# CHÍNH SÁCH AN NINH THÔNG TIN VÀ BẢO VỆ, XỬ LÝ DỮ LIỆU CÁ NHÂN

## PHẦN I: QUY ĐỊNH CHUNG VỀ BẢO VỆ VÀ XỬ LÝ DỮ LIỆU

### Điều 1: Mục đích

Chính sách Bảo vệ và Xử lý dữ liệu cá nhân ("Chính sách") này quy định các điều khoản và điều kiện về Bảo vệ và Xử lý dữ liệu cá nhân của CÔNG TY TNHH AIRCLOSET ENGINEERING trên cơ sở tuân thủ Nghị định 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân và các quy định của pháp luật hiện hành có liên quan.

### Điều 2: Phạm vi, đối tượng áp dụng

2.1. Toàn thể Cán bộ Nhân viên tại CÔNG TY TNHH AIRCLOSET ENGINEERING.

2.2. Bên Cung cấp dữ liệu cá nhân (ứng viên, người lao động, cộng tác viên, thực tập sinh, người tập nghề, đối tác trong các dự án có nhân sự tham gia thực hiện công việc...).

2.3. Chủ thể dữ liệu cá nhân.

2.4. Trong bản Chính sách này, CÔNG TY TNHH AIRCLOSET ENGINEERING là Bên Kiểm soát và Xử lý dữ liệu cá nhân.

### Điều 3: Văn bản pháp luật điều chỉnh

Bộ Luật Dân sự 2015.

Luật An Ninh Mạng 2018

Luật An toàn thông tin mạng 2015

Nghị định 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân

### Điều 4: Giải thích từ ngữ

4.1. Dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể. Dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm.

4.2. Dữ liệu cá nhân cơ bản gồm: Họ, chữ đệm và tên khai sinh, tên gọi khác (nếu có); Ngày, tháng, năm sinh; ngày, tháng, năm chết hoặc mất tích; Giới tính; Nơi sinh, nơi đăng ký khai sinh, nơi thường trú, nơi tạm trú, nơi ở hiện tại, quê quán, địa chỉ liên hệ; Quốc tịch; Hình ảnh của cá nhân; Số điện thoại, số chứng minh nhân dân, số định danh cá nhân, số hộ chiếu, số giấy phép lái xe, số biển số xe, số mã số thuế cá nhân, số bảo hiểm xã hội, số thẻ bảo hiểm y tế; Tình trạng hôn nhân; Thông tin về mối quan hệ gia đình (cha mẹ, con cái); Thông tin về tài khoản số của cá nhân; dữ liệu cá nhân phản ánh hoạt động, lịch sử hoạt động trên không gian mạng; Các thông tin khác gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể mà không phải là dữ liệu cá nhân nhạy cảm.

4.3. Dữ liệu cá nhân nhạy cảm là dữ liệu cá nhân gắn liền với quyền riêng tư của cá nhân mà khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp tới quyền và lợi ích hợp pháp của cá nhân gồm: Quan điểm chính trị, quan điểm tôn giáo; Tình trạng sức khỏe và đời tư được ghi trong hồ sơ bệnh án, không bao gồm thông tin về nhóm máu; Thông tin liên quan đến nguồn gốc chủng tộc, nguồn gốc dân tộc; Thông tin về đặc điểm di truyền được thừa hưởng hoặc có được của cá nhân; Thông tin về thuộc tính vật lý, đặc điểm sinh học riêng của cá nhân; Thông tin về đời sống tình dục, xu hướng tình dục của cá nhân; Dữ liệu về tội phạm, hành vi phạm tội được thu thập, lưu trữ bởi các cơ quan thực thi pháp luật; Thông tin khách hàng của tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán, các tổ chức được phép khác, gồm: thông tin định danh khách hàng theo quy định của pháp luật, thông tin về tài khoản, thông tin về tiền gửi, thông tin về tài sản gửi, thông tin về giao dịch, thông tin về tổ chức, cá nhân là bên bảo đảm tại tổ chức tín dụng, chi nhánh ngân hàng, tổ chức cung ứng dịch vụ trung gian thanh toán; Dữ liệu về vị trí của cá nhân được xác định qua dịch vụ định vị; Dữ liệu cá nhân khác được pháp luật quy định là đặc thù và cần có biện pháp bảo mật cần thiết.

4.4. Bảo vệ dữ liệu cá nhân là hoạt động phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi vi phạm liên quan đến dữ liệu cá nhân theo quy định của pháp luật.

4.5. Xử lý dữ liệu cá nhân là một hoặc nhiều hoạt động tác động tới dữ liệu cá nhân, như: thu thập, ghi, phân tích, xác nhận, lưu trữ, chỉnh sửa, công khai, kết hợp, truy cập, truy xuất, thu hồi, mã hóa, giải mã, sao chép, chia sẻ, truyền đưa, cung cấp, chuyển giao, xóa, hủy dữ liệu cá nhân hoặc các hành động khác có liên quan.

4.6. Bên Nhận Dữ Liệu Cá Nhân là CÔNG TY TNHH AIRCLOSET ENGINEERING và/hoặc bên được CÔNG TY TNHH AIRCLOSET

ENGINEERING ủy quyền nhằm mục đích thực hiện các hoạt động về bảo vệ và xử lý dữ liệu cá nhân theo quy định của pháp luật.

4.7. Bên Cung Cấp Dữ Liệu Cá nhân là cá nhân hoặc tổ chức cung cấp dữ liệu cá nhân cho Bên nhận dữ liệu cá nhân.

4.8. Bên Kiểm Soát Và Xử Lý Dữ Liệu Cá Nhân là CÔNG TY TNHH AIRCLOSET ENGINEERING đồng thời quyết định mục đích, phương tiện và trực tiếp xử lý dữ liệu cá nhân.

4.9. Chủ Thể Dữ Liệu là cá nhân được dữ liệu cá nhân phản ánh.

4.10. Sự đồng ý của chủ thể dữ liệu là việc thể hiện rõ ràng, tự nguyện, khẳng định việc cho phép xử lý dữ liệu cá nhân của chủ thể dữ liệu.

4.11. Chuyển dữ liệu cá nhân ra nước ngoài là hoạt động sử dụng không gian mạng, thiết bị, phương tiện điện tử hoặc các hình thức khác chuyển dữ liệu cá nhân của công dân Việt Nam tới một địa điểm nằm ngoài lãnh thổ của nước Cộng hòa xã hội chủ nghĩa Việt Nam hoặc sử dụng một địa điểm nằm ngoài lãnh thổ của nước Cộng hòa xã hội chủ nghĩa Việt Nam để xử lý dữ liệu cá nhân của công dân Việt Nam, bao gồm: (a)Tổ chức, doanh nghiệp, cá nhân chuyển dữ liệu cá nhân của công dân Việt Nam cho tổ chức, doanh nghiệp, bộ phận quản lý ở nước ngoài để xử lý phù hợp với mục đích đã được chủ thể dữ liệu đồng ý; (b) Xử lý dữ liệu cá nhân của công dân Việt Nam bằng các hệ thống tự động nằm ngoài lãnh thổ của nước Cộng hòa xã hội chủ nghĩa Việt Nam của Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân phù hợp với mục đích đã được chủ thể dữ liệu đồng ý.

4.12. Bên Thứ Ba là cá nhân, tổ chức ngoài Bên Nhận Dữ Liệu Cá Nhân và Bên Cung Cấp Dữ Liệu Cá Nhân được phép Xử Lý Dữ Liệu Cá nhân theo quy định của pháp luật Việt Nam hiện hành, bao gồm nhưng không giới hạn (a) Công ty mẹ của CÔNG TY TNHH AIRCLOSET ENGINEERING (“Công ty mẹ”), các nhà thầu, đại diện của Công ty mẹ, (b) các kiểm toán viên, các nhà tư vấn pháp lý/thuế/kế toán/bảo hiểm/khám sức khỏe...của CÔNG TY TNHH AIRCLOSET ENGINEERING hoặc của các bên đối tác cung cấp dịch vụ cho CÔNG TY TNHH AIRCLOSET ENGINEERING hoặc của Công ty mẹ, (c) nhà cung cấp dịch vụ phần mềm kế toán và những người thực hiện việc bảo trì, nâng cấp, bảo hành của phần mềm đó; (d) Các cơ quan Nhà nước có thẩm quyền của Việt Nam; (e ) Bất kỳ đối tác nào mà hợp tác với CÔNG TY TNHH AIRCLOSET ENGINEERING nhằm cung cấp các sản phẩm/dịch vụ trong phạm vi kinh doanh của CÔNG TY TNHH

AIRCLOSET ENGINEERING; và (f) bất kỳ bên thứ ba nào khác hợp pháp hoặc được yêu cầu bởi luật pháp, lệnh của cơ quan nhà nước có thẩm quyền hoặc bởi tòa án, trung tâm trọng tài quốc tế có đủ thẩm quyền hoặc yêu cầu của Chính Phủ, hoặc theo yêu cầu từ các chính sách nội bộ phù hợp với luật pháp Việt Nam hiện hành của Công ty mẹ hoặc CÔNG TY TNHH AIRCLOSET ENGINEERING để phục vụ cho mục đích Xử Lý Dữ Liệu Cá Nhân nêu tại bản Chính sách này.

