


Soạn thảo	Xem xét	Phê duyệt	Đóng dấu
Nguyễn Thị Kim Anh	Hsu Chia Yuan	Chou Chun Kai	

CHÍNH SÁCH AN NINH BẢO MẬT

1. MỤC ĐÍCH:

Quy trình này nhằm bảo vệ công ty: chống lại các sự xâm nhập và tiếp cận trái phép từ bên ngoài; bảo mật thông tin & sản phẩm; tuân thủ yêu cầu về bảo mật của khách hàng; thực hiện các cam kết khác của công ty trong lĩnh vực sở hữu trí tuệ và bảo mật.

2. PHẠM VI:

- Áp dụng cho tất cả CBCNV tại công ty và mọi đối tác đến giao dịch hay làm việc tại mặt bằng công ty;
- Áp dụng cho các lĩnh vực an ninh cơ sở vật chất, nghiên cứu và phát triển sản phẩm, in ấn tem security label, sản xuất và công nghệ thông tin.

3. TRÁCH NHIỆM VÀ QUYỀN HẠN:

3.1. Ban TGD và đại diện Ban TGD về quản lý an ninh bảo mật: Có trách nhiệm lãnh đạo & điều phối hoạt động an ninh bảo mật trong toàn công ty, cung cấp nguồn lực đầy đủ để các BP-PX thực hiện đầy đủ các yêu cầu về an ninh bảo mật.

3.2 Toàn thể CBCNV: Có trách nhiệm tuân thủ nghiêm chỉnh mọi quy định của công ty liên quan đến an ninh bảo mật.

4. ĐỊNH NGHĨA:

- Khách: Là người đến công ty để liên hệ công việc hoặc thực hiện các hoạt động thi công, dịch vụ tại công ty.

- Ban TGD: Ban Tổng Giám Đốc
- CBCNV: Cán bộ công nhân viên
- BPPX: Bộ phận – phân xưởng
- Tem security: Tem nhãn dùng để nhận diện thương hiệu, xác định đây là sản phẩm thật, chính hãng.
- Hệ thống kiểm soát ra vào điện tử (EAC) là hệ thống máy nhận diện người được phép ra vào khu vực giới hạn bằng dấu vân tay.
- Hệ thống camera an ninh CCTV là hệ thống các camera được lắp đặt ở nhiều nơi trong công ty và kết nối đến trung tâm quản lý nhằm mục đích kiểm soát an ninh bảo mật tại công ty.
- Hệ thống phát hiện xâm nhập (IDS) là hệ thống báo động được lắp đặt ở nhiều nơi trong công ty nhằm giúp phát hiện sự xâm nhập trái phép ngoài giờ làm việc.
- Insole: Mặt đế trong, chỗ tiếp xúc với lòng bàn chân.

5. CHÍNH SÁCH VỀ AN NINH BẢO MẬT

5.1. Chính sách chung

5.1.1. Công ty chỉ định đại diện Ban TGD phụ trách lĩnh vực an ninh bảo mật và báo cáo cho Ban TGD về tình hình và kết quả thực hiện.

5.1.2. Công ty tổ chức đào tạo cho CBCNV về quy định an ninh bảo mật định kỳ hàng năm và khi bắt đầu tuyển dụng. Hồ sơ đào tạo cần lưu trữ đầy đủ.

5.1.3. Công ty tổ chức thực hiện đánh giá nội bộ sự tuân thủ quy định an ninh 1 lần/năm và thực hiện các biện pháp khắc phục & phòng ngừa để tránh lặp lại các vấn đề không tuân thủ.

5.1.4. Các CBCNV làm việc trực tiếp với sản phẩm và thông tin bảo mật cần ký kết với công ty bản “Thoả thuận bảo mật” - theo Quy Định Bảo Mật Thông Tin, Hồ Sơ, Tài Liệu - nhằm thể hiện rõ cam kết của CBCNV trong việc tuân thủ các quy định an ninh bảo mật của công ty.

5.1.5. Công ty ban hành và định kỳ cập nhật danh sách liên hệ khẩn cấp trong trường hợp xảy ra sự cố về an ninh bảo mật và danh sách này được ban hành cho các đơn vị thuộc phạm vi áp dụng của chính sách này. Khi có sự cố, CBCNV cần nhanh chóng báo cáo với các cá nhân trong danh sách này.

5.1.6. Bất kỳ sự cố an ninh nào, chẳng hạn như tai nạn, trộm cắp, mất trật tự, sự cố của hệ thống an ninh ...vv đều phải được ghi chép trên “Sổ ghi chép tình hình an ninh bảo mật hằng ngày” và phải được lưu trữ trong 3 năm.

5.2. Kiểm soát an ninh vành đai công ty và ra vào các khu vực

5.2.1. Bộ phận bảo vệ cần đảm bảo vành đai xung quanh công ty được giám sát thường trực nhằm ngăn chặn xâm nhập trái phép.

5.2.2. Cổng lớn ra vào công ty phải đóng khi không có xe ra vào. Bảo vệ trực cổng cần giám sát mọi trường hợp ra vào cổng.

5.2.3. Bộ phận bảo vệ thực hiện kiểm soát ra vào cổng theo Quy Trình Hoạt Động Đội Bảo Vệ và các hướng dẫn đi kèm đối với tất cả CBCNV và khách ra vào công ty.

5.2.4. Ở cửa ra vào của các bộ phận sau đây để đặt bảng cảnh báo:

- Bộ phận nghiên cứu và phát triển sản phẩm
- Phòng in tem security
- Kho thành phẩm
- Kho hàng B/C
- Phòng máy chủ của IT
- Phòng thử nghiệm
- Xưởng sản xuất
- Khu vực chất hàng/dỡ hàng

Nội dung của bảng cảnh báo bao gồm:

- Khu vực không phận sự xâm vào (Authorized Personnel Only)
- Nghiêm cấm quay phim, chụp hình (No Photo and Video Taking)
- Nơi đây có đặt camera giám sát (CCTV Surveillance in Operation)
- Nơi đây có đặt hệ thống báo động (Protected by Alarm System)

5.2.5. Tất cả CBCNV phải đeo thẻ theo quy định thẻ đeo của công ty để nhận dạng và kiểm soát việc ra vào khu vực trong công ty.

