Chính sách An toàn thông tin

M?c ?ích

- Xác định các nguyên tắc và quy định về an toàn bảo mật dữ liệu trong toàn bộ doanh nghiệp.
- Bảo vệ tính bảo mật, tính toàn vẹn và tính khả dụng của dữ liệu.
- Đảm bảo tuân thủ các quy định pháp luật liên quan đến bảo vệ dữ liệu.
- Xây dựng văn hóa an toàn thông tin trong toàn bộ nhân viên.
- Giảm thiểu rủi ro và thiệt hại do các sự cố an ninh mạng và vi phạm dữ liệu gây ra.

Ph?m vi áp d?ng

- Chính sách này áp dụng cho tất cả nhân viên, đối tác, nhà cung cấp và bất kỳ bên thứ ba nào có quyền truy cập vào dữ liệu của doanh nghiệp (Công ty TNHH Điện tử ASTI).
- Chính sách này áp dụng cho tất cả các loại dữ liệu mà doanh nghiệp thu thập, lưu trữ, xử lý và truyền tải, bao gồm dữ liệu khách hàng, dữ liệu nhân viên, dữ liệu tài chính, dữ liệu hoạt động và các dữ liệu quan trọng khác.
- Chính sách này áp dụng cho tất cả các hệ thống, thiết bị và phương tiện lưu trữ và xử lý dữ liệu của doanh nghiệp, bao gồm máy tính, máy chủ, thiết bị di động, mạng nội bộ, internet và các dịch vụ đám mây.

Khái ni?m

- **Dữ liệu**: Tất cả các thông tin được lưu trữ hoặc xử lý dưới dạng điện tử hoặc trên giấy.
- **Dữ liệu cá nhân**: Thông tin liên quan đến một cá nhân cụ thể hoặc có thể xác định được danh tính của một cá nhân cụ thể.
- **An toàn bảo mật dữ liệu**: Việc bảo vệ dữ liệu khỏi các hành vi truy cập, sử dụng, tiết lộ, sửa đổi, phá hoại hoặc mất mát trái phép.
- **Tính bảo mật**: Đảm bảo rằng dữ liệu chỉ được truy cập bởi những người được ủy quyền.
- **Tính toàn vẹn**: Đảm bảo rằng dữ liệu là chính xác, đầy đủ và không bị thay đổi trái phép.
- **Tính khả dụng**: Đảm bảo rằng người dùng được ủy quyền có thể truy cập dữ liệu khi cần thiết.
- **Sự cố an ninh mạng**: Bất kỳ sự kiện không mong muốn nào gây ảnh hưởng đến tính bảo mật, tính toàn vẹn hoặc tính khả dụng của dữ liệu hoặc hệ thống thông tin.
- **Vi phạm dữ liệu**: Hành vi truy cập, tiết lộ, sử dụng hoặc chiếm đoạt dữ liệu trái phép.

Tham kh?o

- TCVN ISO-IEC-27001
- Luật An toàn thông tin mạng (86/2015/QH13)
- Luật An ninh mạng (24/2018/QH14)

Nguyên t?c chung

- **Tuân thủ pháp luật**: Mọi hoạt động liên quan đến dữ liệu phải tuân thủ các quy định pháp luật hiện hành về bảo vệ dữ liệu.
- **Trách nhiệm**: Tất cả nhân viên đều có trách nhiệm tuân thủ chính sách này và báo cáo bất kỳ sự cố an ninh nào mà họ phát hiện.
- **Minh bạch**: Doanh nghiệp sẽ minh bạch về các hoạt động thu thập, sử dụng và bảo vệ dữ liệu.
- **Hạn chế truy cập**: Quyền truy cập vào dữ liệu sẽ được giới hạn dựa trên vai trò và trách nhiệm của từng cá nhân.
- **Phòng ngừa**: Doanh nghiệp sẽ áp dụng các biện pháp phòng ngừa để ngăn chặn các sự cố an ninh mạng và vi phạm dữ liệu.
- **Phản ứng**: Doanh nghiệp sẽ có quy trình rõ ràng để xử lý các sự cố an ninh mạng và vi phạm dữ liệu một cách nhanh chóng và hiệu quả.
- **Đánh giá và cải tiến**: Chính sách này sẽ được định kỳ đánh giá và cập nhật để đảm bảo tính hiệu quả và phù hợp với các thay đổi.

Các quy ??nh c? th?