4.13. Bên chuyển dữ liệu ra nước ngoài bao gồm Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên Kiểm soát dữ liệu cá nhân (nếu có), Bên Xử lý dữ liệu cá nhân (nếu có), Bên thứ ba (nếu có).

4.14. Để tránh hiểu lầm, trong Chính sách này, những nội dung được ghi là "theo quy định của pháp luật", "theo quy định của pháp luật hiện hành" , "theo quy định của CÔNG TY TNHH AIRCLOSET ENGINEERING" sẽ đều được hiểu là quy định tại từng thời điểm nhất định. Những quy định đó có thể thay đổi do sự thay đổi của pháp luật hoặc thay đổi theo quyết định riêng của CÔNG TY TNHH AIRCLOSET ENGINEERING.

4.15. Trong bản Chính sách này khi một khái niệm/định nghĩa được nhắc tới, sẽ được hiệu là đề cập tới một và/hoặc đồng thời nhiều khái niệm/định nghĩa/hành vi như được mô tả tại định nghĩa/khái niệm đó.

**Điều 5: Nguyên tắc Bảo vệ và Xử lý dữ liệu cá nhân**

5.1. Dữ liệu cá nhân được xử lý theo quy định của pháp luật.

5.2. Chủ thể dữ liệu được biết về hoạt động liên quan tới xử lý dữ liệu cá nhân của mình, trừ trường hợp luật có quy định khác.

5.3. Dữ liệu cá nhân chỉ được xử lý đúng với mục đích đã được Bên Kiểm soát và xử lý dữ liệu cá nhân thông báo/tuyên bố về xử lý dữ liệu cá nhân.

5.4. Dữ liệu cá nhân thu thập phải phù hợp và giới hạn trong phạm vi, mục đích cần xử lý. Dữ liệu cá nhân không được mua, bán dưới mọi hình thức, trừ trường hợp pháp luật có quy định khác.

5.5. Dữ liệu cá nhân được cập nhật, bổ sung phù hợp với mục đích xử lý.

5.6. Dữ liệu cá nhân được áp dụng các biện pháp bảo vệ, bảo mật trong quá trình xử lý, bao gồm cả việc bảo vệ trước các hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân và phòng, chống sự mất mát, phá hủy hoặc thiệt hại do sự cố, sử dụng các biện pháp kỹ thuật.

5.7. Dữ liệu cá nhân chỉ được lưu trữ trong khoảng thời gian phù hợp với mục đích xử lý dữ liệu, trừ trường hợp pháp luật có quy định khác.

5.8. Bên Kiểm soát dữ liệu, Bên Kiểm soát và xử lý dữ liệu cá nhân phải chịu trách nhiệm tuân thủ các nguyên tắc xử lý dữ liệu được quy định tại các văn bản pháp luật hiện hành và Chính sách này và chứng minh sự tuân thủ của mình với các nguyên tắc xử lý dữ liệu đó.

## PHẦN II: CÁC QUY TẮC VỀ AN NINH THÔNG TIN TỔNG THỂ

### Điều 6: Quản lý tài sản thông tin

6.1. Phân loại và Gán Chủ sở hữu

Phân loại: Tất cả Tài sản Thông tin (bao gồm dữ liệu, hệ thống, thiết bị phần cứng, phần mềm) phải được phân loại theo mức độ nhạy cảm và giá trị đối với Công ty. Mức phân loại tối thiểu bao gồm: Công khai, Nội bộ, Bí mật/Tuyệt mật.

Gán Chủ sở hữu: Mỗi Tài sản Thông tin phải được gán cho một Chủ sở hữu chịu trách nhiệm về tính toàn vẹn, bảo mật và tính sẵn sàng của tài sản đó, đồng thời đảm bảo tài sản được bảo vệ theo mức phân loại.

6.2. Quy tắc Sử dụng Thiết bị

Sử dụng Thiết bị Công ty: Thiết bị do Công ty cấp chỉ được sử dụng cho mục đích công việc. Nhân viên không được phép can thiệp hoặc thay đổi cấu hình bảo mật cơ bản đã được Bộ phận IT thiết lập.

Sử dụng Phần mềm: Nhân viên chỉ được phép cài đặt và sử dụng phần mềm đã được cấp phép và phê duyệt. Việc cài đặt bất kỳ phần mềm không rõ nguồn gốc hoặc các ứng dụng P2P bị nghiêm cấm tuyệt đối.

6.3. Bảo vệ Thiết bị Di động và Làm việc Từ xa

6.3.1. Mã hóa Bắt buộc: Tất cả thiết bị di động (laptop, điện thoại) được sử dụng để truy cập mạng hoặc xử lý dữ liệu của Công ty (bao gồm cả thiết bị cá nhân được chấp thuận) phải được cài đặt Mã hóa ổ cứng.

6.3.2. Yêu cầu Bảo mật: Nhân viên làm việc từ xa phải đảm bảo môi trường làm việc tại nhà an toàn, sử dụng kết nối mạng có bảo mật (ví dụ: Wi-Fi có mật khẩu mạnh) và tuân thủ các quy định về VPN của Công ty khi truy cập hệ thống.

6.3.3. Lưu trữ Dữ liệu: Nghiêm cấm lưu trữ dữ liệu Bí mật/Tuyệt mật của Công ty trên thiết bị cá nhân hoặc các dịch vụ lưu trữ đám mây cá nhân không được phê duyệt.

6.4. Hủy bỏ Tài sản và Xóa Bỏ Dữ liệu An toàn

Xóa Bỏ Dữ liệu: Khi dữ liệu hoặc hồ sơ không còn cần thiết (sau khi hết thời gian lưu trữ), chúng phải được xóa bỏ một cách an toàn và không thể phục hồi.

Hủy Vật lý: Thiết bị lưu trữ vật lý (như ổ cứng, USB, đĩa CD) chứa dữ liệu Bí mật/Tuyệt mật phải được hủy bỏ bằng phương pháp vật lý (ví dụ: nghiền nát) trước khi bị loại bỏ khỏi Công ty.

Ghi nhận: Mọi quy trình Hủy bỏ Tài sản hoặc Xóa Bỏ Dữ liệu quan trọng phải được ghi lại trong hồ sơ của Bộ phận IT.

6.5. Xử lý Mất mát hoặc Đánh cắp Thiết bị

6.5.1. Báo cáo Khẩn cấp: Nhân viên có trách nhiệm báo cáo ngay lập tức (trong vòng 1 giờ) cho Bộ phận IT và Quản lý trực tiếp khi phát hiện thiết bị Công ty (laptop, điện thoại, thiết bị lưu trữ) bị mất hoặc bị đánh cắp.

6.5.2. Biện pháp Khẩn cấp: Bộ phận IT có quyền và trách nhiệm thực hiện các biện pháp khẩn cấp, bao gồm xóa dữ liệu từ xa (Remote Wipe) và vô hiệu hóa tài khoản truy cập, để ngăn chặn rò rỉ thông tin ngay khi nhận được thông báo mất mát.

**Điều 7: Kiểm soát truy cập**

7.1. Nguyên tắc Cấp quyền Truy cập

Nguyên tắc "Cần Biết": Quyền truy cập vào bất kỳ hệ thống, mạng hoặc dữ liệu nào chỉ được cấp khi nhân viên thực sự cần để hoàn thành nhiệm vụ được giao (Nguyên tắc Đặc quyền tối thiểu).