5.2.6. Bộ phận bảo vệ thực hiện kiểm soát ra vào cổng theo quy trình bảo vệ.

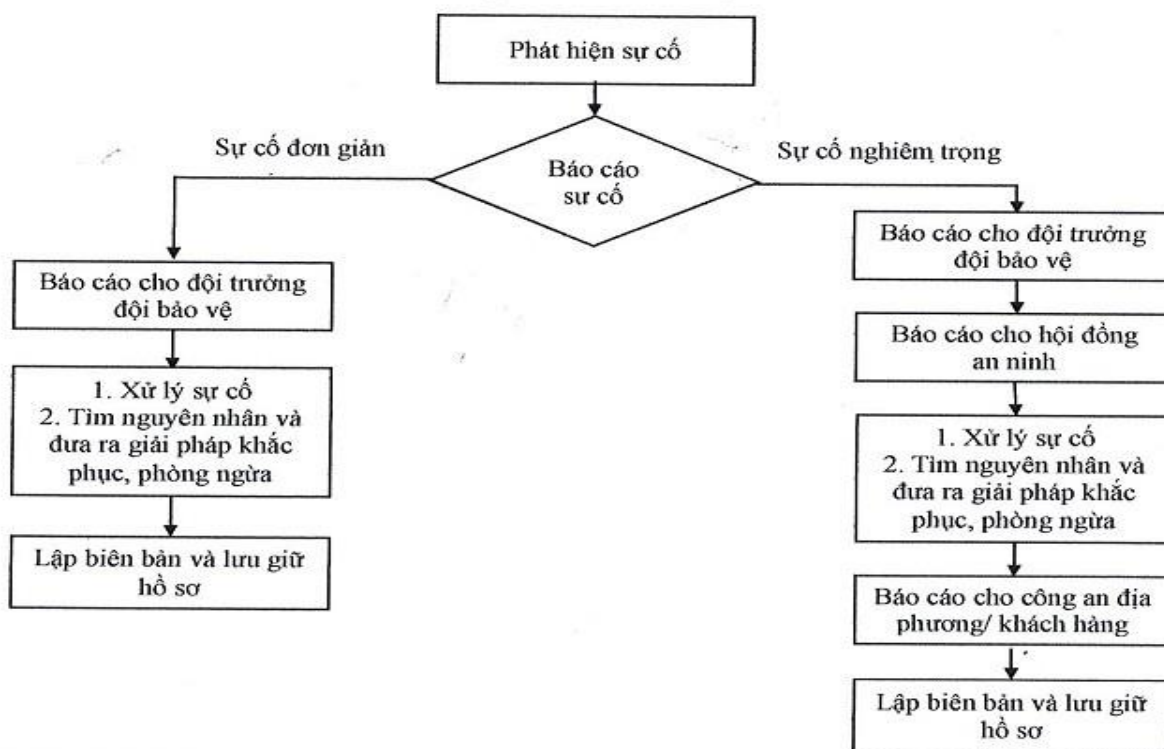
5.2.7. Tại phòng bảo vệ phải có hướng dẫn sử dụng và vận hành cho các hệ thống sau đây:

- Hệ thống camera theo dõi CCTV
- Hệ thống phát hiện xâm nhập (IDS)
- Hệ thống báo động cửa và cửa sổ: Bảo vệ chịu trách nhiệm phải được đào tạo cách thức kích hoạt và vô hiệu hóa các hệ thống này và các biện pháp bảo dưỡng thông thường.

5.2.8. Bảo vệ và IT phải phối hợp kiểm tra các thiết bị an ninh cần được ít nhất 1 năm 1 lần, và phải lưu giữ lại các thông tin sửa chữa.

5.2.9. Trong phòng bảo vệ phải có tủ treo chìa khóa để bảo quản chìa khóa sau giờ làm việc. Phải có danh sách người sử dụng chìa.

5.2.10. Nhân viên bảo vệ nên thường xuyên đi tuần tra theo những tuyến đường ngẫu nhiên để đảm bảo an ninh. Khi xảy ra bất kỳ sự cố an ninh nào, nhân viên bảo vệ phải có mặt tại hiện trường trong vòng 3 phút để xử lý sự việc. Sau đó, nhân viên bảo vệ phải liên hệ ngay với “Người cần liên lạc đầu tiên” trong “Danh sách liên hệ khẩn cấp khi có sự cố an ninh”. Nếu không liên hệ được với “Người cần liên lạc đầu tiên” thì liên hệ ngay với “Người cần liên lạc thứ 2” trong danh sách đó. Việc báo cáo và xử lý sự cố được thực hiện như sau:



5.3. Hệ thống kiểm soát ra vào điện tử (EAC)

5.3.1. Công ty chỉ định và ủy quyền cho bộ phận IT quản lý hệ thống kiểm soát ra vào điện tử (EAC) được lắp đặt tại nhiều nơi trong công ty.

5.3.2. Các khu vực nhạy cảm sau đây cần phải được lắp đặt hệ thống kiểm soát ra vào điện tử (EAC):

- Bộ phận nghiên cứu phát triển sản phẩm.
- Phòng in tem security.
- Kho thành phẩm.
- Kho hàng B/C.
- Phòng máy chủ IT.
- Phòng thử nghiệm.

