

QUYẾT ĐỊNH

**Về việc ban hành Tài liệu Bộ quy tắc cấu hình an toàn thông tin
cho các hệ thống thông tin trong Tập đoàn Điện lực Quốc gia Việt Nam**

TỔNG GIÁM ĐỐC TẬP ĐOÀN ĐIỆN LỰC VIỆT NAM

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số 26/2018/NĐ-CP ngày 28/02/2018 của Chính phủ về Điều lệ tổ chức và hoạt động của Tập đoàn Điện lực Việt Nam;

Căn cứ Tờ trình số 900/TTr-EVNICT ngày 19/11/2021 của Công ty Viễn thông Điện lực và Công nghệ thông tin về việc ban hành Bộ quy tắc cấu hình an toàn thông tin trong Tập đoàn Điện lực Việt Nam;

Theo đề nghị của Trưởng ban Viễn thông và Công nghệ thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Tài liệu Bộ quy tắc cấu hình an toàn thông tin cho các hệ thống thông tin trong Tập đoàn Điện lực Quốc gia Việt Nam.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký, là cơ sở để các đơn vị áp dụng, ban hành tài liệu hướng dẫn chi tiết trong nội bộ, phù hợp với thực tế tại đơn vị.

Điều 3. Các Phó Tổng giám đốc, các Ban EVN, các công ty con do EVN nắm giữ 100% vốn điều lệ (Công ty TNHH MTV cấp II), người đứng đầu các đơn vị trực thuộc EVN, Công ty con do Công ty TNHH MTV cấp II nắm giữ 100% vốn điều lệ (Công ty TNHH MTV cấp III), người đại diện phần vốn của EVN và người đại diện phần vốn của Công ty TNHH MTV cấp II tại các công ty cổ phần, công ty trách nhiệm hữu hạn chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3;
- HĐTV (để b/c);
- TGD (để b/c);
- Lưu: VT, VTCNTT.

**KT. TỔNG GIÁM ĐỐC
PHÓ TỔNG GIÁM ĐỐC**

Võ Quang Lâm

TẬP ĐOÀN ĐIỆN LỰC VIỆT NAM



BỘ QUY TẮC CẤU HÌNH AN TOÀN THÔNG TIN CHO CÁC HỆ THỐNG THÔNG TIN TRONG TẬP ĐOÀN ĐIỆN LỰC QUỐC GIA VIỆT NAM

Hà Nội, tháng 8/2022

MỤC LỤC

CHƯƠNG I. QUY ĐỊNH CHUNG.....	5
<i>Điều 1. Mục đích</i>	5
<i>Điều 2. Đối tượng áp dụng.....</i>	5
<i>Điều 3. Thuật ngữ và từ ngữ viết tắt</i>	5
<i>Điều 4. Tài liệu tham chiếu và tiêu chuẩn áp dụng</i>	9
<i>Điều 5. Danh mục quy tắc cấu hình ATTT và phạm vi áp dụng.....</i>	11
CHƯƠNG II. BỘ QUY TẮC CẤU HÌNH ATTT CHO MẠNG VĂN PHÒNG	13
<i>Điều 6. Quy tắc cấu hình ATTT cho hệ điều hành Windows của máy tính người dùng cuối.....</i>	13
<i>Điều 7. Quy tắc cấu hình ATTT cho hệ thống mạng nội bộ.....</i>	22
CHƯƠNG III. BỘ QUY TẮC CẤU HÌNH ATTT CHO ỨNG DỤNG... 39	
<i>Điều 8. Quy tắc lập trình an toàn trong phát triển ứng dụng web</i>	39
<i>Điều 9. Quy tắc lập trình an toàn sử dụng ứng dụng C/C++</i>	51
<i>Điều 10. Quy tắc lập trình an toàn cho ứng dụng mobile</i>	54
CHƯƠNG IV. BỘ QUY TẮC CẤU HÌNH ATTT CHO HỆ THỐNG ... 57	
<i>Điều 11. Quy tắc cấu hình ATTT cho hệ điều hành máy chủ</i>	57
<i>Điều 12. Quy tắc cấu hình ATTT cho Web server</i>	64
<i>Điều 13. Quy tắc cấu hình ATTT cho hệ quản trị CSDL.....</i>	71
<i>Điều 14. Quy tắc cấu hình ATTT cho Email Server.....</i>	76
<i>Điều 15. Quy tắc cấu hình ATTT cho hệ thống AD (Active Directory).....</i>	83
<i>Điều 16. Quy tắc cấu hình ATTT cho hệ thống Proxy.....</i>	89
<i>Điều 17. Quy tắc cấu hình ATTT cho hệ thống quản lý Antivirus tập trung.....</i>	95

<i>Điều 18. Quy tắc cấu hình ATTT cho hệ thống VPN tập trung</i>	<i>100</i>
--	------------

CHƯƠNG V. BỘ QUY TẮC CẤU HÌNH ATTT CHO CÁC THIẾT BỊ MẠNG 103

<i>Điều 19. Quy tắc cấu hình ATTT cho hệ thống firewall</i>	<i>103</i>
---	------------

<i>Điều 20. Quy tắc cấu hình ATTT cho thiết bị mạng</i>	<i>119</i>
---	------------

BỘ QUY TẮC CẤU HÌNH AN TOÀN THÔNG TIN CHO CÁC HỆ THỐNG THÔNG TIN TRONG TẬP ĐOÀN ĐIỆN LỰC QUỐC GIA VIỆT NAM

CHƯƠNG I. QUY ĐỊNH CHUNG

Điều 1. Mục đích

Tài liệu này quy định về các quy tắc lập trình an toàn và cấu hình đối với các thiết bị, hệ thống, ứng dụng đảm bảo an toàn thông tin, áp dụng thống nhất trong Tập đoàn Điện lực Quốc gia Việt Nam.

Điều 2. Đối tượng áp dụng

Bộ quy tắc các quy tắc lập trình an toàn và cấu hình đối với các thiết bị, hệ thống, ứng dụng đảm bảo an toàn thông tin áp dụng đối với:

- Tập đoàn Điện lực Việt Nam (EVN);
- Công ty con do EVN nắm 100% vốn điều lệ;
- Công ty con do Công ty TNHH MTV cấp II nắm giữ 100% vốn điều lệ;
- Người đại diện phần vốn của EVN, của Công ty TNHH MTV cấp II tại các công ty cổ phần, công ty trách nhiệm hữu hạn.

Điều 3. Thuật ngữ và từ ngữ viết tắt

1. Thuật ngữ

Trong bộ Quy tắc này, các từ ngữ dưới đây được hiểu như sau:

- *Active Directory*: hệ thống quản lý tài khoản người dùng tập trung.
- *Buffer overflow*: lỗi tràn bộ nhớ đệm, có thể là vùng nhớ stack hoặc heap. Lỗi xảy ra ghi chương trình ghi đè nội dung của bộ nhớ đệm do vượt quá giới hạn kích thước của bộ nhớ.
- *Câu lệnh CGI, SSI*: là chương trình gateway để giao tiếp thông tin với các server như là HTTP server.

- *CERT Coordination Center*: Trung tâm phối hợp Đội phản ứng nhanh An ninh mạng máy tính.
- *Client Injection*: những phương pháp tấn công chèn mã độc vào từ phía người dùng.
 - *Domain Controller*: máy chủ điều khiển chính.
 - *Email server*: máy chủ cài đặt ứng dụng thư điện tử.
 - *Firewall*: thiết bị tường lửa bảo vệ hệ thống mạng.
 - *Gateway*: là một nút mạng được sử dụng trong viễn thông nhằm kết nối hai mạng có giao thức truyền thông khác nhau có thể giao tiếp được với nhau.
 - *Hardcode*: các dữ liệu được đặt vào trong mã nguồn và không thay đổi.
 - *Hệ thống Antivirus tập trung*: hệ thống quản lý phần mềm Antivirus trên máy tính người dùng cuối, máy chủ tập trung. Hệ thống Antivirus tập trung thường được sử dụng để quản lý một số chính sách trên máy tính người dùng cuối như chính sách về chặn USB, chính sách tường lửa mềm hoặc thực hiện một số tác vụ như cập nhật bản vá, cài đặt phần mềm từ xa.
 - *Hệ thống Proxy*: máy chủ trung gian làm nhiệm vụ chuyển tiếp thông tin và kiểm soát, đảm bảo an toàn cho việc truy cập Internet của các máy khách sử dụng dịch vụ Internet.
 - *Integer overflow*: lỗi tràn số nguyên xảy ra khi giá trị của biến vượt quá khoảng giá trị của kiểu dữ liệu tương ứng.
 - *Mạng office*: là mạng văn phòng.
 - *Nhóm đặc quyền*: nhóm Built-in Administrators, Enterprise Admins, Domain Admins, Enterprise Admin.
 - *Phiên eBGP*: là phiên trao đổi thông tin định tuyến cho Internet và là giao thức được sử dụng giữa các ISP (là những AS khác nhau).
 - *Session, Cookie*: phiên đăng nhập của người dùng.
 - *SQL Injection*: là phương pháp tấn công chèn dữ liệu vào các câu truy vấn sql.
 - *Struct Exception Handling*: là một cấu trúc do Microsoft đưa ra nhằm xử lý các ngoại lệ trên hệ thống Windows.
 - *Tài khoản đặc quyền*: tài khoản quản trị Administrator có các quyền đặc biệt trong hệ thống.
 - *TapJacking*: xảy ra khi một ứng dụng độc hại cài đặt trên điện thoại chạy Android tạo ra các giao diện giả mạo người dùng nhằm lừa người dùng mua hàng, nhấp vào quảng cáo, cài đặt các ứng dụng, hoặc thậm chí xóa sạch tất cả các dữ liệu từ điện thoại...

- *Tấn công chéo*: tấn công giữa các máy chủ thành viên trong hệ thống hoặc các máy trạm.
- *Tấn công leo thang*: tấn công từ máy tính người dùng lên các máy chủ hệ thống lên đến máy chủ điều khiển chính (Domain Controller).
- *Use after free*: lỗi xảy ra khi chương trình tiếp tục sử dụng một con trỏ đến vùng nhớ sau khi đã giải phóng nó.
- *VPN*: Virtual Private Network (mạng riêng ảo), cho phép người dùng thiết lập một mạng riêng ảo an toàn trên Internet.
- *Web server*: máy chủ cài đặt ứng dụng web.
- *Whitelist*: là danh sách các thiết bị, IP được ưu tiên không áp dụng các chính sách, quy tắc ATTT mặc định.

2. Từ ngữ viết tắt

- Trong tài liệu này, các ký tự viết tắt được hiểu như sau:

STT	Từ viết tắt	Ý nghĩa
1	AD	Active Directory - Hệ thống quản lý user người dùng tập trung
2	APT	Advanced Persistent Threat - Tấn công có chủ đích
3	ASLR	Address Space Layout Randomization - là cơ chế của hệ điều hành nhằm tải chương trình lên bộ nhớ ở các địa chỉ ngẫu nhiên nhằm cản trở khả năng khai thác thành công các lỗ hổng phần mềm.
4	ATTT	An toàn thông tin
5	C&C	Command and Control - Máy chủ điều khiển và kiểm soát là một máy vi tính ra hiệu lệnh cho các thiết bị bị nhiễm mã độc và nhận thông tin ngược lại từ các thiết bị đó.
6	CERT	Computer Emergency Response Team - Đội phản ứng nhanh an ninh mạng máy tính.
7	CIS	Center for Internet Security - Trung tâm An ninh Internet
8	CVE	Common Vulnerabilities and Exposures - là danh sách các lỗi bảo mật máy tính công khai.
9	DEP	Data Execution Prevention - là cơ chế trong kiến trúc vi xử lý trong đó đánh dấu vùng nhớ nào là dữ liệu thì nếu

STT	Từ viết tắt	Ý nghĩa
		con trỏ lệnh chỉ vào vùng dữ liệu thì sẽ phát sinh cảnh báo lỗi.
10	GLBP	Gateway Load Balancing Protocol - là một giao thức dự phòng gateway của Cisco.
11	HA	High Availability – Tính sẵn sàng cao
12	HĐH Windows	Hệ điều hành Windows
13	HSRP	Hot Standby Router Protocol - là một giao thức chuẩn của Cisco cung cấp tính sẵn sàng cho hệ thống mạng.
14	IMAP	Post Office Protocol version 3 - Giao thức nhận email IMAP
15	MTA	Mail Transfer Agent
16	NIST	National Institute of Standards and Technology - Viện tiêu chuẩn và công nghệ Hoa Kỳ.
17	NSRP	NetScreen Redundancy Protocol - là một giao thức độc quyền được phát triển ban đầu bởi NetScreen Technologies Inc.
18	NTP	Network Time Protocol - là một thuật toán phần mềm giữ cho các máy tính và các thiết bị công nghệ khác nhau có thể đồng bộ hóa thời gian với nhau.
19	OTP	One Time Password - Mật khẩu sử dụng một lần
20	OWASP	Open Web Application Security Project - là một tổ chức phi lợi nhuận quốc tế chuyên về bảo mật ứng dụng web.
21	POP3	Post Office Protocol version 3 - Giao thức nhận email POP3.
22	SMTP	Mail Transfer Protocol - Giao thức truyền tải email
23	SNMP	Simple Network Monitoring Protocol - Giao thức giám sát mạng đơn giản.
24	SSID	Service Set Identifier - là tên chính của mạng cục bộ không dây.
25	URL	Uniform Resource Locator - được gọi một cách thông thường là một địa chỉ web, là một tham chiếu đến tài nguyên web chỉ định vị trí của nó trên hệ thống mạng và cơ chế để truy xuất nó.