Quy trình Phê duyệt: Mọi yêu cầu cấp mới, sửa đổi hoặc thu hồi quyền truy cập phải được sự phê duyệt chính thức từ Chủ sở hữu Tài sản và/hoặc Quản lý trực tiếp.

7.2. Quản lý Danh tính và Mật khẩu

Mật khẩu Mạnh:

Mật khẩu phải có độ dài tối thiểu 8-12 ký tự.

Mật khẩu phải bao gồm kết hợp Chữ hoa, chữ thường, số, và ký tự đặc biệt.

Mật khẩu phải được thay đổi tối thiểu 90 ngày một lần.

Tài khoản và mật khẩu là cá nhân và không được chia sẻ dưới bất kỳ hình thức nào.

Xác thực Đa yếu tố: Bắt buộc kích hoạt Xác thực Đa yếu tố cho tất cả các tài khoản truy cập từ xa và các hệ thống chứa dữ liệu Bí mật/Tuyệt mật.

7.3. Quản lý Tài khoản Đặc quyền

7.3.1. Sử dụng Giới hạn: Các tài khoản có quyền quản trị cấp cao nhất chỉ được sử dụng cho mục đích bảo trì, quản lý hệ thống và không được sử dụng cho các hoạt động làm việc thường nhật (ví dụ: duyệt web, email).

7.3.2. Yêu cầu Bảo mật: Tài khoản đặc quyền phải sử dụng mật khẩu mạnh hơn tiêu chuẩn thông thường và bắt buộc sử dụng Xác thực Đa yếu tố.

7.3.3. Giám sát và Ghi nhật ký: Mọi hành động sử dụng tài khoản đặc quyền phải được ghi nhật ký chi tiết, lưu trữ và được Bộ phận IT kiểm tra, giám sát định kỳ.

**Điều 8: An ninh vật lý và môi trường**

8.1. Kiểm soát Ra vào

Khu vực Hạn chế: Các khu vực chứa tài sản quan trọng (ví dụ: Phòng máy chủ, khu vực lưu trữ hồ sơ nhân sự, tài chính) phải được xác định là khu vực hạn chế.

Quy định Khách thăm: Khách thăm phải luôn được đăng ký, được cấp thẻ và luôn được nhân viên Công ty tháp tùng trong suốt thời gian ở văn phòng.

8.2. Bảo vệ Khu vực làm việc

Chính sách "Màn hình Sạch/Bàn làm việc Sạch":

Nhân viên phải khóa máy tính ngay khi rời khỏi bàn làm việc, dù chỉ trong thời gian ngắn.

Tài liệu và các thiết bị lưu trữ vật lý chứa thông tin Nội bộ trở lên phải được cất giữ an toàn (khóa tủ, khóa ngăn kéo) khi nhân viên rời văn phòng hoặc không có mặt tại chỗ.

**Điều 9: An ninh mạng và hệ thống**

9.1. Bảo vệ Hệ thống và Chống Mã độc

Phòng chống Mã độc: Tất cả các thiết bị đầu cuối phải cài đặt và duy trì phần mềm chống mã độc được Công ty phê duyệt, đảm bảo cập nhật tự động và quét định kỳ.

Quản lý Bản vá: Nhân viên phải đảm bảo hệ điều hành và các ứng dụng quan trọng trên máy tính làm việc được cập nhật bản vá bảo mật kịp thời theo hướng dẫn của Bộ phận IT (ví dụ: trong vòng 7 ngày kể từ khi có bản vá).

9.2. Quy tắc An toàn Email và Internet

Email: Nghiêm cấm gửi tài liệu Bí mật/Tuyệt mật ra bên ngoài mạng Công ty mà không sử dụng các biện pháp mã hóa hoặc bảo vệ bằng mật khẩu.

Internet: Nghiêm cấm truy cập, tải xuống hoặc truyền tải nội dung bất hợp pháp, độc hại hoặc không phù hợp thông qua mạng và thiết bị của Công ty.

9.3 Đánh giá Lỗ hổng và Kiểm tra Thâm nhập

Đánh giá Lỗ hổng: Bộ phận IT phải thực hiện đánh giá lỗ hổng bảo mật định kỳ (tối thiểu 1 lần mỗi năm) đối với các hệ thống và ứng dụng quan trọng.

Khắc phục: Các lỗ hổng bảo mật được phát hiện phải được xử lý và khắc phục theo quy trình Quản lý Bản vá đã quy định.

**Điều 10: Quản lý an ninh nhân sự**

10.1. Đào tạo An ninh Thông tin

Nhận thức Bắt buộc: Tất cả nhân viên phải tham gia khóa đào tạo nhận thức về An ninh Thông tin và Bảo vệ Dữ liệu Cá nhân tối thiểu một (1) lần mỗi năm.

Phòng chống Lừa đảo: Chương trình đào tạo phải bao gồm nội dung nhận biết và báo cáo các mối đe dọa như Lừa đảo qua email và Tấn công Kỹ thuật xã hội.

10.2. Quy trình Thôi việc

Thu hồi Quyền truy cập: Bộ phận IT phải ngay lập tức vô hiệu hóa hoặc xóa toàn bộ tài khoản và quyền truy cập hệ thống của nhân viên thôi việc vào cuối ngày làm việc cuối cùng.

Thu hồi Tài sản: Toàn bộ tài sản vật lý của Công ty (laptop, thẻ từ, thiết bị lưu trữ) phải được hoàn trả và kiểm tra tình trạng trước khi nhân viên rời đi.

**PHẦN III: QUY ĐỊNH CỤ THỂ VỀ XỬ LÝ DỮ LIỆU CÁ NHÂN**

**Điều 11: Những hành vi bị nghiêm cấm khi Bảo vệ và Xử lý dữ liệu cá nhân**

11.1. Xử lý dữ liệu cá nhân trái với quy định của pháp luật về bảo vệ dữ liệu cá nhân.

11.2. Xử lý dữ liệu cá nhân để tạo ra thông tin, dữ liệu nhằm chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

11.3. Xử lý dữ liệu cá nhân để tạo ra thông tin, dữ liệu gây ảnh hưởng tới an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân khác.

11.4. Cản trở hoạt động bảo vệ dữ liệu cá nhân của cơ quan có thẩm quyền.

11.5. Lợi dụng hoạt động bảo vệ dữ liệu cá nhân để vi phạm pháp luật.

**Điều 12: Trách nhiệm của Bên Kiểm Soát Và Xử Lý Dữ Liệu Cá Nhân**

12.1. Thực hiện các biện pháp tổ chức và kỹ thuật cùng các biện pháp an toàn, bảo mật phù hợp để chứng minh các hoạt động xử lý dữ liệu đã được thực hiện theo quy định của pháp luật về bảo vệ dữ liệu cá nhân, rà soát và cập nhật các biện pháp này khi cần thiết.

12.2. Ghi lại và lưu trữ nhật ký hệ thống quá trình xử lý dữ liệu cá nhân.

12.3. Thông báo hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân theo quy định của pháp luật hiện hành.

12.4. Bảo đảm các quyền của chủ thể dữ liệu theo quy định của pháp luật hiện hành.

12.5. Chịu trách nhiệm trước chủ thể dữ liệu về các thiệt hại do quá trình xử lý dữ liệu cá nhân gây ra.

12.6. Phối hợp với Bộ Công an, cơ quan nhà nước có thẩm quyền trong bảo vệ dữ liệu cá nhân, cung cấp thông tin phục vụ điều tra, xử lý hành vi vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân.

12.7. Thực hiện đầy đủ các biện pháp bảo vệ dữ liệu cá nhân quy định tại các văn bản pháp luật có liên quan.

12.8. Xây dựng nội dung và tổ chức thực hiện việc tuyên truyền, phổ biến kiến thức, kỹ năng, nâng cao nhận thức bảo vệ dữ liệu cá nhân cho cá nhân người lao động trong Công ty.

12.9. Thực hiện hoạt động báo cáo định kỳ cho cơ quan nhà nước có thẩm quyền về việc thực hiện bảo vệ và xử lý dữ liệu cá nhân.