5.3.3. Hệ thống kiểm soát ra vào điện tử (EAC) phải đạt được các tiêu chuẩn tối thiểu sau đây:

- Kiểm soát ra vào bằng dấu vân tay hay các biện pháp sinh trắc học khác.
- Nguồn điện liên tục (UPS) hỗ trợ tối thiểu trong 4 giờ, hoặc 1 giờ với nguồn máy phát điện dự phòng khi xảy ra sự cố mất điện.

5.3.4. Bảng điều khiển và tất cả các thiết bị được lắp đặt ở phía cửa nào có được sự bảo an toàn, sao cho dễ kiểm soát và tránh bị hư hỏng hay lục phá, không dễ tiếp cận hoặc bị tháo gỡ di chuyển đi chỗ khác.

5.3.5. Bộ phận IT chịu trách nhiệm ghi chép lại các sự cố hay các vấn đề bất thường do hệ thống kiểm soát ra vào điện tử (EAC) ghi nhận và báo cáo. Các thông tin này phải được xem xét hàng tuần, khi cần thì phải nhanh chóng xác minh và xử lý vấn đề. Hồ sơ về việc xem xét này phải được lưu giữ ít nhất 1 năm.

5.3.6. Bộ phận IT chịu trách nhiệm kiểm tra phần cứng và phần mềm hệ thống kiểm soát ra vào điện tử (EAC) hàng tuần và thực hiện bảo trì định kỳ hàng năm. Phải có hồ sơ lưu trữ về hoạt động này.

5.4. Hệ thống camera an ninh CCTV

5.4.1. Công ty chỉ định và ủy quyền cho bộ phận IT quản lý hệ thống camera an ninh CCTV toàn công ty.

5.4.2. Các khu vực nhạy cảm sau đây cần lắp đặt hệ thống camera an ninh CCTV:

- Bộ phận nghiên cứu và phát triển sản phẩm
- Phòng in tem security
- Kho thành phẩm
- Kho hàng B/C
- Phòng máy chủ của IT
- Phòng thử nghiệm
- Xưởng sản xuất
- Khu vực chất hàng/dỡ hàng

5.4.3. Bộ phận IT phải bảo quản toàn bộ hệ thống, kể cả máy chủ lưu trữ dữ liệu (DVR), camera, nguồn điện và các thiết bị đầu cuối. Toàn hệ thống phải có nguồn điện liên tục không đứt quãng (UPS) hỗ trợ tối thiểu trong 4 giờ, hoặc 1 giờ với nguồn máy phát điện dự phòng, khi xảy ra sự cố mất điện.

5.4.4. Bảng điều khiển và tất cả các thiết bị được lắp đặt ở phía cửa nào có được sự bảo an toàn, sao cho dễ kiểm soát và tránh bị hư hỏng hay lục phá, không dễ tiếp cận hoặc bị tháo gỡ di chuyển đi chỗ khác.

5.4.5. Yêu cầu và cài đặt cơ bản của camera CCTV và máy chủ lưu trữ dữ liệu camera như sau:

5.4.5.1. Camera CCTV và video DVR độ phân giải tốt nhất là HD (1280 * 720 pixels)

5.4.5.2. Tiêu chuẩn tối thiểu: 640 x 480 pixels

5.4.5.3. Refresh tối thiểu/tỷ lệ khung: 12 khung/ giây.

5.4.5.4. Ghi chép liên tục và không đứt quãng.

5.4.5.5. Có thể tự khởi động lại quá trình ghi hình sau khi bị mất điện.

5.4.5.6. DVR có thể phát lại và ghi hình đồng thời.

5.4.5.7. Camera CCTV có thể ghi nhận suốt ngày và đêm (có chế độ chuyển đổi hình ảnh màu/trắng đen) với khả năng ghi nhận rõ hình ảnh ban đêm. Camera phải được lắp ở vị trí phù hợp để có thể ghi hình rõ nét dù cho bị ngược sáng hoặc ánh sáng quá nhiều. Cảnh phim cần phải lưu giữ rõ ràng mọi chuyển động của chủ thể.

- 5.4.6. Nội dung ghi hình của camera an ninh CCTV phải được lưu giữ tối thiểu 60 ngày, tốt nhất là 90 ngày. Hàng tuần Chủ Quản của bộ phận Bảo Vệ phải xem lại các video một cách ngẫu nhiên để kiểm tra lại xem có sự cố an ninh nào bị bỏ sót trong tuần qua hay không. Nếu có phát hiện sự cố thì phải nhanh chóng xử lý và báo cáo cho Ban TGD theo danh sách quy định.
- 5.4.7. Bộ phận IT cần tạo tài khoản sử dụng với các quyền truy nhập khác nhau cho các CB-CNV được phép truy cập. Sau khi truy cập xong, người sử dụng phải thoát (Log-out) khỏi đăng nhập tài khoản của mình. Hệ thống quản lý trên máy chủ phải được cài đặt để ghi nhận lại tất cả hoạt động của người sử dụng và dữ liệu đó phải được lưu trữ ít nhất 1 năm.
- 5.4.8. Trong trường hợp hệ thống hư hỏng, máy chủ quản lý dữ liệu camera DVR phải có âm thanh báo động, hoặc gửi mail, tin nhắn đến cho người được phân công thuộc bộ phận IT, bảo vệ và chủ quản cấp cao. Máy chủ phải được cài đặt để ghi nhận lại các sự cố hư hỏng như thế và dữ liệu về các sự cố này phải được lưu giữ ít nhất 1 năm.
- 5.4.9. Bộ phận IT phải xuất ra file nội dung ghi hình của camera an ninh CCTV, dưới dạng DVD, lưu trữ ra USB hoặc ổ đĩa hệ thống, để lưu trữ và dùng để xem lại trong trường hợp xảy ra sự cố an ninh. Dữ liệu về sự cố an ninh phải được ghi nhận và lưu lại ít nhất 3 năm.