STT	Từ viết tắt	Ý nghĩa
26	VDI	Virtual Desktop Infrastructure - Hạ tầng máy tính ảo hóa
27	VNCERT/CC	Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam, là Cơ quan điều phối quốc gia về ứng cứu sự cố, thuộc Cục An toàn thông tin - Bộ Thông tin và Truyền thông. Có chức năng điều phối, ứng cứu các sự cố an toàn thông tin mạng trên toàn quốc.
28	VRRP	Virtual Router Redundancy Protocol - là giao thức được mô tả trong RFC3768, nó cho phép sử dụng chung 1 địa chỉ IP gateway cho một nhóm router.
29	XSS	Cross Site Scripting - Kiểu tấn công nhắm vào phía người dùng như đánh cắp thông tin truy cập, hướng người dùng vào các trang web có mã độc,...

Điều 4. Tài liệu tham chiếu và tiêu chuẩn áp dụng

STT	Tài liệu	Mô tả
1	CIS Control Version 7.1.	CIS Control Version 7.1 là một hướng dẫn toàn diện gồm 20 biện pháp bảo vệ và đối phó để phòng thủ an ninh mạng hiệu quả. CIS Controls được phát hành bởi tổ chức CIS.
2	Tài liệu thực hành lập trình an toàn (OWASP Secure Coding Practices) của tổ chức OWASP.	OWASP Secure Coding Practices là một tiêu chuẩn để phục vụ việc kiểm thử do tổ chức OWASP đề xuất.
3	SEI CERT Coding Standard.	SEI CERT Coding Standard là các tiêu chuẩn mã hóa phần mềm được phát triển bởi CERT Coordination Center để cải thiện tính an toàn, độ tin cậy và bảo mật của các hệ thống phần mềm.
4	Secure Coding in C and C++ (Robert C. Seacord, 2013).	Tài liệu hướng dẫn lập trình an toàn trên ngôn ngữ C và C++, tác giả Robert C. Seacord.

STT	Tài liệu	Mô tả
5	https://cwe.mitre.org .	https://cwe.mitre.org là website chứa các lỗ hổng và các điểm yếu phổ biến, được thành lập vào năm 1999 bởi MITRE (Mỹ). Mục đích của chương trình này là phân loại và nhận dạng những lỗ hổng về phần cứng hoặc phần mềm, tập hợp thành 1 hệ thống mở để chuẩn hóa quy trình xác thực các lỗ hổng đã được biết.
6	International Standard ISO/IEC 14882:2020 (E) – Programming Language C++.	International Standard ISO/IEC 14882:2020 (E) – Programming Language C++, Tiêu chuẩn quốc tế ISO chỉ định các yêu cầu đối với việc triển khai ngôn ngữ lập trình C ++.
7	Application Security for the Android Platform (Jeff Six, 2012, published by O'Reilly Media).	Application Security for the Android Platform - Tác giả Jeff Six, các yêu cầu cần đảm bảo về an toàn thông tin khi lập trình ứng dụng Android.
8	Hacking and Securing iOS Applications (Jonathan Zdziarski, 2012, published by O'Reilly Media).	Hacking and Securing iOS Applications - Tác giả Jonathan Zdziarski, các yêu cầu cần đảm bảo về an toàn thông tin khi lập trình ứng dụng iOS.
9	Mobile Application Security (Himanshu Dwivedi, Chris Clark, David Thiel, 2010, published by The McGraw-Hill Companies).	Mobile Application Security, Tác giả Himanshu Dwivedi, Chris Clark, David Thiel, các yêu cầu cần đảm bảo về an toàn thông tin khi lập trình ứng dụng trên thiết bị di động.
10	Các bộ Tiêu chuẩn NIST SP 800-123, NIST SP 800-44, NIST.CSWP.04162018 của tổ chức NIST.	Hướng dẫn an toàn máy chủ và hướng dẫn an toàn máy chủ web.
11	Tiêu chuẩn an toàn thông tin cho hệ thống thông tin cấp độ 3 (sau đây gọi tắt là TLTK 1).	Thông tư 03/2017/TT-BTTTT của Bộ thông tin và Truyền thông ngày 24/4/2017 quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về đảm bảo an toàn hệ thống thông tin theo cấp độ.

STT	Tài liệu	Mô tả
12	Tiêu chuẩn TCVN 11930:2017 (sau đây gọi tắt là TLTK 2).	TCVN 11930:2017 do Cục An toàn thông tin biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố. Tiêu chuẩn này quy định các yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ, bao gồm hai nhóm: yêu cầu quản lý và yêu cầu kỹ thuật.
13	Mitigating Pass-the-Hash and Other Credential Theft, version 2 (sau đây gọi tắt là TLTK 3).	Mitigating Pass-the-Hash and Other Credential Theft, version 2, Microsoft, cách phòng chống các kỹ thuật tấn công trộm cắp thông tin và xác thực.

Điều 5. Danh mục quy tắc cấu hình ATTT và phạm vi áp dụng

1. Quy tắc cấu hình ATTT cho hệ điều hành Windows của người dùng cuối
 - Áp dụng cho các máy tính người dùng sử dụng hệ điều hành Windows.
2. Quy tắc cấu hình ATTT cho hệ thống mạng nội bộ
 - Áp dụng cho bộ phận Quản trị hệ thống mạng nội bộ.
3. Quy tắc lập trình an toàn trong phát triển ứng dụng web
 - Áp dụng cho bộ phận Quản trị và phát triển ứng dụng web.
4. Quy tắc lập trình an toàn sử dụng ứng dụng C/C++
 - Áp dụng cho bộ phận Phát triển ứng dụng sử dụng C/C++.
5. Quy tắc lập trình an toàn cho ứng dụng mobile
 - Áp dụng cho bộ phận Phát triển ứng dụng Mobile.
6. Quy tắc cấu hình ATTT cho hệ điều hành máy chủ
 - Áp dụng cho bộ phận Quản trị máy chủ.
7. Quy tắc cấu hình ATTT cho web server
 - Áp dụng cho bộ phận Quản trị hệ thống web server.
8. Quy tắc cấu hình ATTT cho hệ quản trị cơ sở dữ liệu
 - Áp dụng cho bộ phận Quản trị hệ thống cơ sở dữ liệu.
9. Quy tắc cấu hình ATTT cho Email server
 - Áp dụng cho bộ phận Quản trị hệ thống Email.

10. Quy tắc cấu hình ATTT cho hệ thống Active Directory
 - Áp dụng cho bộ phận Quản trị hệ thống Active Directory.
11. Quy tắc cấu hình ATTT cho hệ thống Proxy
 - Áp dụng cho bộ phận Quản trị hệ thống Proxy.
12. Quy tắc cấu hình ATTT cho hệ thống quản lý Antivirus tập trung
 - Áp dụng cho bộ phận Quản trị hệ thống Antivirus.
13. Quy tắc cấu hình ATTT cho hệ thống VPN tập trung
 - Áp dụng cho bộ phận Quản trị hệ thống VPN.
14. Quy tắc cấu hình ATTT cho hệ thống Firewall
 - Áp dụng cho bộ phận Quản trị Firewall.
15. Quy tắc cấu hình ATTT cho thiết bị mạng
 - Áp dụng cho bộ phận Quản trị thiết bị mạng.

CHƯƠNG II.
BỘ QUY TẮC CẤU HÌNH ATTT CHO MẠNG VĂN PHÒNG

Điều 6. Quy tắc cấu hình ATTT cho hệ điều hành Windows của máy tính người dùng cuối

Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
Thiết lập BIOS ở chế độ UEFI (nếu có).	Chế độ UEFI cho phép thiết lập nhiều tùy chọn bảo mật hơn so với chế độ Legacy	Phụ lục 01	Kiểm tra trực tiếp cấu hình BIOS trên máy		
Enable tùy chọn Secure Boot (nếu có).	Secure boot đảm bảo chỉ có firmware đã được verified mới được nạp trong quá trình khởi động máy	Phụ lục 01	Kiểm tra trực tiếp cấu hình BIOS trên máy	NIST.CSWP.04 162018	
Thiết lập Boot Order luôn boot từ Harddisk.	Không được thiết lập first boot từ các nguồn khác như: CD-ROM drive, USB device, ethernet controller,...	Phụ lục 01	Kiểm tra trực tiếp cấu hình BIOS trên máy	NIST.CSWP.04 162018	
Tắt tùy chọn network boot (Wake-On LAN).	Chống việc sử dụng boot máy từ xa qua kết nối network	Phụ lục 01	Kiểm tra trực tiếp cấu hình BIOS trên máy		

Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
Cài đặt mật khẩu BIOS (tùy chọn áp dụng).	Chống việc thay đổi cấu hình BIOS máy tính	Phụ lục 01	Kiểm tra trực tiếp cấu hình BIOS trên máy	NIST.CSWP.04 162018	Tùy chọn áp dụng
Thiết lập lại tất cả các cấu hình BIOS trong trường hợp pin CMOS được thay thế, hoặc bị tháo ra.	Đảm bảo tính toàn vẹn cấu hình BIOS	Phụ lục 01	Kiểm tra trực tiếp cấu hình BIOS trên máy	NIST.CSWP.04 162018	
Disable các network interface không sử dụng.	Tránh việc khai thác từ bên ngoài qua các interface không sử dụng	Phụ lục 01	Trình quản lý network device của hệ điều hành		
Tường lửa của hệ điều hành hoặc của phần mềm antivirus phải luôn được bật. Cấu hình ghi log tường lửa.		Phụ lục 01	Trình quản lý firewall của hệ điều hành	NIST.CSWP.04 162018	
Thiết lập chính sách tường lửa chiều vào (Inbound) và chiều ra (Outbound).		Phụ lục 01	Trình quản lý firewall của hệ điều hành	NIST.CSWP.04 162018	
Cấu hình chặn kết nối giữa các máy người dùng với nhau theo các cổng sau: 135->139	Đây là các cổng dịch vụ có thể được sử dụng để	Phụ lục 01	Trình quản lý firewall của hệ điều hành hoặc		Thống kê để Whitelist

Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
(NetBIOS), 445 (windows shared). Trong trường hợp đơn vị có 1 số máy in dùng Printer-share thì có thể thống kê để whitelist.	khai thác lỗ hổng của Windows.		theo policy từ hệ thống AD tập trung		
Máy tính cần sử dụng Proxy của đơn vị (nếu có) để truy cập Internet, không truy cập Internet trực tiếp.		Phụ lục 01	Trình quản lý proxy của hệ điều hành		
Sử dụng cấu hình DNS của EVN (nếu có).		Phụ lục 01	Trình quản lý network device của hệ điều hành		
Cài đặt phiên bản HĐH Windows còn hỗ trợ. Không sử dụng phiên bản đã ngừng hỗ trợ.	Đảm bảo Microsoft tiếp tục đưa ra các bản cập nhật vá lỗi nếu có.	Phụ lục 01	Theo lộ trình hỗ trợ phiên bản của hãng	NIST.CSWP.04 162018	
Với các hệ điều hành có yêu cầu bản quyền, phải sử dụng license hợp lệ của đơn vị.		Phụ lục 01	Trình quản lý license của hệ điều hành	NIST.CSWP.04 162018	
Trong trường hợp không có hệ thống quản lý bản vá, bắt chế độ cập nhật bản vá tự động, tối	Các bản vá loại Security, Critical cung cấp các cập nhật fix lỗi	Phụ lục 01	Trình quản lý update của hệ điều hành hoặc	NIST.CSWP.04 162018	

Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
thiếu phải cập nhật bản vá loại Security, Critical.	ngghiêm trọng của hệ điều hành.		theo policy từ hệ thống AD tập trung		
Khuyến nghị update qua WSUS tập trung trên Windows (nếu có).		Phụ lục 01	Trình quản lý update của HĐH và trên update server của đơn vị		
Yêu cầu thiết lập ghi log hệ thống. Bật log Application, Security, System trên Windows		Phụ lục 01	Trình quản lý ghi log của HĐH	NIST.CSWP.04 162018	
Không cho phép người dùng chia sẻ file trên máy tính (tùy chọn áp dụng). Tắt chia sẻ mặc định.	Hạn chế việc tấn công lây lan qua giao thức chia sẻ file	Phụ lục 01	Trình quản lý policy của hệ điều hành hoặc theo policy từ hệ thống AD tập trung		Tùy chọn áp dụng
Hiển thị đầy đủ thông tin định dạng tập tin (file extension) trên máy người dùng.	Hạn chế việc tấn công qua giả mạo file	Phụ lục 01	Trình quản lý Folder Option của hệ điều hành		
Khi sử dụng các phần mềm chat để phục vụ công việc (ví dụ: Skype, Google talk, MSN chat hoặc các phần mềm tương đương) cần sự chấp	Hạn chế nguy cơ lộ lọt thông tin trong tổ chức.	Phụ lục 01	Trình quản lý cài đặt phần mềm của hệ điều hành		Đơn vị ban hành danh mục các phần mềm chat được

Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
thuận có thời hạn của bộ phận CNTT, lãnh đạo đơn vị phê duyệt và chịu trách nhiệm.					phép cài đặt, sử dụng
Hạn chế sử dụng các phần mềm bên ngoài cho phép remote, điều khiển máy tính từ xa (ví dụ: teamviewer, logmein, vnc, radmin, x-manager hoặc các phần mềm tương đương). Khi cài đặt, sử dụng các phần mềm này cần được sự phê duyệt của bộ phận CNTT, lãnh đạo đơn vị và tuân thủ các quy định ATTT của EVN	Hạn chế nguy cơ lộ lọt thông tin trong tổ chức.	Phụ lục 01	Trình quản lý cài đặt phần mềm của hệ điều hành		
Hạn chế sử dụng các phần mềm vượt tường lửa, proxy như các phần mềm proxy, VPN, tunnel (ví dụ: hotspot shield, ultrasurf hoặc các phần mềm tương đương). Khi cài đặt, sử dụng các phần mềm này cần được sự phê	Hạn chế nguy cơ lộ lọt thông tin trong tổ chức. Các nguy cơ bị tấn công điều khiển từ xa.	Phụ lục 01	Trình quản lý cài đặt phần mềm của hệ điều hành		Tùy chọn áp dụng.

Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
duyet của bộ phận CNTT, lãnh đạo đơn vị và tuân thủ các quy định ATTT của EVN.					
Máy tính cài đặt: Phần mềm diệt virus hoặc phần mềm giám sát bất thường theo quy định, chính sách hiện hành.		Phụ lục 01	Trình quản lý cài đặt phần mềm của hệ điều hành	NIST.CSWP.04 162018	
Đối với phần mềm diệt virus: khuyến nghị thiết lập cấu hình update định kỳ, cấu hình bảo vệ, giám sát thường trực.		Phụ lục 01	Trình quản lý cài đặt của phần mềm diệt virus	NIST.CSWP.04 162018	
Máy tính phải được join domain để quản lý chính sách tập trung.		Phụ lục 01	Máy tính được khai báo trên hệ thống domain		
Người dùng sử dụng mạng nội bộ của đơn vị phải dùng tài khoản domain để sử dụng máy tính. Với các trường hợp ngoại lệ cần có sự phê duyệt của lãnh đạo đơn vị.		Phụ lục 01	Tài khoản được khai báo trên hệ thống domain		

Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
Tên tài khoản chuẩn hóa.	Đảm bảo việc quản lý tài khoản được chính xác, hiệu quả.	Phụ lục 01		NIST.CSWP.04 162018	
Tên máy tính chuẩn hóa.	Đảm bảo việc quản lý máy tính, thiết bị được chính xác, hiệu quả.	Phụ lục 01		NIST.CSWP.04 162018	
Với các máy join domain, tài khoản người dùng không được có quyền administrator trên máy tính.		Phụ lục 01	Danh sách các tài khoản trên máy người dùng		
Thiết lập chính sách mật khẩu mạnh cho tài khoản theo quy định chính sách mật khẩu mạnh hiện hành của EVN ban hành.		Phụ lục 01			
Xóa bỏ hoặc vô hiệu hóa tài khoản thừa, không sử dụng.		Phụ lục 01	Danh sách các tài khoản trên máy người dùng	NIST.CSWP.04 162018	
Giới hạn máy đăng nhập của người dùng với các máy join domain. Mỗi tài khoản người dùng chỉ được đăng nhập vào		Phụ lục 01	Quyền của tài khoản trên hệ thống domain	NIST.CSWP.04 162018	Chính sách này cấu hình trên GPO trên

Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
các máy tính được cho phép (không được phép đăng nhập chéo trên máy khác).					AD cho các máy tính join domain
Cấu hình đồng bộ thời gian trên máy tính về server NTP tập trung hoặc thông qua server AD.		Phụ lục 01	Trình quản lý cài đặt thời gian của hệ điều hành		
Tắt tính năng tự động chạy khi kết nối tới các thiết bị lưu trữ gắn ngoài.	Hạn chế khai thác tấn công khi cắm thiết bị ngoại vi.	Phụ lục 01	Trình quản lý cài đặt thiết bị ngoại vi của hệ điều hành hoặc chính sách policy từ AD tập trung	NIST.CSWP.04 162018	
Không cho phép máy tính người dùng sử dụng các thiết bị lưu trữ, đọc ghi dữ liệu (USB, Ổ cứng di động, ổ đĩa CD, DVD, ...). Với các trường hợp ngoại lệ cần được phê duyệt bằng văn bản của lãnh đạo đơn vị.	Hạn chế khai thác tấn công hoặc lộ lọt dữ liệu khi sử dụng thiết bị ngoại vi.	Phụ lục 01	Trình quản lý cài đặt thiết bị ngoại vi của hệ điều hành hoặc chính sách policy từ AD tập trung		

Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
Các dữ liệu mật, tài liệu quan trọng cần được lưu trữ trong thư mục, phân vùng có mã hóa hoặc được bảo vệ bởi phần mềm mã hóa (khuyến nghị).	Hạn chế nguy cơ lộ lọt thông tin trong tổ chức.	Phụ lục 01	Theo phần mềm mã hóa, bảo vệ dữ liệu đơn vị lựa chọn sử dụng		Khuyến nghị

Điều 7. Quy tắc cấu hình ATTT cho hệ thống mạng nội bộ

a) Toàn bộ hạ tầng mạng nội bộ phải được bảo vệ và kiểm soát chính sách bằng Firewall. Đảm bảo phân tách về mặt logic giữa các hệ thống khác nhau.

b) Các thiết bị đầu cuối kết nối vào mạng nội bộ cần được bảo vệ khỏi virus, mã độc, botnets, các phần mềm độc hại và đảm bảo các yêu cầu về chính sách bảo mật khác của tổ chức.

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
1. Hạ tầng mạng						
Yêu cầu sử dụng Firewall cứng	Hạ tầng mạng nội bộ phải có firewall cứng làm nhiệm vụ bảo vệ.	Sử dụng Firewall cứng để quản lý chính sách kết nối sẽ đảm bảo hơn do các Firewall mềm chạy trên các hệ điều hành có tồn tại nhiều lỗi tiềm ẩn		Kiểm tra mô hình mạng thực tế.		
Yêu cầu phân tách vùng mạng bằng Firewall	Người dùng và các hệ thống phải được phân tách vùng mạng bằng các Firewall và quản lý chính sách thông qua Firewall	Đảm bảo phân tách người dùng và hệ thống, sẽ khai báo và phân quyền người dùng vào các hệ thống cụ thể theo quy định		Kiểm tra thiết kế mạng.	Tham chiếu một phần các tiêu chuẩn: - TLTK 1. - TLTK 2. - CIS Control V7.1	

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
	Tách biệt zone người dùng và server Farm				mục 14.1, 14.2	
	Tách biệt vùng có kết nối Internet (DMZ,..) với các phân vùng khác với các vùng Office (vùng mạng Văn phòng), Internet, WAN, Server Farm	Phòng tránh rủi ro khi hệ thống có kết nối internet bị chiếm quyền thì sẽ không lây lan sang các hệ thống nội bộ				
	Tách biệt người dùng quản trị và người dùng thường	Tránh tấn công người dùng quản trị thông qua người dùng thường thiếu kiến thức ATTT				
	Phân tách theo chức năng nghiệp vụ, phân tách theo độ quan trọng	Đảm bảo security level cho các hệ thống để có chính sách bảo vệ phù hợp, không để tấn công lây lan từ hệ thống kém quan				

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
		trọng sang hệ thống quan trọng				
Yêu cầu sử dụng Proxy	Kết nối internet của người dùng phải đi qua Proxy, không mở kết nối trực tiếp	Đảm bảo kết nối an toàn qua chính sách của Proxy		Kiểm tra mô hình mạng thực tế.		
Yêu cầu thiết bị mạng phải theo tiêu chuẩn của thiết bị mạng	Cấu hình các thiết bị mạng phải theo tiêu chuẩn của thiết bị mạng	Đảm bảo an toàn cho các thiết bị mạng		Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - TLTK 1. - TLTK 2.	
2. Hệ thống Firewall						
Yêu cầu chặn các kết nối đến các máy chủ điều khiển mã độc (C&C - Command and Control)	Khai báo chặn các kết nối C&C, các domain độc hại Khai báo rule ở vị trí có hiệu lực đầu tiên	Danh sách C&C và Domain theo khuyến nghị của VNCERT/CC,.. để tránh các máy nhiễm APT kết nối về máy chủ C&C	Phụ lục 14	Kiểm tra khai báo policy trên các thiết bị Firewall	Tham chiếu một phần các tiêu chuẩn: - TLTK 1. - TLTK 2. - CIS Control V7.1 mục 12.3	

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
Yêu cầu chặn người dùng quản trị ra Internet	Khai báo rule chặn người dùng quản trị ra Internet trực tiếp và qua Proxy Chỉ mở cho người dùng quản trị đến các hệ thống theo các port quản trị	Các kết nối từ người dùng quản trị ra internet hoặc qua proxy đều có tiềm ẩn nguy cơ kết nối tới máy chủ C&C chưa được phát hiện khi máy người dùng quản trị bị tấn công APT mà các công cụ khác chưa kịp phát hiện và ngăn chặn. Người dùng quản trị chỉ được vào các hệ thống quản trị, mở port khác như người dùng thông thường	Phụ lục 14		Tham chiếu một phần tiêu chuẩn: - CIS Control V7.1 mục 11.6	
Yêu cầu chặn kết nối port quản trị từ vùng có security level thấp sang vùng	Khai báo rule chặn kết nối port quản trị từ vùng có security level thấp sang vùng có security level cao	Đảm bảo các hệ thống có mức security level thấp hơn không thể quản trị được các hệ thống có mức	Phụ lục 14		Tham chiếu một phần tiêu chuẩn: - CIS Control V7.1 mục 14.2	

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
có security level cao		security level cao hơn			- TLTK 1.	
Yêu cầu về khai báo/thiết lập chính sách	Thiết lập chính sách cho phép vừa đủ các địa chỉ nguồn, địa chỉ đích, port dịch vụ và kiểm soát ứng dụng đối với từng hệ thống cụ thể	Đảm bảo việc chỉ người dùng quản trị hệ thống nào được truy cập hệ thống đó, không mở thừa nguồn, đích hoặc port dịch vụ để tránh bị tấn công thông qua các kết nối tunnel giữa các hệ thống. Mở không qua chi tiết để đảm bảo về tài nguyên và hiệu năng của Firewall/IPS	Phụ lục 14		Tham chiếu một phần tiêu chuẩn: - CIS Control V7.1 mục 9.2 - TLTK 2.	
3. Hệ thống AD (Active Directory)						
Yêu cầu sử dụng AD cho người dùng	Tất cả máy tính người dùng phải được join AD để	Đảm bảo tất cả người dùng được quản lý tập trung và được áp dụng	Phụ lục 10			

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
	quản lý về chính sách tập trung	chính sách thông qua hệ thống AD				
Yêu cầu thiết lập chính sách ATTT cho AD	Trên máy chủ AD phải thực hiện thiết lập chính sách ATTT cho người dùng theo Tiêu chuẩn thiết lập chính sách máy tính người dùng	Đảm bảo ATTT cho hệ thống AD				
Yêu cầu thực hiện quản lý hiện trạng tài khoản người dùng trên hệ thống AD	Loại bỏ những tài khoản không sử dụng	Loại bỏ các tài khoản thừa, tránh nguy cơ lợi dụng tài khoản thừa để tấn công				
	Giám sát được những tài khoản chưa bao giờ logon, máy tính không hoạt động					
	Thực hiện báo cáo tình hình, các vấn đề về hiện trạng tài khoản - máy tính người dùng định kỳ	Nắm rõ được tình hình hệ thống và người dùng theo thời gian, phục vụ cho việc phân tích hành vi				

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
	(hàng tuần/tháng/năm)					
4. Hệ thống mạng không dây						
Yêu cầu thay đổi giá trị mặc định	Thay đổi SSID mặc định	Tránh tấn công bằng tài khoản mặc định			Tham chiếu một phần tiêu chuẩn: - CIS Control V7.1 mục 15.10	
	Thay đổi mật khẩu quản trị					
Yêu cầu thống nhất định danh SSID	Định danh SSID phải thể hiện được tên đối tượng sử dụng, có thể kết hợp mã đơn vị (MDV)	Xác định rõ mục đích của từng SSID, có mức bảo vệ phù hợp cho mỗi loại		Kiểm tra cấu hình trên các thiết bị Controller, AP	Tham chiếu một phần tiêu chuẩn: - CIS Control V7.1 mục 15.10	
	SSID cho khách: MDV-GUEST					
	SSID cho nhân viên truy cập Internet: MDV hoặc MDV-Wifi					
	SSID cho nhân viên truy cập nội bộ: MDV-PRIVATE					