**Điều 13: Các biện pháp và điều kiện bảo đảm hoạt động Bảo Vệ Dữ Liệu Cá Nhân**

13.1. Biện pháp bảo vệ dữ liệu cá nhân được áp dụng ngay từ khi bắt đầu và trong suốt quá trình xử lý dữ liệu cá nhân.

13.2. Các biện pháp bảo vệ dữ liệu cá nhân, bao gồm:

13.2.1. Biện pháp quản lý (xây dựng, ban hành các quy định) do Công ty tổ chức thực hiện.

13.2.2. Chỉ định bộ phận có chức năng bảo vệ dữ liệu cá nhân, chỉ định nhân sự phụ trách bảo vệ dữ liệu cá nhân và trao đổi thông tin về bộ phận và cá nhân phụ trách bảo vệ dữ liệu cá nhân với Cơ quan chuyên trách bảo vệ dữ liệu cá nhân.

13.2.3. Thực hiện các biện pháp tổ chức và kỹ thuật cùng các biện pháp an toàn, bảo mật phù hợp để chứng minh các hoạt động xử lý dữ liệu đã được thực hiện theo quy định của pháp luật về bảo vệ dữ liệu cá nhân, rà soát và cập nhật các biện pháp này khi cần thiết.

13.2.4. Kiểm tra an ninh mạng đối với hệ thống và phương tiện, thiết bị phục vụ xử lý dữ liệu cá nhân trước khi xử lý, xóa không thể khôi phục được hoặc hủy các thiết bị chứa dữ liệu cá nhân.

13.2.5. Thực hiện các biện pháp bảo vệ dữ liệu cá nhân phù hợp với lĩnh vực, ngành nghề của Công ty.

13.2.6. Thông báo cho chủ thể dữ liệu biết việc dữ liệu cá nhân nhảy cảm của chủ thể dữ liệu được xử lý (nếu có xử lý dữ liệu cá nhân nhạy cảm), trừ trường hợp pháp luật có quy định khác.

13.2.7. Xây dựng nội dung và tổ chức thực hiện việc tuyên truyền, phổ biến kiến thức, kỹ năng, nâng cao nhận thức bảo vệ dữ liệu cá nhân cho cá nhân người lao động trong Công ty.

13.2.8. Tuân thủ các quy định của pháp luật hiện hành về Bảo vệ và Xử lý dữ liệu cá nhân.

**Điều 14: Thông báo xử lý dữ liệu cá nhân**

14.1. Việc thông báo được thực hiện một lần trước khi tiến hành đối với hoạt động xử lý dữ liệu cá nhân.

14.2. Nội dung thông báo cho chủ thể dữ liệu về xử lý dữ liệu cá nhân: Mục đích xử lý; Loại dữ liệu cá nhân được sử dụng có liên quan tới mục đích xử lý; Cách thức xử lý; Thông tin về các tổ chức, cá nhân khác có liên quan tới mục đích xử lý; Hậu quả, thiệt hại không mong muốn có khả năng xảy ra; Thời gian bắt đầu, thời gian kết thúc xử lý dữ liệu.

14.3. Việc thông báo cho chủ thể dữ liệu phải được thể hiện ở một định dạng có thể được in, sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được.

14.4. Bên Kiểm soát và xử lý dữ liệu cá nhân không cần thực hiện quy định tại khoản 14.1 Điều này trong các trường hợp sau: Chủ thể dữ liệu đã biết rõ và đồng ý toàn bộ với nội dung quy định tại khoản 14.1 và khoản 14.2 Điều này trước khi đồng ý cho Bên Kiểm soát và xử lý dữ liệu cá nhân tiến hành thu thập dữ liệu cá nhân, phù hợp với các quy định của pháp luật hiện hành; Dữ liệu cá nhân được xử lý bởi cơ quan nhà nước có thẩm quyền với mục đích phục vụ hoạt động của cơ quan nhà nước theo quy định của pháp luật.

**Điều 15: Quyền của Chủ Thể Dữ Liệu**

15.1. Quyền được biết: Chủ thể dữ liệu được biết về hoạt động xử lý dữ liệu cá nhân của mình, trừ trường hợp luật có quy định khác.

15.2. Quyền đồng ý: Chủ thể dữ liệu được đồng ý hoặc không đồng ý cho phép xử lý dữ liệu cá nhân của mình, trừ trường hợp được xử lý dữ liệu cá nhân mà không cần sự đồng ý của chủ thể dữ liệu theo quy định của pháp luật.

15.3. Quyền truy cập: Chủ thể dữ liệu được truy cập để xem, chỉnh sửa hoặc yêu cầu chỉnh sửa dữ liệu cá nhân của mình, trừ trường hợp luật có quy định khác.

15.4. Quyền rút lại sự đồng ý: Chủ thể dữ liệu được quyền rút lại sự đồng ý của mình, trừ trường hợp luật có quy định khác.

15.5. Quyền xóa dữ liệu: Chủ thể dữ liệu được xóa hoặc yêu cầu xóa dữ liệu cá nhân của mình, trừ trường hợp luật có quy định khác.

15.6. Quyền hạn chế xử lý dữ liệu: Chủ thể dữ liệu được yêu cầu hạn chế xử lý dữ liệu cá nhân của mình, trừ trường hợp luật có quy định khác; Việc hạn chế xử lý dữ liệu được thực hiện trong 72 giờ sau khi có yêu cầu của chủ thể dữ liệu, với toàn bộ

dữ liệu cá nhân mà chủ thể dữ liệu yêu cầu hạn chế, trừ trường hợp luật có quy định khác.

15.7. Quyền cung cấp dữ liệu: Chủ thể dữ liệu được yêu cầu Bên Kiểm soát và xử lý dữ liệu cá nhân cung cấp cho bản thân dữ liệu cá nhân của mình, trừ trường hợp luật có quy định khác.

15.8. Quyền phản đối xử lý dữ liệu: Chủ thể dữ liệu được phản đối Bên Kiểm soát và xử lý dữ liệu cá nhân xử lý dữ liệu cá nhân của mình nhằm ngăn chặn hoặc hạn chế tiết lộ dữ liệu cá nhân hoặc sử dụng cho mục đích quảng cáo, tiếp thị, trừ trường hợp luật có quy định khác; Bên Kiểm soát và xử lý dữ liệu cá nhân thực hiện yêu cầu của chủ thể dữ liệu trong 72 giờ sau khi nhận được yêu cầu, trừ trường hợp luật có quy định khác.

15.9. Quyền khiếu nại, tố cáo, khởi kiện: Chủ thể dữ liệu có quyền khiếu nại, tố cáo hoặc khởi kiện theo quy định của pháp luật.

15.10. Quyền yêu cầu bồi thường thiệt hại: Chủ thể dữ liệu có quyền yêu cầu bồi thường thiệt hại theo quy định của pháp luật khi xảy ra vi phạm quy định về bảo vệ dữ liệu cá nhân của mình, trừ trường hợp các bên có thỏa thuận khác hoặc luật có quy định khác.

15.11. Quyền tự bảo vệ: Chủ thể dữ liệu có quyền tự bảo vệ theo quy định của Bộ luật Dân sự, luật khác có liên quan và Nghị định này, hoặc yêu cầu cơ quan, tổ chức có thẩm quyền thực hiện các phương thức bảo vệ quyền dân sự theo quy định tại Điều 11 Bộ luật Dân sự.

**Điều 16: Nghĩa vụ của chủ thể dữ liệu**

16.1. Tự bảo vệ dữ liệu cá nhân của mình; yêu cầu các tổ chức, cá nhân khác có liên quan bảo vệ dữ liệu cá nhân của mình.

16.2. Tôn trọng, bảo vệ dữ liệu cá nhân của người khác.

16.3. Cung cấp đầy đủ, chính xác dữ liệu cá nhân khi đồng ý cho phép xử lý dữ liệu cá nhân.

16.4. Tham gia tuyên truyền, phổ biến kỹ năng bảo vệ dữ liệu cá nhân.

16.5. Thực hiện quy định của pháp luật về bảo vệ dữ liệu cá nhân và tham gia phòng, chống các hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân.

16.6. Thông báo ngay cho CÔNG TY TNHH AIRCLOSET ENGINEERING nếu phát hiện hoặc nghi ngờ Dữ liệu cá nhân của mình hoặc của người khác bị lộ, có nguy cơ bị lộ, có thể dẫn tới rủi ro trong quá trình làm việc/giao dịch/hợp tác...với CÔNG TY TNHH AIRCLOSET ENGINEERING, hoặc bất kỳ vi phạm nào về Bảo vệ và Xử lý dữ liệu cá nhân theo Chính sách này hoặc theo quy định của pháp luật mà Chủ thể Dữ liệu cá nhân có thể biết được/nhận thấy được.