5.5. Hệ thống phát hiện xâm nhập trái phép (IDS)

- 5.5.1. Công ty chỉ định và ủy quyền cho bộ phận IT quản lý hệ thống phát hiện xâm nhập trái phép (IDS) được lắp đặt ở nhiều nơi trong công ty.
- 5.5.2. Các khu vực nhạy cảm sau đây phải lắp đặt hệ thống phát hiện xâm nhập trái phép (IDS):
- Bộ phận nghiên cứu và phát triển sản phẩm
 - Phòng in tem security
 - Kho thành phẩm
 - Kho hàng B/C
 - Phòng máy chủ của IT
 - Phòng thử nghiệm
- 5.5.3. Hệ thống phát hiện xâm nhập trái phép (IDS) phải đạt được các tiêu chuẩn như sau:

- 5.5.3.1. Máy dò chuyển động công nghệ kép kết hợp vi sóng Doppler và cảm biến hồng ngoại thụ động.
- 5.3.1.2. Nguồn điện liên tục không đứt quãng (UPS) hỗ trợ tối thiểu trong 4 giờ, hoặc 1 giờ với nguồn máy phát điện dự phòng, khi xảy ra sự cố mất điện
- 5.3.1.3. Bảng điều khiển và tất cả các thiết bị được lắp đặt ở phía an toàn của cửa.
- 5.3.1.4. Máy tính điều hành được cài đặt mật khẩu bảo vệ.
- 5.3.1.5. Được kiểm soát và được bảo vệ khỏi sự lục lọi, không dễ tiếp cận hoặc chuyển đổi.
- 5.5.4. Bộ phận IT chỉ định 2 nhân viên phụ trách lắp đặt và tháo gỡ hệ thống phát hiện xâm nhập trái phép (IDS) và mỗi người có mật khẩu riêng.
- 5.5.5. Trong trường hợp có sự cố, hệ thống phải báo động cho bộ phận IT, bảo vệ, chủ quản cấp cao và trưởng bộ phận có liên quan thông qua email hoặc tin nhắn SMS. Khi có báo động, nhân viên bảo vệ trực phải lập tức tiếp cận hiện trường và xử lý sự cố. Mọi sự cố phải được bộ phận IT và bảo vệ ghi nhận lại và lưu giữ ít nhất 3 năm.

5.6. Quy định an ninh bảo mật cho bộ phận nghiên cứu phát triển sản phẩm

- 5.6.1. An toàn vật chất
- 5.6.1.1. Bộ phận nghiên cứu phát triển sản phẩm phải chỉ định một nhân viên chịu trách nhiệm về công tác an ninh bảo mật tại bộ phận.
- 5.6.1.2. Cửa ra vào phải lắp đặt biển cảnh báo, camera an ninh CCTV, kiểm soát ra vào (EAC), kiểm soát xâm nhập trái phép (IDS) theo đúng các tiêu chuẩn quy định của công ty ở các hạn mục bên trên.
- 5.6.1.3. Trừ những trường hợp đặc biệt do Ban TGD phê duyệt, tất cả CBCNV đều không được phép mang theo các vật dụng cá nhân vào bên trong bộ phận. Vật dụng cá nhân bao gồm: túi xách, camera và các thiết bị điện tử có chức năng camera. Ở ngoài cửa phòng làm việc phải có tủ.
- 5.6.1.4. Bộ phận nghiên cứu và phát triển sản phẩm chỉ định một nhân viên phụ trách việc chụp ảnh, xuất ảnh ra máy tính và quản lý máy ảnh. Hết giờ làm việc, toàn bộ hình ảnh trên máy ảnh phải được xóa.

5.6.2. Bảo mật thông tin

5.6.2.1. Tất cả mật khẩu máy tính đều phải được bảo vệ ở cấp độ cao, cụ thể:

- Độ dài tối thiểu của mật khẩu là 8 ký tự.
- Có đủ ký tự viết hoa, viết thường, số và biểu tượng.
- Hạn chế việc sử dụng mật khẩu cũ. Bắt buộc thay đổi mật khẩu sau mỗi 90 ngày

5.6.2.2. Mỗi máy tính phải có chương trình chống virus và tường lửa phải. Tất cả các phần mềm được sử dụng phải là phần mềm có bản quyền và thường xuyên nâng cấp.

5.6.2.3. Các thông tin sản xuất, thiết kế và các hồ sơ công việc được lưu trữ ổ đĩa hệ thống và phải có giới hạn quyền truy cập.

5.6.2.4. Máy chủ quản lý emails và các tập tin đính kèm phải đảm bảo an toàn, tốt nhất là sử dụng chương trình IMAP Protocol hoặc chương trình tương đương, thay vì lưu trữ tại máy con thông qua ứng dụng email POP3+.

5.6.2.5. Bộ phận IT phải cài đặt sao lưu mỗi ngày vào máy chủ công ty các tài liệu mật, các hồ sơ mẫu mã mới và các dữ liệu sản xuất phát sinh từ bộ phận nghiên cứu và phát triển sản phẩm. Ngoài ra bộ phận IT cũng phải có một bản sao dự liệu lưu ở nơi an toàn chống cháy bên ngoài phòng máy chủ. Không được phép mang bản sao dữ liệu ra khỏi nơi lưu trữ đã quy định.

5.6.2.6. Tất cả các máy tính không được phép truy cập internet và sử dụng USB sai quy định. Tất cả các cổng USB phải được khóa. Xin tham khảo thêm quy định truy cập internet và sử dụng USB của công ty.

5.6.2.7. Tất cả máy tính được bảo mật bằng mật khẩu đăng nhập và bảo vệ màn hình nếu máy tính không hoạt động trên 3 phút. Máy tính có thể bị vô hiệu hóa nếu có thể.

5.6.3. Đánh dấu và quản lý dép mẫu

5.6.3.1. Dép mẫu cần được may tem security và đánh dấu với từ “Sample” (Dép mẫu) ngay sau trong quá trình làm mẫu. Nếu mẫu không thể may tem security thì phải in hoặc đóng dấu bằng mực không phai.