1. **Quản lý truy cập:**
   - Thiết lập hệ thống quản lý tài khoản và quyền truy cập chặt chẽ.
   - Sử dụng mật khẩu mạnh và thay đổi mật khẩu định kỳ.
   - Áp dụng cơ chế xác thực đa yếu tố (MFA) khi có thể.
   - Thu hồi quyền truy cập của nhân viên khi họ nghỉ việc hoặc thay đổi vai trò.
   - Giám sát và ghi lại các hoạt động truy cập dữ liệu.
2. **Bảo vệ dữ liệu:**
   - Mã hóa dữ liệu quan trọng khi lưu trữ và truyền tải.
   - Thực hiện sao lưu dữ liệu định kỳ và kiểm tra khả năng phục hồi.
   - Triển khai các biện pháp bảo vệ vật lý cho các thiết bị lưu trữ dữ liệu.
   - Sử dụng phần mềm diệt virus và các công cụ bảo mật khác.
   - Cập nhật thường xuyên các bản vá bảo mật cho hệ thống và phần mềm.
3. **Sử dụng dữ liệu:**
   - Chỉ thu thập và xử lý dữ liệu cho các mục đích hợp pháp và đã được thông báo.
   - Hạn chế việc thu thập dữ liệu không cần thiết.
   - Đảm bảo tính chính xác và cập nhật của dữ liệu.
   - Không chia sẻ dữ liệu với các bên thứ ba không được ủy quyền.
   - Tuân thủ các quy định về thời gian lưu trữ dữ liệu.
   - Tiêu hủy dữ liệu an toàn khi không còn cần thiết.
4. **An toàn mạng:**
   - Xây dựng và duy trì hệ thống tường lửa và các biện pháp bảo vệ mạng khác.
   - Giám sát lưu lượng mạng để phát hiện các hoạt động bất thường.
   - Ngăn chặn truy cập trái phép vào mạng nội bộ.
   - Thực hiện kiểm tra an ninh mạng định kỳ.
   - Nâng cao nhận thức về an toàn thông tin cho nhân viên để phòng tránh các tấn công lừa đảo (phishing).
5. **Thiết bị cá nhân:**
   - Quy định rõ ràng về việc sử dụng thiết bị cá nhân cho mục đích công việc (BYOD).
   - Áp dụng các biện pháp bảo mật cho thiết bị cá nhân truy cập vào dữ liệu của doanh nghiệp.
   - Có biện pháp kiểm soát và xóa dữ liệu từ xa trong trường hợp thiết bị bị mất hoặc đánh cắp.
6. **Ứng phó sự cố**:
   - Xây dựng kế hoạch ứng phó sự cố an ninh mạng và vi phạm dữ liệu chi tiết.
   - Thành lập đội ngũ ứng phó sự cố và phân công trách nhiệm rõ ràng.
   - Thực hiện diễn tập ứng phó sự cố định kỳ.
   - Thiết lập quy trình thông báo và xử lý vi phạm dữ liệu theo quy định pháp luật.
7. **Đào tạo và nâng cao nhận thức:**
   - Tổ chức các buổi đào tạo về an toàn bảo mật dữ liệu cho tất cả nhân viên.
   - Cung cấp thông tin và hướng dẫn thường xuyên về các mối đe dọa an ninh mạng và các biện pháp phòng ngừa.

- Khuyến khích nhân viên báo cáo các hành vi đáng ngờ hoặc sự cố an ninh.

Trách nhi?m

- **Ban lãnh đạo:** Chịu trách nhiệm phê duyệt và giám sát việc thực hiện chính sách này.
- **Bộ phận IT/An ninh thông tin:** Chịu trách nhiệm xây dựng, triển khai, duy trì và cập nhật chính sách, cũng như quản lý các hệ thống và biện pháp bảo mật.
- **Trưởng các bộ phận:** Chịu trách nhiệm phổ biến và giám sát việc tuân thủ chính sách trong bộ phận của mình.
- **Tất cả nhân viên:** Chịu trách nhiệm tuân thủ chính sách này và các quy định liên quan.

K? lu?t

- Bất kỳ hành vi vi phạm chính sách này đều có thể dẫn đến các biện pháp kỷ luật, bao gồm cảnh cáo, khiển trách, đình chỉ công tác hoặc chấm dứt hợp đồng lao động, tùy thuộc vào mức độ nghiêm trọng của hành vi vi phạm và quy định của công ty.

Hi?u l?c và s?a ??i

- Chính sách này có hiệu lực kể từ ngày [**05/05/2025**].
- Chính sách này có thể được sửa đổi hoặc cập nhật theo quyết định của ban lãnh đạo doanh nghiệp. Mọi sửa đổi sẽ được thông báo đến toàn bộ nhân viên.