16.7. Các nghĩa vụ khác theo từng trường hợp thỏa thuận, hợp đồng, giao dịch...cụ thể tại từng thời điểm và các nghĩa vụ theo quy định của pháp luật.

**Điều 17: Sự đồng ý của chủ thể dữ liệu**

17.1. Sự đồng ý của chủ thể dữ liệu được áp dụng đối với tất cả các hoạt động trong quy trình xử lý dữ liệu cá nhân, trừ trường hợp luật có quy định khác.

17.2. Sự đồng ý của chủ thể dữ liệu chỉ có hiệu lực khi chủ thể dữ liệu tự nguyện và biết rõ các nội dung sau: Loại dữ liệu cá nhân được xử lý; Mục đích xử lý dữ liệu cá nhân; Tổ chức, cá nhân được xử lý dữ liệu cá nhân; Các quyền, nghĩa vụ của chủ thể dữ liệu.

17.3. Sự đồng ý của chủ thể dữ liệu phải được thể hiện rõ ràng, cụ thể bằng văn bản, giọng nói, đánh dấu vào ô đồng ý, cú pháp đồng ý qua tin nhắn, chọn các thiết lập kỹ thuật đồng ý hoặc qua một hành động khác thể hiện được điều này.

17.4. Sự đồng ý phải được tiến hành cho cùng một mục đích. Khi có nhiều mục đích, Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân liệt kê các mục đích để chủ thể dữ liệu đồng ý với một hoặc nhiều mục đích nêu ra.

17.5. Sự đồng ý của chủ thể dữ liệu phải được thể hiện ở một định dạng có thể được in, sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được.

17.6. Sự im lặng hoặc không phản hồi của chủ thể dữ liệu không được coi là sự đồng ý.

17.7. Chủ thể dữ liệu có thể đồng ý một phần hoặc với điều kiện kèm theo.

17.8. Đối với xử lý dữ liệu cá nhân nhạy cảm, chủ thể dữ liệu phải được thông báo rằng dữ liệu cần xử lý là dữ liệu cá nhân nhạy cảm.

17.9. Sự đồng ý của chủ thể dữ liệu có hiệu lực cho tới khi chủ thể dữ liệu có quyết định khác hoặc khi cơ quan nhà nước có thẩm quyền yêu cầu bằng văn bản.

17.10. Trong trường hợp có tranh chấp, trách nhiệm chứng minh sự đồng ý của chủ thể dữ liệu thuộc về Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân.

17.11. Thông qua việc ủy quyền theo quy định của Bộ luật Dân sự, tổ chức, cá nhân có thể thay mặt chủ thể dữ liệu thực hiện các thủ tục liên quan tới xử lý dữ liệu cá nhân của chủ thể dữ liệu với Bên Kiểm soát và xử lý dữ liệu cá nhân trong trường hợp chủ thể dữ liệu đã biết rõ và đồng ý theo quy định tại khoản 17.3 Điều này, trừ trường hợp luật có quy định khác.

**Điều 18: Xử lý dữ liệu cá nhân trong trường hợp không cần sự đồng ý của chủ thể dữ liệu**

18.1. Trong trường hợp khẩn cấp, cần xử lý ngay dữ liệu cá nhân có liên quan để bảo vệ tính mạng, sức khỏe của chủ thể dữ liệu hoặc người khác. Bên Kiểm soát và xử lý dữ liệu cá nhân có trách nhiệm chứng minh trường hợp này.

18.2. Việc công khai dữ liệu cá nhân theo quy định của luật.

18.3. Việc xử lý dữ liệu của cơ quan nhà nước có thẩm quyền trong trường hợp tình trạng khẩn cấp về quốc phòng, an ninh quốc gia, trật tự an toàn xã hội, thảm họa lớn, dịch bệnh nguy hiểm; khi có nguy cơ đe dọa an ninh, quốc phòng nhưng chưa đến mức ban bố tình trạng khẩn cấp; phòng, chống bạo loạn, khủng bố, phòng, chống tội phạm và vi phạm pháp luật theo quy định của luật.

18.4. Để thực hiện nghĩa vụ theo hợp đồng của chủ thể dữ liệu với cơ quan, tổ chức, cá nhân có liên quan theo quy định của luật.

18.5. Phục vụ hoạt động của cơ quan nhà nước đã được quy định theo luật chuyên ngành.

**Điều 19: Chủ thể dữ liệu rút lại sự đồng ý**

19.1. Việc rút lại sự đồng ý không ảnh hưởng đến tính hợp pháp của việc xử lý dữ liệu đã được đồng ý trước khi rút lại sự đồng ý.

19.2. Việc rút lại sự đồng ý phải được thể hiện ở một định dạng có thể được in, sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được.

19.3. Khi nhận yêu cầu rút lại sự đồng ý của chủ thể dữ liệu, Bên Kiểm soát và xử lý dữ liệu cá nhân thông báo cho chủ thể dữ liệu về hậu quả, thiệt hại có thể xảy ra khi rút lại sự đồng ý.

19.4. Sau khi thực hiện quy định tại khoản 19.2 Điều này, Bên Kiểm soát và xử lý dữ liệu phải ngừng và yêu cầu các tổ chức, cá nhân có liên quan (nếu có) ngừng xử lý dữ liệu của chủ thể dữ liệu đã rút lại sự đồng ý.

**Điều 20: Lưu trữ và cung cấp dữ liệu cá nhân**

20.1. Lưu trữ dữ liệu cá nhân: Dữ liệu cá nhân sẽ được Bên nhận dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân lưu trữ và áp dụng các biện pháp thích hợp để bảo mật. Trong phạm vi pháp luật cho phép, Bên nhận dữ liệu cá nhân có thể lưu trữ Dữ liệu cá nhân tại Việt Nam hoặc tại nước ngoài, kể cả giải pháp lưu trữ trên điện toán đám mây. Việc lưu trữ Dữ liệu cá nhân được thực hiện trong khoảng thời gian cần thiết để hoàn thành các mục đích như thỏa thuận với Chủ thể dữ liệu cá nhân tại các bản cam kết, các hợp đồng, thỏa thuận, văn kiện khác được xác lập với Chủ thể dữ liệu cá nhân và/hoặc Bên Cung cấp dữ liệu cá nhân, trừ trường hợp được hoặc phải lưu trữ lâu hơn theo yêu cầu của quy định pháp luật từng thời kỳ.

20.2 Chủ thể dữ liệu được yêu cầu Bên Kiểm soát và xử lý dữ liệu cá nhân cung cấp cho bản thân mình dữ liệu cá nhân của mình.
20.3. Hình thức yêu cầu cung cấp dữ liệu cá nhân như sau:
20.3.1 Chủ thể dữ liệu trực tiếp hoặc ủy quyền cho người khác (sau đây gọi là bên yêu cầu) đến trụ sở Bên Kiểm soát và xử lý dữ liệu cá nhân yêu cầu cung cấp dữ liệu cá nhân.

Người tiếp nhận yêu cầu có trách nhiệm hướng dẫn bên yêu cầu điền các nội dung vào Phiếu yêu cầu cung cấp dữ liệu cá nhân hoặc kiểm tra tính chính xác, đầy đủ của phiếu yêu cầu do bên yêu cầu đã điền trước và mang tới.

Trường hợp bên yêu cầu không biết chữ hoặc bị khuyết tật không thể viết yêu cầu thì người tiếp nhận có trách nhiệm giúp điền các nội dung vào Phiếu yêu cầu cung cấp dữ liệu cá nhân;

20.3.2 Gửi Phiếu yêu cầu cung cấp dữ liệu cá nhân qua mạng điện tử, dịch vụ bưu chính, fax đến Bên Kiểm soát và xử lý dữ liệu cá nhân.

20.3.3. Mẫu phiếu yêu cầu cung cấp dữ liệu cá nhân phải thể hiện bằng tiếng Việt và gồm những nội dung chính sau đây: a) Họ, tên; nơi cư trú, địa chỉ; số chứng minh nhân dân, thẻ căn cước công dân hoặc số hộ chiếu của người yêu cầu. Trường hợp ủy quyền cho cá nhân, tổ chức khác thì phải kèm theo giấy ủy quyền hợp pháp theo quy định của pháp luật và phần thông tin bên yêu cầu sẽ điền thông tin của người được ủy quyền; số fax, điện thoại, địa chỉ thư điện tử (nếu có); b) Dữ liệu cá nhân

được yêu cầu cung cấp, trong đó chỉ rõ tên văn bản, hồ sơ, tài liệu; c) Hình thức cung cấp dữ liệu cá nhân; d) Lý do, mục đích yêu cầu cung cấp dữ liệu cá nhân. Có mẫu phiếu đính kèm với Chính sách này.