5.6.3.2. Tất cả các dép mẫu lưu giữ phải được đục lỗ trên insole.

5.6.3.3. Phải có bảng theo dõi cho từng mẫu, bao gồm ngày và giờ nhận, triển khai, xuất mẫu,

và người chịu trách nhiệm về mẫu.

5.6.4. Lưu trữ dép mẫu

5.6.4.1. Kho lưu dép mẫu phải an toàn và được bảo vệ. Việc ra vào kho phải được kiểm soát.

Nếu dép mẫu được lưu giữ trong tủ, tủ phải được khóa bằng ổ khóa an toàn.

5.6.4.2. Kho phải gọn gàng, sạch sẽ. Phải có sổ theo dõi xuất nhập tồn. Khi xuất hàng ra khỏi kho phải có ít nhất 2 người chứng nhận. Phải kiểm tra tồn khi hàng tháng. Nếu có sai sót phải lập tức báo cáo cho chủ quản cấp cao.

5.6.4.3. Chìa khóa kho không được mang ra khỏi khu vực, mà phải được lưu giữ ở nơi an toàn, có phân công quyền sử dụng.

5.6.5. Kiểm soát tài liệu

5.6.5.1. Tài liệu phải được đánh dấu bảo mật theo Quy Định Bảo Mật Thông Tin của công ty.

Bộ phận phải mở sổ đăng ký khi in tài liệu này.

5.6.5.2. Thiết bị dùng để photo hay scan các tài liệu này phải đặt ở trong phòng nghiên cứu và phát triển sản phẩm, đồng thời phải có cài đặt mật khẩu.

5.6.5.3. Cuối ngày, tất cả giấy không dùng nữa phải được cắt bỏ bằng máy cắt giấy.

5.7. Quy định an ninh dành cho phòng in tem security

5.7.1. Giám Đốc sản xuất phải chỉ định người chịu trách nhiệm về an ninh bảo mật của phòng in tem security và phải quản lý an ninh vật chất, vật liệu và tồn kho của khu vực này.

5.7.2. Phòng in tem phải đủ an toàn, có gắn biển cảnh báo có 4 nội dung, lắp hệ thống kiểm soát ra vào điện tử (EAC), Camera an ninh (CCTV), kiểm soát đăng nhập trái phép (IDS) đạt được các tiêu chuẩn theo quy định ở các hạng mục bên trên.

5.7.3. Trừ những trường hợp đặc biệt do Ban TGD phê duyệt, tất cả CBCNV đều không được phép mang theo các vật dụng cá nhân vào bên trong bộ phận. Vật dụng cá nhân bao gồm: túi xách, camera và các thiết bị điện tử có chức năng camera. Ở ngoài cửa phòng làm việc phải có tủ.

5.7.4. Cửa ra vào phải có khóa tay tự động đóng.

5.7.5. Các tem nhãn đã in, dụng cụ, vật liệu phải được bảo quản an toàn trong tủ đặt trong phòng. Chìa khóa phòng không được mang ra khỏi phòng, và phải được giữ trong một ngăn tủ có khóa và chỉ định người quản lý chìa khóa.

- 5.7.6. Máy tính phải có mật khẩu bảo vệ, khóa internet và cổng USB.
- 5.7.7. Phải có sổ quản lý xuất nhập tồn. Khi xuất tem ra khỏi kho phải có ít nhất 2 người. Phải kiểm tra hàng tồn kho hàng tuần, nếu có sai sót phải báo cáo ngay cho chủ quản.
- 5.7.8. Khu vực lưu trữ tem nhãn và vật liệu phải gọn gàng, sạch sẽ và bảo mật. Có 3 hộp được đánh dấu "Hàng Phế", "Tem nhãn đã in không sử dụng", "Tem nhãn sản xuất trả về" để phân loại tem phế hoặc các tem nhãn lỗi cho đến khi nhận được hướng dẫn xử lý hàng phế. Phải thực hiện báo cáo xử lý hàng phế cho khách hàng và nhà cung cấp vật liệu in tem mỗi tháng.
- 5.7.9. Trường hợp phải xuất tem ra khỏi công ty cho một đơn vị đã được Ban TGD đồng ý, thì chủ quản phải chỉ định một nhân viên phụ trách ghi nhận và chứng kiến việc gửi tem. Chủ quản phòng in tem phải đảm bảo có sẵn quy trình hướng dẫn thực hiện. Nhân viên gửi tem phải ghi nhận và chứng kiến quá trình đưa tem. Sau đó chủ quản phải xem xét lại nội dung ghi chép đó.
- 5.7.10. Quá trình hủy tem cần được chứng kiến bởi đại diện khách hàng hoặc nhà cung cấp vật liệu in tem. Phải có sổ ghi chép lại thông tin và bằng chứng hủy tem. Tham khảo quy định về tem security của khách hàng.

5.8. Quy định an ninh bảo mật tại xưởng sản xuất

- 5.8.1. Bộ phận Tech và quá trình chuyển giao thông tin từ phòng mẫu đến xưởng nằm trong bộ phận nghiên cứu và phát triển sản phẩm. Do đó mọi quá trình chuyển giao này phải tuân thủ quy định an ninh bảo mật dành cho bộ phận nghiên cứu phát triển sản phẩm ở mục 5.6 bên trên.
- 5.8.2. Công ty hiện không có bộ phận làm khuôn. Tuy nhiên, nếu sau này có phát sinh hoạt động làm khuôn nội bộ thì phải tuân thủ quy định an ninh bảo mật dành cho bộ phận nghiên cứu phát triển sản phẩm ở mục 5.6 bên trên.
- 5.8.3. Khu vực sản xuất
- 5.8.3.1. Giám Đốc sản xuất phải chỉ định một nhân viên phụ trách an ninh bảo mật của khu vực sản xuất.
- 5.8.3.2. Nhà xưởng phải đảm bảo an toàn, có gắn bảng cảnh báo 4 nội dung, hệ thống camera an ninh CCTV ở các cửa ra và các hoạt động ở khu vực sản xuất.
- 5.8.3.3. Trừ những trường hợp đặc biệt do Ban TGD phê duyệt, tất cả CBCNV đều không được phép mang theo các vật dụng cá nhân vào bên trong bộ phận. Vật dụng cá nhân

bao gồm: túi xách, camera và các thiết bị điện tử có chức năng camera. Ở ngoài cửa phòng làm việc phải có tủ để đồ cá nhân.

