Phụ lục 4 - Chương 2: Mối đe dọa, Điểm yếu, Các mục tiêu kiểm soát và kiểm soát Rủi ro ATTT - Tài liệu tham khảo

1. Danh sách các mối đe dọa (ISO 27001)

Breach of contractual relations	Vi phạm quan hệ hợp đồng
Breach of legislation	Vi phạm pháp luật
Damage caused by a third party	Thiệt hại do bên thứ ba gây ra
Damages resulting from penetration testing	Thiệt hại do thử nghiệm xâm nhập
Destruction of records	Phá hủy hồ sơ
Eavesdropping	Nghe lén
Embezzlement	Tham ô
Employees going on strike	Nhân viên đình công
Equipment malfunction	Thiết bị trục trặc
Failure of communication links	Lỗi liên lạc
Falsification of records	Làm giả hồ sơ
Fraud from a cyber criminal	Gian lận từ tội phạm mạng
Fraud from an internal party	Gian lận từ một bên nội bộ
Improper disclosure of passwords	Tiết lộ mật khẩu không đúng cách
Improper disclosure of sensitive information	Tiết lộ thông tin nhạy cảm không đúng cách
Industrial espionage	Gián điệp công nghiệp
Interruption of business processes	Gián đoạn quy trình kinh doanh
Lack of data integrity	Thiếu tính toàn vẹn của dữ liệu
Loss of support services	Mất dịch vụ hỗ trợ
Maintenance errors	Lỗi bảo trì
Malicious code	Mã độc hại
Misuse of information systems	Sử dụng sai hệ thống thông tin
Natural or man-made disaster	Thảm họa thiên nhiên hoặc do con người gây ra
Phishing scams	Lừa đảo qua thư điện tử
Power failure	Mất điện
Sensitive data being compromised	Dữ liệu nhạy cảm bị xâm phạm
Social engineering	Kỹ thuật xã hội
Terrorism threat in the immediate vicinity or affecting nearby transport and logistics	Mối đe dọa khủng bố ở khu vực lân cận hoặc ảnh hưởng đến giao thông và hậu cần gần đó
Theft of equipment	Trộm cắp thiết bị
Theft of sensitive data	Trộm cắp dữ liệu nhạy cảm
Unauthorised access to the information system	Truy cập trái phép vào hệ thống thông tin
Unauthorised access to the network	Truy cập trái phép vào mạng
Unauthorised changes of records	Thay đổi trái phép hồ sơ
Unauthorised physical access	Truy cập vật lý trái phép
Unauthorised use of copyright material	Sử dụng trái phép tài liệu có bản quyền

2. Danh sách các điểm yếu (ISO 27001)

Employees not receiving adequate training	Nhân viên không được đào tạo đầy đủ
Equipment not being replaced when it is no longer fit for purpose	Thiết bị không được thay thế khi không còn phù hợp với mục đích sử dụng
Hard drives being disposed of without sensitive data having been deleted	Ổ cứng bị loại bỏ mà không xóa dữ liệu nhạy cảm

Improper cabling security and management	Bảo mật và quản lý cáp không đúng cách
Improper change management	Quản lý thay đổi không đúng cách
Improper internal audit	Kiểm toán nội bộ không đúng cách
Improper network management	Quản lý mạng không đúng cách
Improper validation of the processed data	Xác thực dữ liệu đã xử lý không đúng cách
Inadequate or irregular system backups	Sao lưu hệ thống không đầy đủ hoặc không thường xuyên
Inadequate physical security controls	Kiểm soát bảo mật vật lý không đầy đủ
Insufficient processes or technologies to prevent malicious files from being downloaded	Quy trình hoặc công nghệ không đủ để ngăn chặn việc tải xuống các tệp độc hại
Insufficient processes or technologies to prevent sensitive data from being copied	Quy trình hoặc công nghệ không đủ để ngăn chặn việc sao chép dữ liệu nhạy cảm
Insufficient software testing	Kiểm tra phần mềm không đủ
Insufficient processes or technologies to prevent users from downloading unapproved software	Quy trình hoặc công nghệ không đủ để ngăn chặn người dùng tải xuống phần mềm không được chấp thuận
Inadequate protection of cryptographic keys	Bảo vệ khóa mật mã không đầy đủ
Lack of systems for identification and authentication	Thiếu hệ thống nhận dạng và xác thực
No procedure for removing access rights upon termination of employment	Không có quy trình nào để xóa quyền truy cập khi chấm dứt hợp đồng lao động
No protection for mobile equipment	Không có biện pháp bảo vệ thiết bị di động
Operational and testing facilities not being properly segregated	Cơ sở vận hành và thử nghiệm không được phân tách đúng cách
Passwords not being changed from default settings	Mật khẩu không được thay đổi so với cài đặt mặc định
Passwords not being strong enough	Mật khẩu không đủ mạnh
Poor or non-existent access control policy	Chính sách kiểm soát truy cập kém hoặc không có
Poor or non-existent clean desk and clear screen policy	Chính sách bàn làm việc sạch sẽ và màn hình sạch kém hoặc không có
Poor or non-existent of internal documentation	Tài liệu nội bộ kém hoặc không có
Poor staff morale and potential for malicious action	Nhân viên kém tinh thần và khả năng hành động ác ý
Premises is vulnerable to flooding, fire or other disruptive event	Cơ sở dễ bị ngập lụt, hỏa hoạn hoặc các sự kiện phá hoại khác
Sensitive data not being properly classified	Dữ liệu nhạy cảm không được phân loại đúng cách
Staff duties not being properly segregated	Nhiệm vụ của nhân viên không được phân tách đúng cách
Staff not receiving security awareness training	Nhân viên không được đào tạo nhận thức về an ninh
User rights are not reviewed regularly	Quyền của người dùng không được xem xét thường xuyên
Unprotected public networks	Mạng công cộng không được bảo vệ
Water or heat damage to equipment	Thiết bị bị hư hỏng do nước hoặc nhiệt

./.