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
	SSID cho phòng họp/demo sản phẩm: MDV-MEETING					
Yêu cầu về chính sách truy cập	Đối với SSID sử dụng cho khách: - Chỉ truy cập được ra ngoài Internet qua đường truyền riêng mà không vào được mạng nội bộ - Không yêu cầu ẩn SSID	Đảm bảo cho khách hàng truy cập internet		Kiểm tra thiết kế luồng lưu lượng mạng, cấu hình trên các thiết bị Controller, AP và Firewall	Tham chiếu một phần tiêu chuẩn: - CIS Control V7.1 mục 15.10	
	Đối với SSID sử dụng cho nhân viên truy cập Internet - Chỉ truy cập Internet mà không truy cập được mạng nội bộ - Không yêu cầu ẩn SSID	Đảm bảo cho cán bộ công nhân viên đã được xác thực truy cập internet				
	Đối với SSID sử dụng cho nhân viên	Phòng tránh nguy cơ tấn công APT từ				

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
	<p>truy cập mạng nội bộ:</p> <ul style="list-style-type: none"> - Chỉ truy cập mạng nội bộ và email public mà không truy cập được Internet. - Yêu cầu ẩn SSID 	internet vào hệ thống nội bộ				
	<p>Đối với SSID sử dụng cho phòng họp/demo sản phẩm:</p> <ul style="list-style-type: none"> - Truy cập email public, một số địa chỉ nội bộ phục vụ demo (mở chính sách theo yêu cầu, thời gian), còn lại chặn ra Internet và mạng nội bộ. - Yêu cầu ẩn SSID 	Phòng tránh nguy cơ tấn công APT từ internet vào hệ thống nội bộ				
Yêu cầu đặt chế độ bảo mật cao cho mật khẩu (Password)	Khuyến cáo nên sử dụng mật khẩu cho các SSID.	Đặt mật khẩu cho các SSID để đảm bảo xác thực khi kết nối		Kiểm tra cấu hình trên các thiết bị Controller, AP	Tham chiếu một phần tiêu chuẩn:	

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
	WPA2-AES hoặc WPA2-TKIP	Sử dụng mức cao nhất thiết bị hỗ trợ để đảm bảo không bị tấn công giải mã mật khẩu			- CIS Control V7.1 mục 15.7, 15.8	
	Thiết lập chính sách mật khẩu mạnh theo quy định của đơn vị.	Đảm bảo mật khẩu mạnh chống tấn công dò quét mật khẩu				
Yêu cầu cơ chế xác thực người dùng	SSID sử dụng cho khách: Xác thực bằng Password (WPA2-PSK)	Đảm bảo mật khẩu mạnh chống tấn công dò quét mật khẩu		Kiểm tra cấu hình trên các thiết bị Controller, AP	Tham chiếu một phần tiêu chuẩn: - CIS Control V7.1 mục 15.7, 15.8	
	SSID còn lại áp dụng ít nhất 1 trong 3 cơ chế xác thực: - User 802.1x (WPA2-Enterprise). - Password (WPA2-PSK). - Lọc MAC thiết bị.					
5. Hệ thống giải pháp ATTT trong mạng nội bộ						

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
Yêu cầu triển khai các hệ thống phòng chống mã độc	Toàn bộ máy người dùng, máy chủ Windows nội bộ phải được cài đặt phần mềm phòng chống mã độc	Đảm bảo người dùng được bảo vệ khỏi virus trên thiết bị		Kiểm tra chính sách quản lý máy tính người dùng, cấu hình, hiện trạng của các máy trạm và hệ thống tập trung	Tham chiếu một phần tiêu chuẩn: - CIS Control V7.1 mục 8.2, 8.6 - TLTK 1.	
	Hệ thống máy chủ phòng chống mã độc tập trung phải được thực hiện cập nhật mẫu hàng ngày	Đảm bảo phòng tránh được các mã độc mới nhất				
	Phần mềm phòng chống mã độc trên máy trạm phải được thực hiện cập nhật mẫu hàng ngày					
	Trên máy chủ phòng chống mã độc có thiết lập chính sách định kỳ quét virus trên toàn bộ máy trạm và máy chủ Windows nội bộ tối thiểu 1 tháng 1 lần	Đảm bảo tất cả các máy tính được quét mã độc định kỳ và liên tục				

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
	Không cho phép người dùng can thiệp, tắt hoặc tùy chỉnh sửa tùy chỉnh của chương trình phòng chống mã độc	Đảm bảo chính sách thống nhất, người dùng không bypass được phần mềm phòng chống mã độc				
	Xuất báo cáo hàng tuần về hiện trạng về các máy trạm nhiễm mã độc	Nắm rõ được tình hình hệ thống và người dùng theo thời gian, phục vụ cho việc phân tích hành vi				
Yêu cầu triển khai các hệ thống cập nhật bản vá	Khuyến nghị thực hiện kiểm thử bản vá trước khi thực hiện cập nhật cho máy người dùng, máy chủ nhằm đảm bảo tính an toàn, ổn định của hệ thống.	Đảm bảo tính ổn định, an toàn		Kiểm tra chính sách quản lý máy tính người dùng, cấu hình, hiện trạng của các máy trạm và hệ thống tập trung	Tham chiếu một phần tiêu chuẩn: - TLTK 1.	
	Máy chủ cập nhật bản vá cho máy tính người dùng phải thực hiện cập nhật	Đảm bảo được cập nhật các bản vá mới nhất để phòng tránh và khắc phục				

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
	bản vá hàng ngày từ Internet (khuyến nghị qua hệ thống Proxy – nếu có).	các lỗi vừa được phát hiện				
	Toàn bộ máy tính người dùng và máy chủ ứng dụng nội bộ phải được thực hiện ra quét bản vá hàng ngày từ máy chủ cập nhật bản vá và thực hiện cập nhật bản vá mới nhất.					
	Trên máy chủ cập nhật bản vá phải thực hiện cấu hình cập nhập bản vá về ATTT cho client.	Đảm bảo bản vá ATTT mới nhất cho client và đồng nhất cho tất cả các máy				
	Thực hiện quản lý bản vá và xuất báo cáo hàng tuần về hiện trạng cập nhập các bản vá của máy trạm.	Nắm rõ được tình hình hệ thống và người dùng theo thời gian, phục vụ cho việc phân tích hành vi				

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
Yêu cầu triển khai các hệ thống Proxy	Thực hiện đầy đủ việc cập nhật khắc phục lỗ hổng ATTT được khuyến cáo.	Đảm bảo được cập nhật các bản vá mới nhất để phòng tránh và khắc phục các lỗi vừa được phát hiện	Tham khảo Quy tắc cấu hình ATTT cho hệ thống Proxy			
	Lưu đầy đủ log hoạt động của hệ thống.	Nắm rõ được tình hình hệ thống và người dùng theo thời gian, phục vụ cho việc phân tích hành vi				
	Lưu đầy đủ log của người dùng, thông tin log bao gồm địa chỉ IP, thời gian, URL truy cập.					
	Tất cả log được lưu tập trung tối thiểu 06 tháng.					
	Toàn bộ máy tính người dùng truy cập Internet phải qua hệ thống proxy.	Đảm bảo kết nối an toàn qua chính sách của Proxy và lưu log				
	Thực hiện xác thực người dùng khi sử dụng Proxy.	Đảm bảo việc xác thực và phân quyền				

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
		người dùng theo quy định				
	Cần cấu hình chặn người dùng upload tài liệu lên các trang chia sẻ dữ liệu trực tuyến.	Đảm bảo chống thất thoát dữ liệu				
Yêu cầu triển khai các giải pháp ATTT	Giải pháp Giám sát phát hiện tấn công có chủ đích (APT) cho các Endpoint (máy chủ/máy trạm): Đảm bảo triển khai đủ 100% máy tính trong văn phòng cài đặt giải pháp Endpoint.	Đảm bảo theo dõi được hành vi người dùng trên Endpoint	Phụ lục 02	Kiểm tra chính sách quản lý và hiện trạng hạ tầng.	Tham chiếu một phần tiêu chuẩn: - TLTK 1.	
	Giải pháp Giám sát máy chủ: triển khai đủ 100% server.	Đảm bảo theo dõi được hành vi người quản trị và ứng dụng trên Server				
	Khuyến nghị triển khai giải pháp giám sát phát hiện tấn	Đảm bảo thu thập được tất cả kết nối giữa người dùng,				

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
	<p>công qua lớp/tầng mạng:</p> <ul style="list-style-type: none"> - Giải pháp phải bắt được toàn bộ các loại traffic của nhóm quản trị và traffic đi qua vùng mạng khác của người dùng thường. - Giải pháp phải bắt được toàn bộ traffic của các hệ thống ứng dụng đi các vùng mạng và kết nối tới các hệ thống DNS, AD, Proxy. 	hệ thống và internet				
	<p>Khuyến nghị triển khai giải pháp kiểm soát truy nhập mạng văn phòng - NAC để kiểm soát truy nhập:</p> <ul style="list-style-type: none"> - Kiểm soát truy nhập, đảm bảo baseline (chính sách) mới cho truy 	Đảm bảo kiểm soát được truy cập của người dùng phải theo chính sách mới được kết nối vào mạng				

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu	Ghi chú
	<p>cập mạng: Đảm bảo cài đặt Endpoint, AV và join AD.</p> <p>- Phục vụ cô lập máy tính trong mạng nội bộ khi có sự cố về ATTT.</p>					

CHƯƠNG III. BỘ QUY TẮC CẤU HÌNH ATTT CHO ỨNG DỤNG

Điều 8. Quy tắc lập trình an toàn trong phát triển ứng dụng web

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Thông tin định danh	<ul style="list-style-type: none"> - Tên đăng nhập phải là duy nhất, không phân biệt hoa thường, chỉ nên chứa tập các ký tự là chữ cái, chữ số, dấu gạch dưới. - Thiết lập chính sách mật khẩu mạnh theo yêu cầu tại quy định chính sách mật khẩu mạnh hiện hành của EVN ban hành. - Thiết lập thời gian hết hiệu lực cho mật khẩu tối đa 90 ngày, mật khẩu mới không được trùng với mật khẩu hiện tại. - Đối với chức năng reset/quên mật khẩu: <ul style="list-style-type: none"> ▪ Đường dẫn reset/quên mật khẩu được gửi qua email phải bị mất hiệu lực sau lần truy cập đầu tiên hoặc sau 8 giờ nếu không được truy cập. ▪ Nếu chức năng reset/quên mật khẩu thực hiện gửi mật khẩu qua email, tin nhắn thì mật khẩu phải được sinh ngẫu nhiên và phải tuân theo chính sách mật khẩu mạnh tại mục 1.2. ▪ Nếu chức năng reset/quên mật khẩu sử dụng mã OTP để kiểm tra xác nhận từ 	Bảo vệ tài khoản người dùng.	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 02.	OWASP Secure Coding Practices: Mục "Authentication and Password Management"

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	<p>người dùng, việc sử dụng mã OTP (hướng dẫn tại mục 9 trong cùng tài liệu này).</p> <p>- Chỉ lưu dạng mã hash của mật khẩu, mã PIN trong database (DB), sử dụng thuật toán hash từ SHA-256, SHA-512, SHA-3 và các thuật toán tương đương.</p>				
Quản lý phiên đăng nhập	<p>- Session phải được quản lý bởi server, sinh ngẫu nhiên và độ dài tối thiểu là 128-bit.</p> <p>- Session phải được thiết lập thời gian timeout, giá trị timeout nên cân bằng giữa nhu cầu thương mại và yếu tố bảo mật.</p> <p>- Tạo mới session sau khi đăng nhập thành công.</p> <p>- Xóa giá trị session id và các dữ liệu gắn với session đó khi người dùng đăng xuất.</p> <p>- Cấu hình thuộc tính “Secure” đối với các ứng dụng sử dụng HTTPS và “HTTP-Only” cho trường Cookie.</p> <p>- Đối với các chức năng quan trọng có tương tác với database, ứng với mỗi phiên phải sinh thêm 1 token ngẫu nhiên, và thực hiện kiểm tra tính hợp lệ của token này trước khi xử lý truy vấn từ người dùng.</p>	Bảo vệ phiên đăng nhập của người dùng	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 02.	OWASP Secure Coding Practices: “Session Management”