20.4. Bên Kiểm soát và xử lý dữ liệu cá nhân:

20.4.1. Được cung cấp dữ liệu cá nhân của chủ thể dữ liệu cho tổ chức, cá nhân khác khi có sự đồng ý của chủ thể dữ liệu, trừ trường hợp pháp luật có quy định khác.

20.4.2. Thay mặt chủ thể dữ liệu cung cấp dữ liệu cá nhân của chủ thể dữ liệu cho tổ chức hoặc cá nhân khác khi chủ thể dữ liệu đồng ý cho phép đại diện và ủy quyền, trừ trường hợp pháp luật có quy định khác.

20.4.3. Cung cấp dữ liệu cá nhân trong 72 giờ sau khi có yêu cầu hợp lệ của chủ thể dữ liệu, trừ trường hợp luật có quy định khác.

20.4.4. Bên Kiểm soát và xử lý dữ liệu cá nhân không cung cấp dữ liệu cá nhân trong trường hợp sau: a) Gây tổn hại tới quốc phòng, an ninh quốc gia, trật tự an toàn xã hội; b) Việc cung cấp dữ liệu cá nhân có thể ảnh hưởng tới sự an toàn, sức khỏe thể chất hoặc tinh thần của người khác; c) Chủ thể dữ liệu không đồng ý cung cấp, cho phép đại diện hoặc ủy quyền nhận dữ liệu cá nhân.

20.5. Trường hợp yêu cầu cung cấp dữ liệu cá nhân quy định tại khoản 20.3.1 và 20.3.2 Điều này thì phải kèm theo văn bản đồng ý của cá nhân, tổ chức liên quan.

**Điều 21: Tiếp nhận và giải quyết yêu cầu cung cấp dữ liệu cá nhân**

21.1. Bên Kiểm soát và xử lý dữ liệu cá nhân có trách nhiệm tiếp nhận yêu cầu cung cấp dữ liệu cá nhân và theo dõi quá trình, danh sách cung cấp dữ liệu cá nhân theo yêu cầu; Trường hợp dữ liệu cá nhân được yêu cầu không thuộc thẩm quyền thì Bên Kiểm soát và xử lý dữ liệu cá nhân phải thông báo và hướng dẫn bên yêu cầu đến cơ quan có thẩm quyền hoặc thông báo rõ ràng việc không thể cung cấp dữ liệu cá nhân.

21.2. Khi nhận được yêu cầu cung cấp dữ liệu cá nhân hợp lệ, Bên Kiểm soát và xử lý dữ liệu cá nhân có trách nhiệm cung cấp dữ liệu cá nhân thông báo về thời hạn, địa điểm, hình thức cung cấp dữ liệu cá nhân; chi phí thực tế để in, sao, chụp, gửi thông tin qua dịch vụ bưu chính, fax (nếu có) và phương thức, thời hạn thanh toán; thực hiện việc cung cấp dữ liệu cá nhân theo trình tự, thủ tục quy định tại Điều này.

**Điều 22: Chỉnh sửa dữ liệu cá nhân**

22.1. Chủ thể dữ liệu cá nhân: Được truy cập để xem, chỉnh sửa dữ liệu cá nhân của mình sau khi đã được Bên Kiểm soát và xử lý dữ liệu cá nhân thu thập theo sự đồng ý, trừ trường hợp luật có quy định khác; Trường hợp không thể chỉnh sửa trực tiếp vì lý do kỹ thuật hoặc vì lý do khác, chủ thể dữ liệu yêu cầu Bên Kiểm soát và xử lý dữ liệu cá nhân chỉnh sửa dữ liệu cá nhân của mình.

22.2. Bên Kiểm soát và xử lý dữ liệu cá nhân chỉnh sửa dữ liệu cá nhân của chủ thể dữ liệu sau khi được chủ thể dữ liệu cá nhân đồng ý ngay khi có thể hoặc theo quy định của pháp luật chuyên ngành. Trường hợp không thể thực hiện thì thông báo tới chủ thể dữ liệu sau 72 giờ kể khi nhận được yêu cầu chỉnh sửa dữ liệu cá nhân của chủ thể dữ liệu.

**Điều 23: Xóa, hủy dữ liệu cá nhân**

23.1. Chủ thể dữ liệu được yêu cầu Bên Kiểm soát và xử lý dữ liệu cá nhân xóa dữ liệu cá nhân của mình trong các trường hợp sau: a) Nhận thấy không còn cần thiết cho mục đích thu thập đã đồng ý và chấp nhận các thiệt hại có thể xảy ra khi yêu cầu xóa dữ liệu; b) Rút lại sự đồng ý; c) Phản đối việc xử lý dữ liệu và Bên Kiểm soát và xử lý dữ liệu cá nhân không có lý do chính đáng để tiếp tục xử lý; d) Dữ liệu cá nhân được xử lý không đúng với mục đích đã đồng ý hoặc việc xử lý dữ liệu cá nhân là vi phạm quy định của pháp luật; đ) Dữ liệu cá nhân phải xóa theo quy định của pháp luật.

23.2. Việc xóa dữ liệu sẽ không áp dụng khi có đề nghị của chủ thể dữ liệu trong các trường hợp: a) Pháp luật quy định không cho phép xóa dữ liệu; b) Dữ liệu cá nhân được xử lý bởi cơ quan nhà nước có thẩm quyền với mục đích phục vụ hoạt động của cơ quan nhà nước theo quy định của pháp luật; c) Dữ liệu cá nhân đã được công khai theo quy định của pháp luật; d) Dữ liệu cá nhân được xử lý nhằm phục vụ yêu cầu pháp lý, nghiên cứu khoa học, thống kê theo quy định của pháp luật; đ) Trong trường hợp tình trạng khẩn cấp về quốc phòng, an ninh quốc gia, trật tự an toàn xã hội, thảm họa lớn, dịch bệnh nguy hiểm; khi có nguy cơ đe dọa an ninh, quốc phòng nhưng chưa đến mức ban bố tình trạng khẩn cấp; phòng, chống bạo loạn, khủng bố, phòng, chống tội phạm và vi phạm pháp luật; e) Ứng phó với tình huống khẩn cấp đe dọa đến tính mạng, sức khỏe hoặc sự an toàn của chủ thể dữ liệu hoặc cá nhân khác.

23.3. Trường hợp doanh nghiệp chia, tách, sáp nhập, hợp nhất, giải thể thì dữ liệu cá nhân được chuyển giao theo quy định của pháp luật.

23.4. Việc xóa dữ liệu được thực hiện trong 72 giờ sau khi có yêu cầu của chủ thể dữ liệu với toàn bộ dữ liệu cá nhân mà Bên Kiểm soát và xử lý dữ liệu cá nhân thu thập được, trừ trường hợp pháp luật có quy định khác.

23.5. Bên Kiểm soát và xử lý dữ liệu cá nhân xóa không thể khôi phục trong trường hợp: a) Xử lý dữ liệu không đúng mục đích hoặc đã hoàn thành mục đích xử lý dữ liệu cá nhân được chủ thể dữ liệu đồng ý; b) Việc lưu trữ dữ liệu cá nhân không còn cần thiết với hoạt động của Bên Kiểm soát và xử lý dữ liệu cá nhân; c) Bên Kiểm soát và xử lý dữ liệu cá nhân bị giải thể hoặc không còn hoạt động hoặc tuyên bố phá sản hoặc bị chấm dứt hoạt động kinh doanh theo quy định của pháp luật.

**Điều 24: Thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân**

24.1. Trường hợp phát hiện xảy ra vi phạm quy định bảo vệ dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân thông báo cho Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) chậm nhất 72 giờ sau khi xảy ra hành vi vi phạm (mẫu báo cáo tuân theo mẫu số 03 tại Phụ lục của Nghị định 13/2023/NĐ- CP ngày 17/4/2023). Trường hợp thông báo sau 72 giờ thì phải kèm theo lý do thông báo chậm, muộn.

