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.

Revision #2
Created 17 September 2025 09:53:44 by Hieu Nguyen
Updated 17 September 2025 10:04:31 by Hieu Nguyen