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Phân quyền	<ul style="list-style-type: none"> - Kiểm tra phân quyền dựa trên các đối tượng được lưu tại server (ví dụ: tham số lưu trên session server, dữ liệu lưu trên DB,...). - Phân quyền tối thiểu, chỉ đáp ứng đủ chức năng và tài nguyên cho người dùng/ứng dụng. - Phía giao diện người dùng: Chỉ hiển thị các thành phần giao diện, đường dẫn, hàm,... tương ứng với quyền của người dùng. - Phía server: Kiểm tra quyền tác động của người dùng/ứng dụng trên các hàm và tài nguyên tương ứng trước khi thực hiện bất cứ tác vụ nào tới hệ thống. - Nên có tính năng xóa phiên làm việc hiện tại của người dùng hoặc các cơ chế tương đương đối với các trường hợp quyền người dùng bị thay đổi hoặc bị disable bởi người dùng có thẩm quyền. - Không đặt trang quản trị public internet, trong trường hợp bắt buộc phải đặt public phải giới hạn các IP được phép truy cập hoặc sử dụng cơ chế xác thực đa nhân tố. 	Bảo vệ dữ liệu của ứng dụng	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 02.	OWASP Coding Mục Control” Secure Practices: ”Access

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Mã hóa các dữ liệu nhạy cảm	Đối với các loại dữ liệu nhạy cảm như thông tin tài khoản ngân hàng, private key... phải thực hiện mã hóa trước khi lưu trữ, sử dụng thuật toán AES-256 hoặc các thuật toán tương đương.	Bảo vệ các dữ liệu nhạy cảm	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 02.	OWASP Secure Coding Practices: Mục "Cryptographic Practices"
Tương tác với back-end - SQL	<ul style="list-style-type: none"> - Sử dụng mô hình truy vấn prepared statement (parameterized query) hoặc các hình thức tương đương. - Trong 1 số trường hợp không sử dụng được các mô hình ở trên, phải thiết lập danh sách whitelist các đầu vào mong muốn. 	Đảm bảo việc truy cập dữ liệu bằng SQL an toàn	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 02.	OWASP Secure Coding Practices: Mục "Database Security"
Tương tác với back-end - NoSQL	<ul style="list-style-type: none"> - Không công khai dịch vụ ra mạng internet, cài đặt trong môi trường mạng an toàn. - Đối với các hệ NoSQL có hỗ trợ xác thực, phải cấu hình xác thực khi truy cập. - Phụ thuộc vào hệ NoSQL sử dụng, sử dụng các api hỗ trợ truy vấn an toàn hoặc thực hiện escape các ký tự đặc biệt khi xây dựng câu truy vấn. 	Đảm bảo việc truy cập dữ liệu bằng NoSQL an toàn	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 02.	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Tương tác với back-end - XPath	<ul style="list-style-type: none"> - Thiết lập danh sách whitelist các ký tự đầu vào mong muốn, đầu vào nên là tập hợp của chữ cái, chữ số. - Lập danh sách blacklist các ký tự đặc biệt (() = ' [] : , * / và dấu cách), loại bỏ các đầu vào có chứa các ký tự nằm trong blacklist. 	Đảm bảo việc truy cập dữ liệu bằng XPath an toàn	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 02.	
Tương tác với back-end - LDAP	<ul style="list-style-type: none"> - Thiết lập danh sách whitelist các ký tự đầu vào mong muốn, đầu vào nên là tập hợp của chữ cái, chữ số. - Lập danh sách blacklist các ký tự đặc biệt (() ; , * & = và nullbyte), loại bỏ các đầu vào có chứa các ký tự nằm trong blacklist. 	Đảm bảo việc truy cập dữ liệu bằng LDAP an toàn	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 02.	
Tương tác với back-end - Tương tác với OS	<ul style="list-style-type: none"> - Sử dụng các API hỗ trợ việc thực thi câu lệnh hệ thống. - Không truyền trực tiếp dữ liệu người dùng truyền lên tới OS, trong trường hợp bắt buộc phải thiết lập danh sách whitelist các đầu vào mong muốn. 	Đảm bảo việc tương tác với OS	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 02.	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Tương tác với back-end - Tương tác với file	<ul style="list-style-type: none"> - Không truyền trực tiếp dữ liệu từ người dùng đến các hàm include file. - Lập danh sách whitelist các định dạng file được phép upload tùy theo nghiệp vụ hệ thống (khuyến nghị các loại file như docx, xlsx, pdf, png, jpg). Validate file hợp lệ này bằng cách kiểm tra phần mở rộng của file tương ứng với whitelist định dạng file được upload. - Với các trường hợp không bắt buộc thì không lưu file upload trong thư mục web, bỏ quyền thực thi trên thư mục upload. - Khi cần ánh xạ tới các file tồn tại trên hệ thống phải thiết lập danh sách whitelist đầu vào mong muốn hoặc gán các giá trị định danh tương ứng file thay vì truyền tên file. - Không trả về đường dẫn tuyệt đối của file. - Tất cả dữ liệu, tài nguyên hệ thống (báo cáo, file upload, file cấu hình...) không được lưu trong thư mục cho phép truy cập trực tiếp không qua xác thực. 	Đảm bảo việc tương tác với file	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 02.	
Tương tác với back-end - Xử lý	<ul style="list-style-type: none"> - Khi tạo HTTP request phía server, các tham số GET, POST cho request đó tránh tạo từ dữ liệu phía người dùng, hoặc phải được kiểm 	Đảm bảo việc Xử lý back-end	Phụ lục 02	Kiểm tra mã nguồn ứng dụng	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
back-end HTTP request	tra cẩn thận để chống ghi đè các tham số khác. - Không lấy địa chỉ server từ dữ liệu người dùng gửi lên. Trong trường hợp địa chỉ server cần lấy từ người dùng, phải blacklist các IP trong dải nội bộ sau khi đã phân giải DNS.	HTTP request an toàn		theo hướng dẫn tại Phụ lục 02.	
Tương tác với back-end - XML	- Tắt tính năng “external entity resolve” và “remote doctype retrieval” của xml parser khi đọc dữ liệu xml. - Kiểm tra dữ liệu người dùng, encode các kí tự đặc biệt (< > ' ") khi tạo dữ liệu xml.	Đảm bảo việc truy cập dữ liệu bằng XML an toàn	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 02.	
Tương tác với back-end - deserialize	- Khuyến nghị chỉ thực hiện deserialize các dữ liệu từ các nguồn tin cậy, an toàn hoặc sử dụng kiểu dữ liệu json. - Các trường hợp nằm ngoài mục 4.10.1 phải thực hiện thêm 1 trong 2 tác vụ sau: ▪ Sinh 1 mã bí mật (S) và lưu tại server. Khi cần gửi dữ liệu đã được serialize (D), gửi kèm mã hash được tính theo công thức: $H = \text{hash}(D+S)$.	Đảm bảo việc thực hiện deserialize an toàn	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 02.	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	<ul style="list-style-type: none"> Khi cần deserialize dữ liệu D, thực hiện sinh mã $H1 = \text{hash}(D+S)$, nếu H và H1 trùng khớp mới thực hiện deserialize D. Thiết lập whitelist các class được deserialize. Kiểm tra tên các class trong phần dữ liệu, nếu các class này thuộc whitelist mới thực hiện deserialize dữ liệu. 				
Kiểm soát dữ liệu đầu vào	<ul style="list-style-type: none"> - Việc kiểm tra dữ liệu đầu vào phải được thực hiện phía server. - Thực hiện việc kiểm tra dữ liệu từ tất cả các nguồn dữ liệu có tương tác với người dùng (Các tham số lấy từ GET/POST request, HTTP Headers, dữ liệu lấy từ DB, dữ liệu từ file upload,...). - Xác định 1 kiểu encoding nhất quán sử dụng khi hiển thị, trao đổi hay lưu trữ dữ liệu. Chỉ thực hiện filter, validate dữ liệu sau khi đã đưa dữ liệu về kiểu encoding đã xác định trước đó. - Validate kiểu dữ liệu, phạm vi, kích thước dữ liệu và định dạng dữ liệu. - Nếu dữ liệu đầu vào bắt buộc là các ký tự đặc biệt, phải thiết lập danh sách whitelist các ký tự đầu vào mong muốn. 	Đảm bảo dữ liệu đầu vào an toàn	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 02.	OWASP Coding Mục Validation” Secure Practices: ”Input

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Kiểm soát dữ liệu đầu ra	<ul style="list-style-type: none"> - Phải chỉ rõ character encoding cho dữ liệu đầu ra. - Phải thiết lập giá trị Content-type tương ứng với định dạng dữ liệu trả về (ví dụ dữ liệu json phải tương ứng với Content-type là application/json) - Response body phải được encode theo ngữ cảnh sử dụng. Ví dụ: Đầu ra là html, thực hiện html encode các ký tự đặc biệt (<>'"&) từ các nguồn dữ liệu không an toàn (Các tham số lấy từ GET/POST request, HTTP Headers, dữ liệu lấy từ DB, dữ liệu từ file upload,... có thể điều khiển được bởi người dùng). - Response header: lọc bỏ các ký tự đặc biệt (\n, \r) do dữ liệu người dùng truyền vào. - Cookie trả về phải giới hạn tối thiểu nhất các thuộc tính (domain, path, httponly, expire, secure). Tránh lưu trữ các dữ liệu nhạy cảm trên cookie, nếu cần lưu trữ các dữ liệu nhạy cảm thì phải thực hiện mã hóa các dữ liệu này với thuật toán đối xứng mạnh và key chỉ được lưu trên server. - Hạn chế việc chuyển hướng, chuyển tiếp đến các URI khác. Nếu ứng dụng có chức 	Đảm bảo dữ liệu đầu ra an toàn	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 02.	OWASP Coding Mục Encoding” Secure Practices: ”Output

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	năng này phải lập danh sách whitelist các địa chỉ server được phép thực hiện chuyển hướng, chuyển tiếp.				
Kiểm soát ngoại lệ và ghi log ứng dụng	<ul style="list-style-type: none"> - Xử lý các ngoại lệ bằng try-catch và trả về các thông báo lỗi chung, thông báo lỗi trả về không được chứa các thông tin nhạy cảm của người dùng, hệ thống,... - Các thông tin lỗi, ngoại lệ này phải được log lại để phục vụ bảo trì, xác định nguyên nhân lỗi ứng dụng. - File log phải được đặt tại thư mục an toàn ngoài thư mục web. - Không log lại các dữ liệu nhạy cảm (thông tin người dùng, session id, thông tin hệ thống). - Giới hạn người dùng cho phép truy cập file log. 	Đảm bảo ghi log an toàn	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 02.	OWASP Secure Coding Practices: Mục "Error Handling and Logging"
Sử dụng framework, thư viện (third-party component)	<ul style="list-style-type: none"> - Loại các code thừa, các thành phần và thư viện không cần thiết. - Sử dụng phiên bản mới nhất của framework, thư viện tại thời điểm phát triển ứng dụng. 	Đảm bảo sử dụng framework an toàn	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn	OWASP Secure Coding Practices: Mục "System Configuration"

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	<ul style="list-style-type: none"> - Thường xuyên cập nhật các bản vá lỗi cho framework, thư viện. - Tắt chế độ development của framework khi triển khai ứng dụng thực tế. 			tại Phụ lục 02.	
Xử lý business logic	<ul style="list-style-type: none"> - Lập trình viên phải nắm rõ được toàn bộ luồng nghiệp vụ của ứng dụng, phải xác định các ngoại lệ cho từng nghiệp vụ để tránh các lỗi logic có thể xảy ra. - Các chức năng quan trọng (ví dụ chuyển khoản ngân hàng), sử dụng các hình thức khóa hoặc các hình thức tương đương để tránh lỗi race condition. - Đối với các dịch vụ viễn thông, khi khách hàng đăng ký các dịch vụ các dịch vụ gia tăng trên điện thoại di động (VAS) phải có tin nhắn thông báo tới khách hàng. - Đối với các giao dịch chuyển tiền, ví dụ chuyển từ tài khoản A sang tài khoản B: phải thực hiện trừ tiền tài khoản A thành công rồi mới được thực hiện cộng tiền vào tài khoản B. - Đối với các ứng dụng có chức năng gửi tin nhắn tới người dùng phải giới hạn số lần gửi tin trong 1 ngày ứng với mỗi đầu số nhận tin. 	Đảm bảo xử lý logic an toàn	Phụ lục 02	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 02.	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	<p>Đối với chức năng quan trọng như đăng ký, lấy lại mật khẩu chỉ cho phép gửi ≤ 3 tin/ngày.</p> <p>- Yêu cầu khi sử dụng và sinh mã OTP:</p> <ul style="list-style-type: none"> ● Giới hạn số lần nhập sai với mỗi mã OTP ≤ 3 lần/ngày, xóa mã cũ và sinh mã mới khi nhập sai vượt quá số lần cho phép. ● Không được sử dụng mã OTP làm mật khẩu. 				