24.2. Bên Xử lý dữ liệu cá nhân (nếu thuê ngoài) phải thông báo cho Bên Kiểm soát dữ liệu cá nhân một cách nhanh nhất có thể sau khi nhận thấy có sự vi phạm quy định về bảo vệ dữ liệu cá nhân.

24.3. Nội dung thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân: a) Mô tả tính chất của việc vi phạm quy định bảo vệ dữ liệu cá nhân, bao gồm: thời gian, địa điểm, hành vi, tổ chức, cá nhân, các loại dữ liệu cá nhân và số lượng dữ liệu liên quan; b) Chi tiết liên lạc của nhân viên được giao nhiệm vụ bảo vệ dữ liệu hoặc tổ chức, cá nhân chịu trách nhiệm bảo vệ dữ liệu cá nhân; c) Mô tả các hậu quả, thiệt hại có thể xảy ra của việc vi phạm quy định bảo vệ dữ liệu cá nhân; d) Mô tả các biện pháp được đưa ra để giải quyết, giảm thiểu tác hại của hành vi vi phạm quy định bảo vệ dữ liệu cá nhân.

24.4. Trường hợp không thể thông báo đầy đủ các nội dung quy định tại khoản 24.3 Điều này, việc thông báo có thể được thực hiện theo từng đợt, từng giai đoạn.

24.5. Bên Kiểm soát và xử lý dữ liệu cá nhân phải lập Biên bản xác nhận về việc xảy ra hành vi vi phạm quy định bảo vệ dữ liệu cá nhân, phối hợp với Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) xử lý hành vi vi phạm.

24.6. Tổ chức, cá nhân thông báo cho Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) khi phát hiện các trường hợp sau: a) Phát hiện hành vi vi phạm pháp luật đối với dữ liệu cá nhân; b) Dữ liệu cá nhân bị xử lý sai mục đích, không đúng thỏa thuận ban đầu giữa chủ thể dữ liệu và Bên Kiểm soát và xử lý dữ liệu cá nhân hoặc vi phạm quy định của pháp luật; c) Không bảo đảm quyền của chủ thể dữ liệu hoặc không được thực hiện đúng; d) Trường hợp khác theo quy định của pháp luật.

## PHẦN IV: QUẢN LÝ SỰ CỐ VÀ TÍNH LIÊN TỤC

### Điều 25: Quản lý sự cố an ninh thông tin và xử lý vi phạm

25.1. Báo cáo Sự cố

Trách nhiệm Báo cáo: Mọi nhân viên có trách nhiệm báo cáo ngay lập tức cho Bộ phận IT hoặc Ban An ninh Thông tin (hoặc người được chỉ định) khi phát hiện bất kỳ Sự cố An ninh Thông tin nào (ví dụ: máy tính bị nhiễm virus, mất laptop, nghi ngờ bị tấn công mạng, hay vi phạm Dữ liệu Cá nhân).

Ngăn chặn Sơ bộ: Trong trường hợp phát hiện mã độc hoặc xâm nhập, nhân viên phải ngắt kết nối thiết bị khỏi mạng và giữ nguyên hiện trạng thiết bị (nếu có thể) để hỗ trợ điều tra.

25.2. Quy trình Xử lý Sự cố

Nhóm Ứng phó: Công ty sẽ duy trì Nhóm Ứng phó Sự cố để điều phối hành động.

Các Giai đoạn: IRT sẽ thực hiện các bước: Phát hiện, Ngăn chặn, Điều tra, Loại bỏ, Phục hồi và Đánh giá bài học kinh nghiệm.

Thông báo: Việc thông báo cho cơ quan nhà nước và Chủ thể Dữ liệu về vi phạm Dữ liệu Cá nhân sẽ được thực hiện theo quy định của Nghị định 13/2023/NĐ-CP (trong vòng 72 giờ kể từ khi xảy ra/phát hiện vi phạm).

### Điều 26: Sao lưu và liên tục kinh doanh

26.1. Quy định Sao lưu Dữ liệu

Sao lưu Bắt buộc: Tất cả dữ liệu và hệ thống quan trọng phải được sao lưu định kỳ theo lịch trình và phương pháp được Bộ phận IT phê duyệt.

Lưu trữ An toàn: Bản sao lưu phải được lưu trữ ở vị trí riêng biệt (vật lý hoặc logic) và được bảo vệ khỏi truy cập trái phép.

Kiểm tra Phục hồi: Bộ phận IT phải thực hiện kiểm tra phục hồi định kỳ tối thiểu hai (2) lần mỗi năm để đảm bảo khả năng phục hồi dữ liệu khi cần.

26.2. Kế hoạch Phục hồi Thảm họa

Công ty sẽ duy trì Kế hoạch Phục hồi Thảm họa để đảm bảo các quy trình kinh doanh thiết yếu có thể tiếp tục hoạt động hoặc được khôi phục kịp thời sau một sự cố thảm khốc.

Kế hoạch phải xác định rõ ràng:

Thời gian Mục tiêu Phục hồi: Thời gian tối đa cho phép để khôi phục hoạt động sau sự cố.

Điểm Mục tiêu Phục hồi: Lượng dữ liệu tối đa Công ty chấp nhận mất đi.

**Điều 27: Quản lý rủi ro an ninh và an ninh bên thứ ba.**

27.1. Quản lý Rủi ro An ninh Thông tin

Đánh giá Rủi ro: Công ty sẽ thực hiện đánh giá rủi ro an ninh thông tin định kỳ (tối thiểu một (1) lần mỗi năm) để xác định, phân tích và xử lý các mối đe dọa đối với Tài sản Thông tin của Công ty.

Tiêu chí Chấp nhận Rủi ro: Rủi ro chỉ được chấp nhận nếu đã được Ban Lãnh đạo phê duyệt chính thức và đã có biện pháp giảm thiểu được áp dụng để đưa rủi ro về mức độ chấp nhận được.

27.2. Quản lý An ninh của Bên Thứ Ba

Yêu cầu Hợp đồng: Đối với các nhà cung cấp dịch vụ hoặc đối tác có quyền truy cập vào hệ thống hoặc xử lý dữ liệu của Công ty, Công ty phải yêu cầu họ ký Thỏa thuận Bảo mật và cam kết thực hiện các biện pháp an ninh thông tin tương đương hoặc cao hơn tiêu chuẩn của Công ty.

Quyền Kiểm tra: Hợp đồng với các Bên Thứ Ba nhạy cảm phải bao gồm điều khoản cho phép Công ty hoặc đại diện được chỉ định của Công ty có quyền kiểm tra, đánh giá các biện pháp an ninh của họ khi cần thiết.

Vi phạm của Bên Thứ Ba: Trường hợp xảy ra vi phạm an ninh hoặc dữ liệu cá nhân do Bên Thứ Ba gây ra, Bên Thứ Ba phải chịu trách nhiệm bồi thường và khắc phục theo các điều khoản đã ký kết.

Nghĩa vụ Tuân thủ NĐ 13: Đối với các Bên Thứ Ba ở nước ngoài xử lý Dữ liệu Cá nhân của người Việt Nam, thỏa thuận với họ phải quy định rõ ràng nghĩa vụ của họ trong việc hỗ trợ Công ty hoàn thành Hồ sơ Đánh giá Tác động Chuyển Dữ liệu Cá nhân ra nước ngoài và tuân thủ các yêu cầu liên quan khác của Nghị định 13/2023/NĐ-CP.

Thông báo Thay đổi: Bên Thứ Ba có trách nhiệm thông báo ngay lập tức cho Công ty về bất kỳ sự thay đổi nào trong môi trường pháp lý hoặc môi trường an ninh của họ có thể ảnh hưởng đến tính bảo mật của dữ liệu Công ty.

**Điều 28: Đánh giá tác động xử lý dữ liệu cá nhân**

28.1. Bên Kiểm soát và xử lý dữ liệu cá nhân lập và lưu giữ Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân của mình kể từ thời điểm bắt đầu xử lý dữ liệu cá nhân.

