ty và set up training lại cho NV
 - **Mức độ 3:** Tiến hành xử lý theo quy định của luật hiện hành
- **Đối với nhân viên đã nghỉ việc**
- + Sau thời gian 5 năm kể từ ngày nghỉ việc tại công ty phải đảm bảo các vấn đề liên quan đến bảo mật theo Thỏa thuận bảo mật thông tin.
- + NV nếu vi phạm đối với thỏa thuận BMTT đã ký (tùy theo mức độ thiệt hại), sẽ có biện

	<p style="text-align: center;">QUY ĐỊNH AN TOÀN THÔNG TIN</p>	<p>Mã tài liệu: REG Lần ban hành: 5.0 Ngày ban hành: 17/08/2022</p>
--	--	---

pháp xử lý như sau:

- **Mức độ 1:** Gửi văn bản cảnh báo vi phạm đến cá nhân nhân viên
- **Mức độ 2:** Gửi văn bản cảnh báo vi phạm đến cơ quan nhân viên đang làm việc về việc vi phạm thỏa thuận bảo mật thông tin
- **Mức độ 3:** Tiến hành xử lý theo quy định của luật hiện hành



QUY ĐỊNH AN TOÀN THÔNG TIN

Mã tài liệu: REG
Lần ban hành: 5.0
Ngày ban hành: 17/08/2022

VI. Danh mục biểu mẫu trong quy định

#	Tên hồ sơ	Mã hiệu	Tần suất/thời gian thực hiện	Thời gian lưu	Trách nhiệm lưu
1	Phiếu yêu cầu phát triển và duy trì hệ thống	BM01	Khi phát sinh	3 năm	Phòng IT
2	Biên bản đánh giá kết quả phát triển và duy trì hệ thống.	BM02	Khi phát sinh	3 năm	Phòng IT
3	Danh sách phần mềm được phép cài đặt	BM03	1 năm/1 lần	3 năm	Phòng IT
4	Danh sách hiệp hội, ngành nghề	BM04	1 năm/lần	Vĩnh viễn	Ban ISO
5	Danh sách tham dự đào tạo	BM05	Khi phát sinh	3 năm	Ban ISO
6	Sổ theo dõi sự cố	BM06	Khi phát sinh	3 năm	Phòng ban phụ trách
7	Kế hoạch khắc phục sự cố	BM08	Khi phát sinh	3 năm	Phòng IT