Điều 9. Quy tắc lập trình an toàn sử dụng ứng dụng C/C++

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Thiết lập biên dịch an toàn	<ul style="list-style-type: none"> - Biên dịch với tùy chọn chống ghi đè bộ đệm (buffer overflow) - Biên dịch với tùy chọn chống khai thác qua SEH - Biên dịch với tùy chọn DEP - Biên dịch với tùy chọn ASLR - Bật mức cảnh báo (warning) khi biên dịch phù hợp. 	Đảm bảo trình biên dịch build với các tùy chọn an toàn giúp ngăn nguy cơ xảy ra lỗ hổng cũng như ngăn khả năng khai thác thành công lỗ hổng nếu có	Phụ lục 03	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 03.	Secure Coding in C and C++
Bảo vệ ứng dụng an toàn khỏi các lỗi bộ nhớ	<ul style="list-style-type: none"> - Tránh lỗi tràn bộ đệm (buffer overflow) - Tránh lỗi tràn số nguyên (integer overflow) - Tránh lỗi sử dụng định dạng xâu (format string) - Tránh lỗi sử dụng vùng nhớ sau khi giải phóng 	Phòng tránh phần mềm khỏi các lỗi bộ nhớ phổ biến	Phụ lục 03	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại	Secure Coding in C and C++

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
				Phụ lục 03.	
Bảo vệ ứng dụng an toàn khi thao tác với đối tượng tài nguyên	<ul style="list-style-type: none"> - Tránh lỗi tranh chấp tài nguyên (race-condition) và lỗi deadlock - Tránh lỗi khi truy nhập file - Sử dụng đường dẫn tuyệt đối khi nạp thư viện động - Truy nhập đúng quyền khi thao tác với các đối tượng tài nguyên, tránh sử dụng tài nguyên với quyền lớn hơn nhu cầu cần thiết - Tránh lỗi leak tài nguyên hệ thống 	Phòng tránh phần mềm khỏi các lỗi khi truy cập các đối tượng tài nguyên của hệ thống như file, thư viện, memory,...	Phụ lục 03	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 03.	Secure Coding in C and C++
Bảo mật khi giao tiếp, xác thực, phân quyền ứng dụng	<ul style="list-style-type: none"> - Sử dụng giao thức an toàn - Xác thực an toàn đảm bảo các yếu tố mã hóa mạnh, và sử dụng giao thức an toàn - Phân quyền người dùng an toàn 	Đảm bảo an toàn cho dữ liệu khi giao tiếp, xác thực, phân quyền ứng dụng	Phụ lục 03	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 03.	https://cwe.mitre.org/data/definitions/311.html https://cwe.mitre.org/data/definitions/306.html https://cwe.mitre.org/data/definitions/287.html https://cwe.mitre.org/data/definitions/285.html

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Khuyến cáo bổ sung	<ul style="list-style-type: none"> - Sử dụng an toàn biến môi trường, hạn chế cho người dùng tác động vào biến môi trường chạy của chương trình - Kiểm tra giá trị hàm trả về trước khi tiếp tục xử lý - Không kết nối trực tiếp từ ứng dụng client đến server database tập trung, cần xây dựng server xử lý trung gian đảm bảo có xác thực, phân quyền theo từng tài khoản người dùng - Sử dụng các công cụ phân tích mã nguồn để phát hiện các lỗi lập trình - Không sử dụng các hàm bị đánh dấu obsolete - Sửa hết cảnh báo (warning) khi biên dịch chương trình - Tránh khai báo các mảng tĩnh có kích thước lớn trong hàm - Đảm bảo máy tính lập trình tuân thủ các Quy tắc ATTT cho máy tính người dùng cuối 	<p>Các yêu cầu bổ sung nhằm đảm bảo môi trường an toàn khi phát triển phần mềm cũng như các bước kiểm tra bổ sung để đảm bảo an toàn cho hệ thống</p>	Phụ lục 03	<p>Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 03.</p>	SEI CERT C Coding Standard

Điều 10. Quy tắc lập trình an toàn cho ứng dụng mobile

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Bảo vệ các dữ liệu được lưu trữ trên di động	<ul style="list-style-type: none"> - Không sử dụng tính năng ghi nhớ mật khẩu đối với các ứng dụng quan trọng, có chứa các thông tin nhạy cảm như: các ứng dụng liên quan đến tài chính, ngân hàng, thanh toán điện tử, các ứng dụng nội bộ truy cập vào các hệ thống quan trọng ... - Phân quyền, mã hóa dữ liệu lưu trữ trên thiết bị. - Bảo vệ dữ liệu nhạy cảm khi ứng dụng chạy chế độ nền 	<ul style="list-style-type: none"> - Bảo vệ các dữ liệu nhạy cảm của người dùng, tổ chức trên thiết bị. 	Phụ lục 04	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 04.	<ul style="list-style-type: none"> - Application Security for the Android Platform. - Hacking and Securing iOS Applications. - Mobile Application Security.
Bảo mật giao tiếp giữa ứng dụng và máy chủ	<ul style="list-style-type: none"> - Các thông tin quan trọng khi truyền giữa ứng dụng và máy chủ phải được mã hóa (Có thể sử dụng các giao thức HTTPS, SSL/TLS). - Khi sử dụng HTTPS, SSL phải kiểm tra trusted root CA, thời hạn hết hạn và CN tương ứng với domain. 	<ul style="list-style-type: none"> - Chống tấn công theo dõi dữ liệu trên đường truyền, chỉnh sửa làm sai lệch dữ liệu. - Hạn chế việc lấy các API của ứng dụng, giảm nguy cơ tấn công 	Phụ lục 04	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 04.	<ul style="list-style-type: none"> - Application Security for the Android Platform. - Hacking and Securing iOS Applications. - Mobile Application Security.

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
		công lên server.			
Bảo mật xác thực người dùng	<ul style="list-style-type: none"> - Áp dụng chính sách mật khẩu mạnh đối với những ứng dụng nội bộ theo quy định về mật khẩu mạnh của đơn vị, với các ứng dụng khác, cần khuyến cáo người dùng sử dụng mật khẩu mạnh. - Bảo mật trong lưu trữ mật khẩu trên thiết bị. - Áp dụng xác thực đa yếu tố khi truy cập vào các hệ thống quan trọng. 	<ul style="list-style-type: none"> - Giảm nguy cơ tấn công bằng cách quét mật khẩu của người dùng. - Giảm nguy cơ bị tấn công khi người dùng lộ tên tài khoản, mật khẩu. 	Phụ lục 04	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 04.	<ul style="list-style-type: none"> - Application Security for the Android Platform. - Hacking and Securing iOS Applications. - Mobile Application Security.
Bảo vệ tấn công phía client	<ul style="list-style-type: none"> - Sử dụng Prepare-Statement tránh lỗi Sql injection - Lập trình an toàn ngăn chặn lỗi XSS - Lập trình an toàn ngăn chặn lỗi Tapjacking - Lập trình an toàn ngăn chặn lỗi khi thao tác với file 	<ul style="list-style-type: none"> - Chống ứng dụng bị tấn công khi người dùng nhiễm mã độc hoặc kẻ tấn công có được thiết bị của người dùng. 	Phụ lục 04	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 04.	<ul style="list-style-type: none"> - Application Security for the Android Platform. - Hacking and Securing iOS Applications. - Mobile Application Security.

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Lập trình an toàn với việc xử lý thông tin logs và debugger	<ul style="list-style-type: none"> - Tắt chức năng debug của ứng dụng - Không lưu các thông tin nhạy cảm như tên truy cập và mật khẩu vào trong logs. - Xóa bỏ các thông tin thừa trong code trước khi xuất bản chương trình. 	<ul style="list-style-type: none"> - Ngăn lộ lọt thông tin nhạy cảm của người dùng khi kết nối thiết bị với các thiết bị khác. - Ngăn lộ lọt thông tin nhạy cảm khi ứng dụng bị dịch ngược. 	Phụ lục 04	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 04.	<ul style="list-style-type: none"> - Application Security for the Android Platform. - Hacking and Securing iOS Applications. - Mobile Application Security.
Lưu ý khi sử dụng framework, thư viện do bên thứ 3 cung cấp.	<ul style="list-style-type: none"> - Loại các code thừa, các thành phần và thư viện không cần thiết. - Sử dụng phiên bản mới nhất của framework, thư viện tại thời điểm phát triển ứng dụng. - Thường xuyên cập nhật các bản vá lỗi cho framework, thư viện. - Tắt chế độ development của framework khi triển khai ứng dụng thực tế. 	<ul style="list-style-type: none"> - Giảm thiểu nguy cơ xuất phát từ các lỗ hổng do thư viện của các bên thứ 3 cung cấp 	Phụ lục 04	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 04.	<ul style="list-style-type: none"> - Application Security for the Android Platform. - Hacking and Securing iOS Applications. - Mobile Application Security.

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Bảo vệ mã nguồn của chương trình	<ul style="list-style-type: none"> - Không hardcode các thông tin quan trọng như (keys, username/password...) - Sử dụng kỹ thuật làm nhiễu mã nguồn, biên dịch an toàn trước khi release chương trình. 	<ul style="list-style-type: none"> - Hạn chế việc dịch ngược mã nguồn ứng dụng, có thể lấy được các thông tin nhạy cảm. 	Phụ lục 04	Kiểm tra mã nguồn ứng dụng theo hướng dẫn tại Phụ lục 04.	<ul style="list-style-type: none"> - Application Security for the Android Platform. - Hacking and Securing iOS Applications. - Mobile Application Security.

CHƯƠNG IV. BỘ QUY TẮC CẤU HÌNH ATTT CHO HỆ THỐNG

Điều 11. Quy tắc cấu hình ATTT cho hệ điều hành máy chủ

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Cài đặt và cập nhật Hệ điều hành (HĐH)	<ul style="list-style-type: none"> - Cài đặt phiên bản HĐH mới nhất để đảm bảo HĐH đang được hãng support, update. - Cập nhật bản vá, đảm bảo không mắc các lỗ hổng bảo mật đã được công bố nhằm tránh bị tấn công qua các lỗ hổng 1-days. 	<ul style="list-style-type: none"> - Đảm bảo việc cài đặt được an toàn. 	Phụ lục 05	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 05.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 4.1

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Tắt/disable các thành phần không sử dụng	- Yêu cầu tắt/disable các dịch vụ, ứng dụng, giao thức mạng không sử dụng nhằm tránh việc bật các dịch vụ không sử dụng, hacker có thể lợi dụng để tấn công vào hệ thống.	- Đảm bảo các thành phần không sử dụng không ảnh hưởng đến vấn đề ATTT.	Phụ lục 05	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 05.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 4.2.1
Thiết lập chính sách tài khoản	- Xóa hoặc vô hiệu hóa các tài khoản không sử dụng trên hệ thống. Bởi, các tài khoản không sử dụng có thể bị lợi dụng để hacker có thể xâm nhập hệ thống. - Đổi tên tài khoản mặc định (HĐH Windows) nhằm tránh nguy cơ bị tấn công brute force password với các username mặc định như administrator, guest... - Mật khẩu được đặt theo yêu cầu tại quy định chính sách mật khẩu mạnh hiện hành của EVN ban hành.	- Đảm bảo an toàn cho tài khoản của hệ thống.	Phụ lục 05	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 05.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 4.2.2 và kết quả nghiên cứu tình hình thực tiễn.
Quản trị từ xa	- Yêu cầu quản trị từ xa phải sử dụng kênh truyền có mã hóa: + Trên Windows: sử dụng dịch vụ Remote Desktop.	- Đảm bảo an toàn trong việc quản trị	Phụ lục 05	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 05.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 5.2 và kết quả

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	<ul style="list-style-type: none"> + Trên Linux/Unix: sử dụng dịch vụ SSH. - Cấu hình giới hạn các tài khoản được phép sử dụng dịch vụ quản trị từ xa, không cho phép các user super administrator có quyền này. Giới hạn theo whitelist danh sách các user được phép quản trị từ xa. - Giới hạn số lần tài khoản đăng nhập sai là 05 lần, nếu vi phạm bị chặn trong 05 phút để tránh hacker lợi dụng để brute force password của một account nhiều lần. - Giới hạn thời gian tự động ngắt phiên khi không có hoạt động trong một khoảng thời gian là 05 phút nhằm giảm rủi ro khi hacker chiếm được quyền điều khiển của máy quản trị và có thể remote vào các server đã được thiết lập sẵn phiên kết nối trước đó. 				<p> nghiên cứu tình hình thực tiễn.</p>

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Phân quyền tệp tin trên Linux/Unix	<ul style="list-style-type: none"> - Biến môi trường \$PATH không được chứa các đường tương đối, đường dẫn bất thường, đường dẫn trống. Bởi, hacker có thể đặt các file thực thi vào các đường dẫn này để thay thế các lệnh mặc định trên hệ thống. Từ đó lợi dụng người dùng để thực thi các shell script. - Giới hạn theo whitelist các tài khoản được phép chạy dịch vụ CRON nhằm tránh việc hacker lợi dụng các account chiếm quyền được để chạy các job theo ý muốn trên hệ thống. - Hạn chế quyền sửa các file cấu hình của CRON nhằm tránh việc hacker có thể sửa nội dung file CRON để thực thi các job trên hệ thống. 	- Đảm bảo an toàn cho dữ liệu của hệ thống	Phụ lục 05	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 05.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 5.3 và kết quả nghiên cứu tình hình thực tiễn.
Yêu cầu về Firewall mềm	<ul style="list-style-type: none"> - Yêu cầu sử dụng firewall mềm trên hệ thống: - Trên Windows: sử dụng Windows Firewall. 	- Đảm bảo việc truy cập được an toàn.	Phụ lục 05	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 05.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 3.1, 6.5 và kết

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	<ul style="list-style-type: none"> - Trên Linux/Unix: sử dụng iptables. - Giới hạn địa chỉ IP quản trị được phép truy cập đến máy chủ. Tùy thuộc vào dải mạng, ip của quản trị viên để thiết lập giới hạn IP được phép truy cập quản trị từ xa đến máy chủ được quản lý. Trong trường hợp dùng máy trung gian để truy cập vào máy chủ hệ thống cần giới hạn địa chỉ IP của từng quản trị viên truy cập đến máy trung gian. - Cấu hình tường lửa mềm chỉ mở cho phép với các dịch vụ phục vụ trên máy chủ, chặn các kết nối còn lại. Dựa vào các dịch vụ đang chạy trên hệ thống để xác định các port cần kết nối theo Inbound, Outbound, Forward và thiết lập chặn mặc định. 				quả nghiên cứu tình hình thực tiễn.
Chính sách quản lý log	- Ghi log mặc định của hệ điều hành để đảm bảo đủ log cho việc	- Đảm bảo việc ghi log đầy đủ,	Phụ lục 05	Kiểm tra cấu hình theo	Kế thừa tiêu chuẩn NIST SP 800-123: mục 6.1.

