TẬP ĐOÀN HÒA PHÁT

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập – Tự do – Hạnh phúc

CHÍNH SÁCH BẢO MẬT THÔNG TIN

(Áp dụng cho Cổng dịch vụ thông tin nội bộ)

1. Mục đích

Đảm bảo an toàn, bảo mật thông tin trong toàn bộ hệ thống Cổng dịch vụ thông tin nội bộ, đồng thời ngăn ngừa rò rỉ, thất thoát hoặc truy cập trái phép vào dữ liệu, đặc biệt dữ liệu liên quan đến chuyển đổi xanh, phát thải CO_2, KPI xanh, báo cáo ESG và thông tin khách hàng/đối tác. Từ đó, đáp ứng các tiêu chuẩn quốc tế (ISO 27001, ISO 14064, ESG, CBAM) và quy định pháp luật Việt Nam về an toàn thông tin.

2. Phạm vi

Áp dụng cho toàn bộ nhân sự (nhân viên chính thức, cộng tác viên, thực tập sinh), các bộ phận phòng ban và đối tác có quyền truy cập vào Cổng dịch vụ thông tin. Bao gồm toàn bộ hệ thống CNTT, cơ sở dữ liệu nội bộ, báo cáo định kỳ, dữ liệu môi trường – năng lượng – CO_2, tài liệu đào tạo nội bộ, và các chứng chỉ xanh.

3. Trách nhiệm

3.1. Quản lý các Phòng ban/Bộ phận

- Tổ chức triển khai chính sách bảo mật thông tin trong phạm vi đơn vị mình;
- Đảm bảo nhân sự tuân thủ; phối hợp với Bộ phận An toàn Thông tin (CISO) để xử lý sự cố.

3.2. Nhân viên Bảo mật Thông tin (CISO)

- Xây dựng, duy trì, giám sát và kiểm toán bảo mật;
- Ứng phó, điều tra và khắc phục sự cố;
- Định kỳ tổ chức kiểm toán.

3.3. Người dùng

- Chỉ truy cập dữ liệu trong phạm vi công việc;
- Không chia sẻ tài khoản hoặc dữ liệu;
- Báo cáo ngay sự cố cho CISO.

4. Quy định

4.1. Thu thập và sử dụng thông tin

- Chỉ phục vụ mục tiêu quản trị, báo cáo nội bộ và tuân thủ pháp lý; không dùng cho mục đích cá nhân.

4.2. Bảo mật thông tin

- Dữ liệu phải mã hóa khi lưu trữ và truyền tải; áp dụng xác thực đa yếu tố (MFA); vô hiệu hóa tài khoản không sử dụng quá 90 ngày; sao lưu dữ liệu định kỳ.

4.3. Báo cáo sự cố và vi phạm

- Mọi sự cố phải báo ngay cho CISO; CISO phản hồi trong 24h, báo cáo xử lý trong 72h; vi phạm sẽ bị kỷ luật.

4.4. Quy định về thiết bị và truy cập

- Không cho phép thiết bị cá nhân kết nối nếu chưa được phê duyệt; chỉ truy cập qua VPN; USB phải quét virus trước khi dùng.

5. Đánh giá và cải tiến

- Chính sách được rà soát ít nhất 1 lần/năm hoặc khi có thay đổi pháp luật, tiêu chuẩn ESG/CBAM, hoặc phát sinh rủi ro mới;
- Kết quả đánh giá báo cáo Ban Giám đốc và công bố nội bộ;
- Liên tục cải tiến để nâng cao hiệu quả bảo mật.

6. Lưu trữ và ghi chép

Mọi nhật ký truy cập, thay đổi, vi phạm và sự cố bảo mật phải được ghi chép, lưu trữ ít nhất 05 năm và CISO định kỳ kiểm tra và báo cáo Ban Giám đốc.

7. Tuân thủ Luật và quy định

- Tuân thủ Luật An toàn thông tin mạng (2015), Luật An ninh mạng (2018) và các nghị định hướng dẫn.
- Tuân thủ tiêu chuẩn quốc tế: ISO 27001 (Quản lý an toàn thông tin), ISO 14064 (Phát thải khí nhà kính), CBAM (EU Carbon Border Adjustment Mechanism).
- Nhân sự vi phạm chính sách này sẽ chịu kỷ luật nội bộ và/hoặc truy cứu trách nhiệm theo quy định pháp luật.

8. Liên hệ

Mọi yêu cầu, khiếu nại hoặc thắc mắc liên quan đến bảo mật thông tin vui lòng liên hệ Bộ phận An toàn Thông tin (CISO): security@hoaphat.com.vn

TỔNG GIÁM ĐỐC

(Ký, họ tên)