5.8.3.4. Máy tính phải có mật khẩu bảo vệ, khóa internet và cổng USB.

5.8.3.5. Nơi làm việc phải gọn gàng, ngăn nắp. Tất cả các vật dụng liên quan đến công việc đều phải được giữ an toàn khi nhân viên rời khỏi nơi làm việc.

5.8.3.6. Khu vực đóng gói phải tập trung, không nằm rải rác, có quản lý theo dõi công việc và có lắp camera an ninh CCTV.

5.8.3.7. Hàng đóng gói xong phải chuyển sang kho thành phẩm với sự chứng kiến của 2 người. Phải quét nhập kho bằng phần mềm kho thành phẩm để lưu trữ thông tin.

5.8.3.8. Các biểu mẫu thống kê báo cáo đều phải hiển thị số chỉ lệnh JH# và/hoặc số đơn hàng của khách (PO#)

5.8.3.9. Phải có tủ để giữ hàng B/C và tem security sử dụng không hết trong ngày. Phải phân công người chịu trách nhiệm quản lý tủ này.

5.8.3.10. Hồ sơ liên quan đến đơn hàng phải có tủ bảo quản. Giấy tờ không dùng nữa phải cắt bỏ bằng máy hủy giấy.

5.9. Quy định bảo mật dành cho phòng thử nghiệm

5.9.1. Phòng thử nghiệm phải an toàn, có gắn bảng cảnh báo 4 nội dung, hệ thống kiểm soát ra vào điện tử (EAC), hệ thống camera an ninh CCTV, kiểm soát xâm nhập trái phép (IDS).

5.9.2. Trừ những trường hợp đặc biệt do Ban TGD phê duyệt, tất cả CBCNV đều không được phép mang theo các vật dụng cá nhân vào bên trong bộ phận. Vật dụng cá nhân bao gồm: túi xách, camera và các thiết bị điện tử có chức năng camera. Ở ngoài cửa phòng làm việc phải có tủ để đồ cá nhân.

5.9.3. Máy tính phải có mật khẩu bảo vệ, khóa internet và cổng USB.

5.9.4. Nơi làm việc phải gọn gàng, ngăn nắp. Tất cả các vật dụng liên quan đến công việc đều phải được giữ an toàn khi nhân viên rời khỏi nơi làm việc.

5.9.5. Phải mở sổ theo dõi giao nhận mẫu thử nghiệm. Khi giao nhận phải có ít nhất 2 người.

5.9.6. Phải có kho lưu trữ mẫu thử nghiệm, có nhân viên quản lý và mở sổ theo dõi xuất nhập tồn.

5.9.7. Hồ sơ liên quan đến đơn hàng phải có tủ bảo quản. Giấy tờ không dùng nữa phải cắt bỏ

bằng máy hủy giấy.

5.10. Quy định an ninh dành cho Khu vực chất hàng/ Dỡ hàng

- 5.10.1. Khu vực chất hàng và dỡ hàng phải nằm trong khuôn viên của nhà máy, là khu vực giới hạn, chỉ có CBCNV được cấp phép mới có quyền ra vào khu vực này.
- 5.10.2. CBCNV phụ trách và nhân viên bảo vệ phải giám sát quá trình chất, dỡ hàng thành phẩm.
- 5.10.3. Ở cửa ra vào khu vực này phải có bảng cảnh báo 4 nội dung, có lắp đặt camera an ninh CCTV ở xung quanh có thể theo dõi được hoạt động đóng hàng và bên trong container.
- 5.10.4. Lắp đặt hệ thống ánh sáng đầy đủ để chiếu sáng khu vực này và bên trong container trong suốt quá trình chất, dỡ hàng.

5.11. An ninh bảo mật dành cho kho thành phẩm

- 5.11.1. Giám Đốc sản xuất chỉ định một nhân viên của kho thành phẩm chịu trách nhiệm về an ninh bảo mật của kho.
- 5.11.2. Nhà kho phải đảm bảo an toàn, có gắn bảng cảnh báo 4 nội dung, lắp đặt hệ thống kiểm soát ra vào điện tử (EAC) bằng dấu vân tay hoặc dùng ổ khóa có độ bảo mật cao, có camera an ninh CCTV giám sát các lối vào và các hoạt động ở Kho thành phẩm, có hệ thống chống xâm nhập trái phép (IDS) đáp ứng đầy đủ các tiêu chuẩn đã nêu ở các mục bên trên. Nếu có ra vào kho phải đăng ký sổ. Thông tin ghi nhận ra vào kho ở sổ và camera phải lưu trữ ít nhất 1 năm.
- 5.11.3. Trừ những trường hợp đặc biệt do Ban TGD phê duyệt, tất cả CBCNV đều không được phép mang theo các vật dụng cá nhân vào bên trong bộ phận. Vật dụng cá nhân bao gồm: túi xách, camera và các thiết bị điện tử có chức năng camera. Ở ngoài cửa phòng làm việc phải có tủ để đồ cá nhân.
- 5.11.4. Cửa kho phải có hệ thống khuỷu tay đóng cửa tự động. Chìa khóa kho không được mang ra khỏi kho, mà phải được lưu giữ trong một tủ có khóa, có phân quyền sử dụng.
- 5.11.5. Tất cả các máy tính ở kho phải được bảo mật, không kết nối internet và khóa kết nối USB.
- 5.11.6. Phải dùng phần mềm kho thành phẩm để quét nhập kho, xuất kho và quản lý hàng tồn. Khi xuất kho phải có đủ các bên liên quan giám sát theo quy trình xuất nhập kho của công ty.
Định kỳ hàng quý phải kiểm kê kho, nếu có bất kỳ sai sót nào phải báo cáo ngay cho chủ

quản cấp cao.