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	<p>forensic khi có dấu hiệu hệ thống bị tấn công.</p> <ul style="list-style-type: none"> - Cấu hình thời gian lưu log tối thiểu là 3 tháng để đảm bảo log được lưu trong thời gian đủ lâu cho quá trình forensic. - Đồng bộ thời gian HĐH về máy chủ tập trung để đảm bảo thông tin về thời gian trong các file log là chính xác. 	phục vụ điều tra sự cố.		hướng dẫn tại Phụ lục 05.	
Cài đặt các hệ thống bảo vệ và giám sát hệ thống	<ul style="list-style-type: none"> - Cài đặt, sử dụng phần mềm diệt virus (HĐH Windows) ở chế độ bảo vệ và cập nhật các mẫu diệt virus mới hàng ngày. - Trường hợp đơn vị có giám sát bằng SNMP cần cấu hình để được giám sát bằng hệ thống SNMP tập trung. 	- Đảm bảo phát hiện sớm các vấn đề ATTT trên hệ thống.	Phụ lục 05	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 05.	
Yêu cầu môi trường vận hành an toàn	<ul style="list-style-type: none"> - User remote quản trị hệ thống phải enable cơ chế xác thực đa nhân tố (token/OTP). - Sử dụng 1 máy riêng đảm bảo toàn bộ các tiêu chuẩn ATTT cho 	- Đảm bảo môi trường vận hành hệ thống an toàn.	Phụ lục 05	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 05.	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	<p>máy người dùng cuối để vận hành hệ thống .</p> <p>- Sử dụng các máy riêng để vận hành hệ thống, không dùng cho các công việc thông thường hàng ngày (Duyệt email, truy cập internet, đọc file văn bản MSOffice/pdf.</p>				

Điều 12. Quy tắc cấu hình ATTT cho Web server

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Yêu cầu về cài đặt	Yêu cầu cài đặt trên hệ điều hành an toàn, đã được thiết lập cấu hình chính sách bảo mật theo Quy tắc ATTT cho HĐH máy chủ.	- Đảm bảo việc cài đặt được an toàn	Phụ lục 06, Phụ lục 07	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 06, Phụ lục 07	Kế thừa tiêu chuẩn NIST SP 800-44: mục 4.1, 5.1
Tắt/disable các thành phần mặc định	<ul style="list-style-type: none"> - Gỡ bỏ các thư mục/trang mặc định như: các trang ví dụ, hướng dẫn, các trang quản trị web server từ xa, các trang phục vụ dev, debug nhằm tránh bị khai thác lỗ hổng qua các nội dung web mặc định. - Tắt các Module/Extension nguy hiểm không sử dụng như: các module hiển thị thông tin server (module info, status, version), hiển thị nội dung thư mục, các module xử lý CGI, xử lý webdav nhằm tránh bị khai thác các module extension không sử dụng. - Tắt chế độ AutoDeploy/Debug trên web 	- Đảm bảo các thành phần không sử dụng không ảnh hưởng đến vấn đề ATTT.	Phụ lục 06, Phụ lục 07	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 06, Phụ lục 07	Kế thừa tiêu chuẩn NIST SP 800-44: mục 5.1

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	server (nếu có). Chế độ AutoDeploy/ Debug trên web server có thể đưa ra nhiều thông tin nhạy cảm hoặc gây mất kiểm soát về security.				
Giới hạn truy cập	<ul style="list-style-type: none"> - Chỉ truy cập quản trị từ xa trong mạng nội bộ của doanh nghiệp và có phương thức xác thực người dùng. Hacker có thể chiếm quyền kiểm soát dịch vụ web qua kênh quản trị từ xa từ ngoài internet. Do đó cần cô lập các kết nối quản trị từ xa và có các phương thức xác thực người dùng như: sử dụng username/password, OTP, private key... - Không cho phép liệt kê file, thư mục. Hacker có thể phát hiện ra các file, thư mục nhạy cảm của hệ thống. - Đối với trường hợp cần cấu hình cho phép domain khác truy cập nội dung (Cross-origin 	- Đảm bảo an toàn cho tài khoản của hệ thống	Phụ lục 06, Phụ lục 07	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 06, Phụ lục 07	Kế thừa tiêu chuẩn NIST SP 800-44: mục 5.2 .

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	resource sharing – CORS), chỉ được thêm từng domain, không được thêm nhóm domain hoặc tất cả domain nhằm tránh bị tấn công qua phương thức CORS.				
Yêu cầu về phân quyền an toàn	<ul style="list-style-type: none"> - Chạy tiến trình web server với tài khoản user được giới hạn quyền (không phải tài khoản quản trị hoặc có quyền tương đương). Khi hacker chiếm được quyền kiểm soát web sẽ chỉ có quyền tối thiểu và không thể nâng quyền, chiếm quyền trên toàn bộ hệ thống. - Không cho phép thực thi các câu lệnh CGI, SSI nhằm tránh việc hacker lợi dụng các script CGI, SSI để thực thi các câu lệnh tương tác với hệ thống. 	- Đảm bảo an toàn cho dữ liệu	Phụ lục 06, Phụ lục 07	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 06, Phụ lục 07	Kế thừa tiêu chuẩn NIST SP 800-44: mục 5.2.1, 5.2.2
Sử dụng mã hóa SSL	- Không sử dụng SSL version 2.0, SSL version 3.0 do SSL có lỗi bảo mật không thể khắc phục được và đã không được hỗ trợ nâng cấp từ năm 2015. Cần	- Đảm bảo an toàn trên đường truyền	Phụ lục 06, Phụ lục 07	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 06, Phụ lục 07	Kế thừa tiêu chuẩn NIST SP 800-44: mục 7.5

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	<p>chuyển đổi sử dụng từ SSL sang TLS.</p> <p>- Không sử dụng các SSLCipherSuite không an toàn: EXPORT, NULL, MD5, DES, RC4. Đây là các thuật toán mã hóa yếu, có thể bị giải mã.</p>				
Chính sách quản lý log	<p>- Thiết lập chế độ ghi log, ghi luân phiên/xoay vòng log file theo ngày nhằm tránh việc file log lưu quá lớn, khó truy vết, điều tra theo người dùng.</p> <p>- Định dạng dữ liệu log phải có đủ thông tin phục vụ cho việc điều tra, truy vết vi phạm ATTT để đảm bảo ghi log lại các thông tin quá trọng của người dùng, bao gồm: Client IP, X-Forwarded-For, Data/time, Request, Status, Bytes Send, HTTP Referer, User Agent.</p>	<p>- Đảm bảo log được ghi đầy đủ, sử dụng trong các trường hợp điều tra sự cố</p>	Phụ lục 06, Phụ lục 07	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 06, Phụ lục 07	Kế thừa tiêu chuẩn NIST SP 800-44: mục 9.1

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	<ul style="list-style-type: none"> - Lưu trữ tối thiểu 3 tháng, có thể lưu trữ tập trung hoặc trực tiếp trên máy chủ để đảm bảo thông tin log đủ lâu phục vụ cho forensic. 				
Yêu cầu cho web server PHP	<ul style="list-style-type: none"> - Ngăn chặn Remote code Execute. Chặn hacker có thể thực hiện RCE qua web. - Giới hạn thư mục PHP truy cập để tránh việc hacker có thể local file từ các thư mục khác không phải thư mục web root. - Vô hiệu hóa các hàm thực thi tới hệ thống không cần thiết, bao gồm: exec, passthru, shell_exec, system, proc_open, popen, curl_exec, curl_multi_exec, parse_ini_file, show_source, symlink, tránh việc gọi trực tiếp các hàm thực thi với hệ thống. Từ đây hacker có thể lợi dụng những hàm này để chiếm quyền điều khiển máy chủ. 	- Đảm bảo an toàn trường hợp sử dụng PHP	Phụ lục 06, Phụ lục 07	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 06, Phụ lục 07	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	- Tắt chế độ hiển thị thông tin lỗi của php để tránh để lộ các thông tin lỗi quan trọng, nhạy cảm như tên file, thư mục web, thông tin lỗi...				
Yêu cầu cho web server chạy ASP.NET (IIS)	- Cấu hình validate dữ liệu để hạn chế tấn công XSS. - Tắt chế độ debug nhằm tránh bị khai thác, để lộ các thông tin nhạy cảm qua chế độ debug của các web.	- Đảm bảo an toàn trường hợp sử dụng Aspx	Phụ lục 06, Phụ lục 07	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 06, Phụ lục 07	.
Yêu cầu môi trường vận hành an toàn	- User remote quản trị hệ thống phải enable cơ chế xác thực đa nhân tố (token/OTP). - Sử dụng 1 máy riêng đảm bảo toàn bộ các tiêu chuẩn ATTT cho máy người dùng cuối để vận hành hệ thống . - Sử dụng các máy riêng để vận hành hệ thống, không dùng cho các công việc thông thường hàng ngày (Duyệt email, truy cập internet, đọc file văn bản MSOffice/pdf.	- Đảm bảo môi trường vận hành hệ thống an toàn	Phụ lục 06, Phụ lục 07	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 06, Phụ lục 07	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Quản trị từ xa	Thiết lập an toàn cho quản trị từ xa theo Quy tắc ATTT hệ điều hành máy chủ.	- Đảm bảo an toàn trong việc quản trị	Tham khảo theo Quy tắc cấu hình ATTT hệ điều hành máy chủ.	Tham khảo theo Quy tắc cấu hình ATTT hệ điều hành máy chủ.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 5.2 và kết quả nghiên cứu tình hình thực tiễn.

Điều 13. Quy tắc cấu hình ATTT cho hệ quản trị CSDL

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Yêu cầu về việc cài đặt hệ quản trị CSDL an toàn	<ul style="list-style-type: none"> - Cài đặt phiên bản HĐH an toàn. Hệ quản trị CSDL phải được cài đặt trên hệ điều hành an toàn, đã được thiết lập cấu hình chính sách bảo mật đảm bảo theo Quy tắc ATTT cho Hệ điều hành máy chủ. - Cài đặt phiên bản Hệ quản trị CSDL an toàn. Phiên bản cài đặt phải là phiên bản vẫn duy trì các bản vá cập nhật bởi nhà sản xuất, được cập nhật bản vá và đảm bảo không mắc các lỗ hổng bảo mật đã được công bố. 	<ul style="list-style-type: none"> - Đảm bảo việc cài đặt được an toàn 	Phụ lục 08	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 08.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 4.1
Yêu cầu về việc gỡ bỏ/tắt các thành phần thừa, thành phần không sử dụng	<ul style="list-style-type: none"> - Xóa hoặc khóa các tài khoản, các CSDL thừa, không sử dụng. Các tài khoản, các CSDL thừa có thể tiềm ẩn các nguy cơ ATTT. Các tài khoản, CSDL thừa, không sử dụng là các tài khoản, CSDL không có trong kế hoạch sử dụng của Hệ quản trị CSDL. - Khuyến cáo nên tắt các hàm tương tác với tài nguyên hệ điều hành (hàm 	<ul style="list-style-type: none"> - Đảm bảo các thành phần không sử dụng không ảnh hưởng đến vấn đề ATTT. 	Phụ lục 08	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 08.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 5.1 và kết quả nghiên cứu ATTT áp dụng trên hệ quản trị cơ sở dữ liệu.