28.2. Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân của Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, bao gồm: a) Thông tin và chi tiết liên lạc của Bên Kiểm soát và xử lý dữ liệu cá nhân; b) Họ tên, chi tiết liên lạc của tổ chức được phân công thực hiện nhiệm vụ bảo vệ dữ liệu cá nhân và nhân viên bảo vệ dữ liệu cá nhân của Bên Kiểm soát và xử lý dữ liệu cá nhân; c) Mục đích xử lý dữ liệu cá nhân; d) Các loại dữ liệu cá nhân được xử lý; đ) Tổ chức, cá nhân nhận dữ liệu cá nhân, bao gồm tổ chức, cá nhân ngoài lãnh thổ Việt Nam; e) Trường hợp chuyển dữ liệu cá nhân ra nước ngoài; g) Thời gian xử lý dữ liệu cá nhân; thời gian dự kiến để xóa, hủy dữ liệu cá nhân (nếu có); h) Mô tả về các biện pháp bảo vệ dữ liệu cá nhân được áp dụng; i) Đánh giá mức độ ảnh hưởng của việc xử lý dữ liệu cá nhân; hậu quả, thiệt hại không mong muốn có khả năng xảy ra, các biện pháp giảm thiểu hoặc loại bỏ nguy cơ, tác hại đó.

28.3. Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân quy định tại khoản 20.1 và khoản 28.2 Điều này được xác lập bằng văn bản có giá trị pháp lý của Bên Kiểm soát và xử lý dữ liệu cá nhân.

28.4. Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân phải luôn có sẵn để phục vụ hoạt động kiểm tra, đánh giá của Bộ Công an và gửi Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) 01 bản chính theo Mẫu số 04 tại Phụ lục của Nghị định 13/2023/NĐ-CP ngày 17/4/2023 trong thời gian 60 ngày kể từ ngày tiến hành xử lý dữ liệu cá nhân.

28.5. Bên Kiểm soát và xử lý dữ liệu cá nhân hoàn thiện Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân trong trường hợp hồ sơ chưa đầy đủ và đúng quy định.

28.6. Bên Kiểm soát và xử lý dữ liệu cá nhân cập nhật, bổ sung Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân khi có sự thay đổi về nội dung hồ sơ đã gửi cho Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) theo Mẫu số 05 tại Phụ lục của Nghị định 13/2023/NĐ-CP ngày 17/4/2023.

**Điều 29: Chuyển dữ liệu cá nhân ra nước ngoài**

29.1. Dữ liệu cá nhân của công dân Việt Nam được chuyển ra nước ngoài trong trường hợp Bên chuyển dữ liệu ra nước ngoài lập Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài và thực hiện các thủ tục theo quy định tại khoản 29.3, 29.4 và 29.5 Điều này.

29.2. Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài, gồm: a) Thông tin và chi tiết liên lạc của Bên chuyển dữ liệu và Bên tiếp nhận dữ liệu cá nhân của công dân Việt Nam; b) Họ tên, chi tiết liên lạc của tổ chức, cá nhân phụ trách của Bên chuyển dữ liệu có liên quan tới việc chuyển và tiếp nhận dữ liệu cá nhân của công dân Việt Nam; c) Mô tả và luận giải mục tiêu của các hoạt động xử lý dữ liệu cá nhân của Công dân Việt Nam sau khi được chuyển ra nước ngoài; d) Mô tả và làm rõ loại dữ liệu cá nhân chuyển ra nước ngoài; đ) Mô tả và nêu rõ sự tuân thủ quy định bảo vệ dữ liệu cá nhân tại Nghị định 13/2023/NĐ-CP ngày 17/4/2023, chi tiết các biện pháp bảo vệ dữ liệu cá nhân được áp dụng; e) Đánh giá mức độ ảnh hưởng của việc xử lý dữ liệu cá nhân; hậu quả, thiệt hại không mong muốn có khả năng xảy ra, các biện pháp giảm thiểu hoặc loại bỏ nguy cơ, tác hại đó; g) Sự đồng ý của chủ thể dữ liệu theo quy định tại Điều 11 Nghị định 13/2023/NĐ-CP ngày 17/4/2023 trên cơ sở biết rõ cơ chế phản hồi, khiếu nại khi có sự cố hoặc yêu cầu phát sinh; h) Có văn bản thể hiện sự ràng buộc, trách nhiệm giữa các tổ chức, cá nhân chuyển và nhận dữ liệu cá nhân của Công dân Việt Nam về việc xử lý dữ liệu cá nhân.

29.3. Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài phải luôn có sẵn để phục vụ hoạt động kiểm tra, đánh giá của Bộ Công an. Bên chuyển dữ liệu ra nước ngoài gửi 01 bản chính hồ sơ tới Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) theo Mẫu số 06 tại Phụ lục của Nghị định 13/2023/NĐ-CP ngày 17/4/2023 trong thời gian 60 ngày kể từ ngày tiến hành xử lý dữ liệu cá nhân.

29.4. Bên chuyển dữ liệu thông báo gửi Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) thông tin về việc chuyển dữ liệu và chi tiết

liên lạc của tổ chức, cá nhân phụ trách bằng văn bản sau khi việc chuyển dữ liệu diễn ra thành công.

29.5. Trong trường hợp hồ sơ chưa đầy đủ và đúng quy định và được cơ quan có thẩm quyền yêu cầu, Bên chuyển dữ liệu cá nhân ra nước ngoài có trách nhiệm hoàn thiện lại hồ sơ và nộp lại cho Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) theo quy định.

29.6. Bên chuyển dữ liệu ra nước ngoài cập nhật, bổ sung Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài khi có sự thay đổi về nội dung hồ sơ đã gửi cho Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) theo Mẫu số 05 tại Phụ lục của Nghị định 13/2023/NĐ-CP ngày 17/4/2023. Thời gian hoàn thiện hồ sơ dành cho Bên chuyển dữ liệu ra nước ngoài là 10 ngày kể từ ngày yêu cầu.

29.7. Bộ Công an là cơ quan quyết định việc kiểm tra chuyển dữ liệu cá nhân ra nước ngoài 01 lần/năm, trừ trường hợp phát hiện hành vi vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân tại Nghị định 13/2023/NĐ-CP ngày 17/4/2023 hoặc để xảy ra sự cố lộ, mất dữ liệu cá nhân của công dân Việt Nam.

29.8. Trường hợp có yêu cầu/quyết định của Bộ Công an, Bên chuyển dữ liệu cá nhân ra nước ngoài phải ngừng chuyển dữ liệu cá nhân ra nước ngoài trong trường hợp sau: a) Khi phát hiện dữ liệu cá nhân được chuyển được sử dụng vào hoạt động vi phạm lợi ích, an ninh quốc gia của nước Cộng hòa xã hội chủ nghĩa Việt Nam; b) Bên chuyển dữ liệu ra nước ngoài không chấp hành quy định tại khoản 29.5, khoản 29.6 Điều này; c) Để xảy ra sự cố lộ, mất dữ liệu cá nhân của công dân Việt Nam.

**Điều 30: Cơ chế thực hiện quyền phản hồi, khiếu nại của Chủ thể dữ liệu**

30.1. Chủ thể dữ liệu nếu có bất kỳ phản hồi nào hoặc khiếu nại nào liên quan đến quyền, nghĩa vụ của mình về bảo vệ và xử lý dữ liệu cá nhân như quy định tại Chính sách này, Chủ thể dữ liệu cần liên hệ/phản hồi ngay cho CÔNG TY TNHH AIRCLOSET ENGINEERING qua email aircloset-engineering-admin@air-closet.com, hoặc liên hệ trực tiếp tại văn phòng công ty tại địa chỉ: Tầng 4, Tòa nhà 3D, số 3 phố Duy Tân, phường Dịch Vọng Hậu, quận Cầu Giấy, thành phố Hà Nội, Việt Nam.

30.2. Trường hợp chủ thể khiếu nại cần có đơn khiếu nại theo đúng quy định của pháp luật và gửi tới CÔNG TY TNHH AIRCLOSET ENGINEERING trong thời

hiệu khiếu nại. Đơn khiếu nại phải nêu rõ họ và tên người khiếu nại, thông tin loại, số, ngày cấp giấy tờ chứng thực cá nhân, địa chỉ thường trú, nơi ở hiện tại, điện thoại/email liên lạc, bên bị khiếu khại, nội dung việc khiếu nại, tài liệu, chứng cứ kèm theo (nếu có).

**Điều 31: Hiệu lực thi hành**

31.1. Chính sách này có hiệu lực thi hành từ ngày 25 tháng 07 năm 2024, sửa đổi lần 1 ngày 10/10/2025.

31.2. Mọi sửa đổi/bổ sung/thay thế Chính sách này sẽ được CÔNG TY TNHH AIRCLOSET ENGINEERING ban hành bằng văn bản và cập nhật công khai.