5.12. Quy định an ninh bảo mật cho kho hàng B/C

- 5.12.1. Quản lý QIP phải chỉ định một nhân viên chịu trách nhiệm về an ninh bảo mật của kho B/C.
- 5.12.2. Nhà kho phải đảm bảo an toàn, có gắn bảng cảnh báo 4 nội dung, lắp đặt hệ thống kiểm soát ra vào điện tử (EAC) bằng dấu vân tay, có camera an ninh CCTV giám sát các lối vào và các hoạt động ở Kho, có hệ thống chống xâm nhập trái phép (IDS) đáp ứng đầy đủ các tiêu chuẩn đã nêu ở các mục bên trên. Nếu có ra vào kho phải đăng ký sổ. Thông tin ghi nhận ra vào kho ở sổ, camera và máy quét vân tay phải lưu trữ ít nhất 1 năm
- 5.12.3. Trừ những trường hợp đặc biệt do Ban TGD phê duyệt, tất cả CBCNV đều không được phép mang theo các vật dụng cá nhân vào bên trong bộ phận. Vật dụng cá nhân bao gồm: túi xách, camera và các thiết bị điện tử có chức năng camera. Ở ngoài cửa phòng làm việc phải có tủ để đồ cá nhân.
- 5.12.4. Cửa kho phải có hệ thống khuỷu tay đóng cửa tự động. Chìa khóa kho không được mang ra khỏi kho, mà phải được lưu giữ trong một tủ có khóa, có phân quyền sử dụng.
- 5.12.5. Tất cả các máy tính ở kho phải được bảo mật, không kết nối internet và khóa kết nối USB.
- 5.12.6. Hàng hóa trong kho phải sắp xếp gọn gàng, theo thứ tự thời gian như khách hàng quy định. Khi xuất kho phải có đủ các bên liên quan giám sát theo quy trình xuất nhập kho của công ty. Định kỳ hàng tháng phải kiểm kê kho, nếu có bất kỳ sai sót nào phải báo cáo ngay cho chủ quản cấp cao.

- 5.12.7. Hàng C phải được cất ở eo trong, eo ngoài và có dán tem theo quy định của khách hàng

5.13. Quy định về việc cắt phế

- 5.13.1. Việc cắt phế các sản phẩm bị lỗi, các hàng mẫu, hàng B/C, các khuôn gỗ cũ, các khuôn nhôm và khuôn thép phải tuân theo quy định của khách hàng và quy định hàng phế của công ty.
- 5.13.2. Các bằng chứng cắt phế, hình ảnh hoặc video, phải được lưu lại trong 3 năm. Trước khi tiêu hủy, phải báo cáo cho ít nhất một đại diện adidas để làm chứng việc cắt phế.
- 5.13.3. Cuối ngày, tất cả các hồ sơ liên quan đến hàng hóa và thông tin của khách hàng phải được thu gom lại và hủy bằng máy hủy giấy.

5.13.4. Khu vực bãi rác phải gọn gàng, ngăn nắp, không được có bất kỳ tài liệu bảo mật hoặc nhạy cảm nào liên quan đến khách hàng.

5.14. Quy định an ninh bảo mật dành cho bộ phận IT

- 5.14.1. Bảo mật thông tin IT liên quan đến việc bảo vệ các máy tính và hệ thống đường truyền khỏi các sự rò rỉ thông tin ra bên ngoài. Do đó, bộ phận IT phải giới hạn việc truy cập internet và khóa cổng USB theo quy định của công ty.
- 5.14.2. Bộ phận IT phải chỉ định một cá nhân chịu trách nhiệm đảm bảo an ninh thông tin cho bộ phận IT.
- 5.14.3. Bộ phận IT phải hướng dẫn đào tạo cho người dùng các quy định về sử dụng máy tính. Sau khi đào tạo, người dùng phải ký xác nhận đã đọc và hiểu “quy định dành cho người dùng”.
- 5.14.4. Phòng máy chủ phải đảm bảo an toàn, có gắn bảng cảnh báo 4 nội dung, hệ thống kiểm soát ra vào điện tử (EAC) bằng dấu vân tay, camera an ninh CCTV giám sát các lối vào và các hoạt động ở phòng máy chủ, hệ thống phát hiện xâm nhập trái phép (IDS) đáp ứng đầy đủ các tiêu chuẩn theo quy định bên trên. Ra vào phòng máy chủ phải đăng ký sổ. Nội dung ra ghi chép việc ra vào tại sổ, máy quét vân tay và CCTV phải được lưu trữ ít nhất 1 năm.
- 5.14.5. Máy chủ phải có nguồn điện liên tục không đứt quãng (UPS) hỗ trợ tối thiểu trong 4 giờ, hoặc 1 giờ với nguồn máy phát điện dự phòng, khi xảy ra sự cố mất điện.
- 5.14.6. Máy chủ phải được cài đặt mật khẩu đạt độ bảo mật cao, cụ thể:
- Tối thiểu dài 4 ký tự.
 - Có đủ chữ viết hoa, viết thường, số và ký hiệu.
 - Hạn chế việc sử dụng mật khẩu cũ. Bắt buộc thay đổi mật khẩu sau mỗi 90 ngày.
 - Giới hạn số lượng nhập mật khẩu tối đa.
 - Cài đặt chương trình diệt virus và tường lửa ở mỗi khu vực làm việc và máy chủ.
 - Tất cả phần mềm được sử dụng phải có bản quyền và thường xuyên cập nhật.
- 5.14.7. Các thiết kế, dữ liệu sản xuất và nội dung công việc của các BPPX phải được lưu trữ trên ổ đĩa hệ thống (máy chủ), có phân quyền sử dụng cụ thể.

5.14.8. Tốt nhất nên cài đặt webmail, IMAP hoặc đường truyền tương đương thay vì POP3.

5.14.9. Mỗi ngày bộ phận IT phải sao lưu các tài liệu bảo mật, các thiết kế nhạy cảm và dữ liệu sản xuất liên quan đến khách hàng. Một bản sao lưu phải được lưu trữ ở một nơi an toàn và có khả năng chống cháy bên ngoài phòng máy chủ. Không được phép mang bản sao lưu ra khỏi nơi lưu trữ theo quy định.

5.14.10. Bộ phận IT phải giới hạn quyền truy cập internet và khóa cổng USB với các máy tính có sử dụng các thiết kế nhạy cảm và các dữ liệu sản xuất theo quy định sử dụng internet của công ty. Hàng tháng bắt buộc phải rà soát việc truy cập internet và sử dụng cổng USB này.

5.14.11. Bộ phận IT phải cài đặt để đảm bảo tất cả máy tính đều được bảo vệ với mật khẩu đăng nhập và bảo vệ màn hình nếu máy tính không hoạt động trên 3 phút.

6. TÀI LIỆU LIÊN QUAN:

6.1. Hướng dẫn an ninh bảo mật nguồn cung ứng dành cho các nhà máy và nhà thầu phụ của adidas (Sourcing security guidelines for adidas Groupd factories and contractors)

6.2. Quy định bảo mật thông tin, hồ sơ, tài liệu 007/QTHT/HC

6.3. Quy Trình Hoạt Động Đội Bảo Vệ 050/QTHT/TV

6.4. Quy định truy cập internet và sử dụng USB của công ty

6.5. Quy Định Bảo Mật Thông Tin

6.6. Quy định về tem security của adidas.

6.7. Quy trình xuất nhập kho của công ty

6.8. Quy định hủy hàng phế của công ty.

7. BIỂU MẪU SỬ DỤNG:

7.1. Kế hoạch đánh giá nội bộ an ninh bảo mật BM01/017/CSHT/LĐ

7.2. Sổ ghi chép tình hình an ninh bảo mật hằng ngày BM02/017/CSHT/LĐ

7.3. Danh sách liên hệ khẩn cấp khi có sự cố an ninh BM03/017/CSHT/LĐ

8. LỊCH SỬ TÀI LIỆU:

1.1. Ban hành lần đầu ngày 05/05/2016

1.2. Ban hành lần hai ngày 01/06/2018

Lần sửa	Hạng mục sửa đổi	Nội dung sửa đổi
1		Thay đổi người soạn thảo, xem xét, phê duyệt Thay đổi danh sách liên hệ khẩn cấp nội bộ khi có sự cố

DANH SÁCH LIÊN HỆ KHẨN CẤP NỘI BỘ KHI CÓ SỰ CỐ

STT	HỌ VÀ TÊN	BỘ PHẬN	SỐ ĐIỆN THOẠI	GHI CHÚ
1	LI CHUN YEN	BAN TGD	0908.016.889	
2	CHOU CHUN KAI	BAN TGD	0988.080.929	
3	YANG MING TA	BAN TGD	0908.585.324	
4	HSU CHIA YUAN	GIÁM ĐỐC CR	0902.704.583	
5	NGUYỄN THỊ KIM ANH	PHÓ GIÁM ĐỐC CR	0918.798.493	
6	VIÊN Y MI	CHỦ NHIỆM HR	0908.355.677	
7	TRẦN TUYẾT ÂN	TRỢ LÝ TGD	0122.7779.700	
8	TRẦN ANH DŨNG	CHỦ NHIỆM BẢO VỆ	0938.339.254	

DANH SÁCH LIÊN HỆ KHẨN CẤP BÊN NGOÀI KHI CÓ SỰ CỐ

STT	HỌ VÀ TÊN	BỘ PHẬN	SỐ ĐIỆN THOẠI	GHI CHÚ
1	MERRY NGUYỄN	KHÁCH HÀNG NB	0908.805.019	
2	ĐỖ KỲ QUỐC	CÔNG AN	0917.676.717	
3		HẢI QUAN	0272.3891.632	
4	COREANA	HÃNG TÀU	84 (8) 3848- 4241	
5	EVERGREEN	HÃNG TÀU	866-2-2512-6932	
6	IG LOGISTIC VIETNAM CO.,LTD	HÃNG TÀU	84-8-3915-3021	
7	UNIQUE	HÃNG TÀU	84-8-38222352	
8	APL	HÃNG TÀU	84-8-38221166	
9	SG SAGAWA VIET NAM CO.,LTD	HÃNG TÀU	84-8-3840-9330	
10	EVERLINES	HÃNG TÀU	(848)39140835	
11	FDI CO.,LTD	HÃNG TÀU	84 8-3997779	
12	WORLDWIDE LOGISTICS VN CO.; LTD	HÃNG TÀU	84 8 8107669	

STT	HỌ VÀ TÊN	BỘ PHẬN	SỐ ĐIỆN THOẠI	GHI CHÚ
13	SAGAWA EXPRESS VIET NAM	HÃNG TÀU	84-4-38432088/82/83	
14	ANH NGUYEN	ADIDAS	0933 223 044	
15	KEVIN RYAN	ADIDAS	0932 107 379	
16	LINH NGUYEN	ADIDAS	091 5775 449	
17	CUONG TRAN	ADIDAS	0913 745 240	
18	LAC NGUYEN	ADIDAS	0918 133 168	