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	đọc, ghi file, thực thi câu lệnh hệ thống) nhằm tránh việc truy cập tới các tài nguyên hệ điều hành, cũng như thực thi các lệnh hệ thống thông qua các truy vấn tới CSDL.				
Yêu cầu thiết lập chính sách tài khoản	<ul style="list-style-type: none"> - Các ứng dụng không dùng tài khoản có quyền quản trị để kết nối đến CSDL nhằm đảm bảo kẻ tấn công không có quyền cao nhất với CSDL khi ứng dụng có lỗ hổng và bị khai thác. - Yêu cầu về mật khẩu tài khoản: Mật khẩu được đặt theo yêu cầu tại quy định chính sách mật khẩu mạnh hiện hành của EVN ban hành. 	- Đảm bảo an toàn cho tài khoản của hệ thống	Phụ lục 08	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 08.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 4.2.2 và kết quả nghiên cứu ATTT áp dụng trên hệ quản trị cơ sở dữ liệu.
Yêu cầu về phân quyền an toàn	- Không dùng các tài khoản quản trị, nhóm quản trị của hệ điều hành như: root, Administrator, Local System,... để chạy dịch vụ CSDL nhằm đảm bảo kẻ tấn công không có quyền cao nhất với HĐH khi ứng dụng có lỗ hổng và bị khai thác.	- Đảm bảo an toàn cho dữ liệu	Phụ lục 08	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 08.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 5.2 và kết quả nghiên cứu tình hình thực tiễn.

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	<p>- Phân quyền chỉ cho phép tài khoản chạy dịch vụ CSDL được phép truy cập đến các thư mục chứa file dữ liệu, file log nhằm tránh việc truy cập không mong muốn từ các tài khoản khác tới các dữ liệu nhạy cảm.</p> <p>- Yêu cầu về thiết lập quyền kết nối CSDL đối với tài khoản ứng dụng nhằm tránh việc tấn công sâu hơn vào hệ thống khi kẻ tấn công có được kết nối tới một CSDL:</p> <ul style="list-style-type: none"> + Với mỗi ứng dụng, tạo một tài khoản kết nối CSDL riêng. + Với mỗi tài khoản truy cập CSDL, chỉ được cấp quyền tối thiểu đảm bảo hoạt động theo yêu cầu nghiệp vụ của ứng dụng. 				
Yêu cầu về cấu hình ghi log cho hệ quản trị CSDL	<p>- Nếu hệ quản trị CSDL hỗ trợ tính năng ghi log audit:</p> <ul style="list-style-type: none"> + Cấu hình ghi log tất cả lần đăng nhập thành công và không thành công vào hệ quản trị CSDL. 	- Đảm bảo các trường hợp điều tra sự cố	Phụ lục 08	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 08.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 6.1

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	<ul style="list-style-type: none"> + Thời gian lưu log yêu cầu tối thiểu là 3 tháng. - Log truy cập hỗ trợ theo dõi hệ thống, ghi nhận những truy cập bất thường tới CSDL 				
Yêu cầu về giới hạn truy cập	<ul style="list-style-type: none"> - Giới hạn chỉ được những IP cần thiết được kết nối đến CSDL nhằm đảm bảo việc kết nối tới CSDL từ những IP xác định, tránh việc kết nối tới CSDL từ IP bất thường. 	<ul style="list-style-type: none"> - Đảm bảo việc truy cập được an toàn. 	Phụ lục 08	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 08.	Kế thừa tiêu chuẩn NIST SP 800-123: 6.5 và kết quả nghiên cứu tình hình thực tiễn.
Yêu cầu môi trường vận hành an toàn	<ul style="list-style-type: none"> - User remote quản trị hệ thống phải enable cơ chế xác thực đa nhân tố (token/OTP). - Sử dụng 1 máy riêng đảm bảo toàn bộ các quy tắc ATTT cho máy người dùng cuối để vận hành hệ thống . - Sử dụng các máy riêng để vận hành hệ thống, không dùng cho các công việc thông thường hàng ngày (Duyệt email, truy cập internet, đọc file văn bản MSOffice/pdf. 	<ul style="list-style-type: none"> - Đảm bảo môi trường vận hành hệ thống an toàn 	Phụ lục 08	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 08.	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Quản trị từ xa	- Thiết lập an toàn cho quản trị từ xa theo Quy tắc ATTT hệ điều hành máy chủ.	- Đảm bảo an toàn trong việc quản trị	Tham khảo theo Quy tắc cấu hình ATTT hệ điều hành máy chủ.	Tham khảo theo Quy tắc cấu hình ATTT hệ điều hành máy chủ.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 5.2 và kết quả nghiên cứu tình hình thực tiễn.

Điều 14. Quy tắc cấu hình ATTT cho Email Server

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Yêu cầu về việc cài đặt Hệ thống Email Server an toàn	<ul style="list-style-type: none"> - Các thành phần của hệ thống email phải được cài đặt trên hệ điều hành an toàn, đã được thiết lập cấu hình chính sách bảo mật đảm bảo theo Quy tắc ATTT cho HĐH. - Phiên bản phần mềm email server cài đặt phải là phiên bản vẫn duy trì các bản vá cập nhật bởi nhà sản xuất, được cập nhật bản vá và đảm bảo không mắc các lỗ hổng bảo mật đã được công bố. 	- Đảm bảo môi trường cài đặt an toàn	Phụ lục 09	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 09.	Tham chiếu tiêu chuẩn: - TLTK 1. - TLTK 2.
Yêu cầu môi trường vận hành an toàn.	<ul style="list-style-type: none"> - User remote quản trị hệ thống phải enable cơ chế xác thực đa nhân tố (token/OTP). - Sử dụng 1 máy riêng đảm bảo toàn bộ các quy tắc ATTT cho máy người dùng cuối để vận hành hệ thống . - Sử dụng các máy riêng để vận hành hệ thống, không dùng cho các công việc thông thường hàng ngày (Duyệt email, truy cập internet, đọc file văn bản MSOffice/pdf). 	- Đảm bảo môi trường vận hành hệ thống an toàn	Phụ lục 09	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 09.	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Yêu cầu phân tách các thành phần trong hệ thống Email	<ul style="list-style-type: none"> - Phải có firewall quản lý chính sách traffic giữa internet và các thành phần nhận/gửi email - Trường hợp có sử dụng Edge role của exchange phải phân tách thành phần này với các thành phần còn lại bằng firewall quản lý chính sách 	<ul style="list-style-type: none"> - Đảm bảo phân tách hệ thống, giảm thiểu nguy cơ bị tấn công chéo giữa các thành phần thì một thành phần bị chiếm quyền 	Phụ lục 09	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 09.	Tham chiếu tiêu chuẩn: - TLTK 1. - TLTK 2.
Yêu cầu về tính sẵn sàng	<ul style="list-style-type: none"> - Tất cả thành phần của hệ thống phải đảm bảo cơ chế dự phòng mức vật lý, ứng dụng - CSDL người dùng, mailbox phải được backup định kỳ 	<ul style="list-style-type: none"> - Đảm bảo tính HA cho hệ thống email 	Phụ lục 09	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 09.	Tham chiếu tiêu chuẩn: - TLTK 1.
Yêu cầu mã hóa dữ liệu email	<ul style="list-style-type: none"> - Toàn bộ traffic gửi/nhận email phải được mã hóa SSL/TLS (SMTPS, POP3S, IMAPS, HTTPS) với chứng thư số của nhà cung cấp uy tín - Đối với thành phần nhận email gửi từ bên ngoài: Phải bật hỗ trợ STARTTLS 	<ul style="list-style-type: none"> - Giảm thiểu nguy cơ bị snip, đánh cắp thông tin trên kênh truyền 	Phụ lục 09	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 09.	Tham chiếu tiêu chuẩn: - TLTK 1. - TLTK 2.

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	- Đối với thành phần gửi email ra bên ngoài: Phải bật cơ chế sử dụng STARTTLS nếu bên nhận có hỗ trợ STARTTLS				
Yêu cầu về chống email giả mạo (phishing email)	<ul style="list-style-type: none"> - Phòng chống email bị giả mạo: <ul style="list-style-type: none"> + Tạo bản ghi SPF, DKIM cho tên miền + Tạo bản ghi ngược cho IP của các thành phần gửi/nhận email - Phòng chống giả mạo nội bộ: <ul style="list-style-type: none"> + Yêu cầu người dùng phải xác thực trước khi gửi email (SMTP) + Phải ngăn chặn được việc giả mạo nội bộ bằng cách giả mạo câu lệnh MAIL FROM, hoặc giả mạo header FROM khi gửi email - Phòng chống nhận được email giả mạo: <ul style="list-style-type: none"> + Phải có cơ chế kiểm tra bản ghi SPF/DKIM của email nhận được 	- Giảm thiểu nguy cơ bị giả mạo email	Phụ lục 09	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 09.	Tham chiếu tiêu chuẩn: - TLTK 2.
Yêu cầu về chống email spam	- Không cho phép open relay	Giảm thiểu nguy cơ bị	Phụ lục 09	Kiểm tra cấu hình theo hướng dẫn	Tham chiếu tiêu chuẩn: - TLTK 2.

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	<ul style="list-style-type: none"> - Cấu hình kiểm tra IP, domain blacklist (reputation) theo tổ chức uy tín trên thành phần nhận mail - Phải hỗ trợ cấu hình chặn lọc theo các tiêu chí: IP, domain, địa chỉ email, tiêu đề, từ khóa trong luồng mail sử dụng trực tiếp nội bộ - Phải giới hạn tốc độ gửi nhận email trên các thiết bị trên thành phần gửi email MTA - Hỗ trợ phát hiện email spam theo nội dung (Khuyến cáo) 	spam hệ thống email		tại Phụ lục 09.	
Yêu cầu về chống mã độc	<ul style="list-style-type: none"> - Toàn bộ email gửi/nhận phải được chặn lọc spam và quét virus + Riêng đối với email gửi/nhận trao đổi với bên ngoài phải đi qua thiết bị email gateway chuyên dụng đảm bảo lọc spam và quét virus (ví dụ: fortimail, cisco ironport, ...). (*) - Hệ thống email server cần phải có cơ chế chặn lọc mã độc, APT - Cập nhật mẫu virus hàng ngày 	- Giảm thiểu bị lây nhiễm mã độc	Phụ lục 09	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 09.	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	- Hệ thống Email Server không cho phép gửi nhận email có đính kèm file thực thi kể cả trong file nén: <i>.exe, .msi, .bat, .cmd, .com, .bin, .vb, .vbs, .vbe</i>				
Yêu cầu về xác thực đa nhân tố khi sử dụng email	- Phải xác thực đa nhân tố khi người dùng sử dụng email qua web mail. - Đối với ứng dụng email client không hỗ trợ xác thực đa nhân tố như: Outlook, thunderbird, email client trên điện thoại, ... thì sử dụng cơ chế App-specific passwords (App passwords).	- Giảm thiểu bị chiếm quyền email	Phụ lục 09	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 09.	Khuyến cáo
Chống rà quét mật khẩu trong luồng mail nội bộ	- Đối với đăng nhập qua web mail nội bộ: Nếu 1 account đăng nhập sai 5 lần liên tục thì sẽ yêu cầu nhập captcha - Đối với đăng nhập qua giao thức smtp, pop3, imap: + Trong 1 connection chỉ được phép đăng nhập sai 2 lần, quá 2 lần sẽ hủy connection đó + Giới hạn số tốc độ tạo connection của 1 ip client từ internet trên các thành phần giao tiếp với client (SMTP, POP3, IMAP)	- Giảm thiểu bị rà quét mật khẩu	Phụ lục 09	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 09.	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Cấu hình log truy vết hệ thống Email	<ul style="list-style-type: none"> - Lưu đầy đủ log đăng nhập của người dùng nội bộ trước khi gửi email, thông tin trong log bao gồm user account, thời gian, trạng thái, ip người dùng. - Lưu đầy đủ log gửi email khi trao đổi email nội bộ và email bên ngoài. Thông tin trong log bao gồm: người gửi, người nhận, thời gian, tiêu đề, dung lượng, tên file đính kèm, trạng thái, ip chính xác của người dùng. - Lưu log đầy đủ tác động vào hệ thống email: thời gian, user tác động, nội dung tác động, kết quả tác động, IP tác động. - Tất cả các log được lưu tập trung, lưu tối thiểu 3 tháng. - Log phải được đẩy về hệ thống log tập trung/SIEM. 	<ul style="list-style-type: none"> - Sử dụng trong quá trình forensic khi cần thiết 	Phụ lục 09	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 09.	Tham chiếu tiêu chuẩn: <ul style="list-style-type: none"> - TLTK 1. - TLTK 2.
Yêu cầu về việc đánh giá ATTT định kỳ	<ul style="list-style-type: none"> - Việc đánh giá ATTT cho hệ thống Email phải được thực hiện định kỳ tối thiểu 6 tháng 1 lần. 	<ul style="list-style-type: none"> - Đảm bảo duy trì tiêu chuẩn ATTT 	Phụ lục 09	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 09.	Tham chiếu tiêu chuẩn: <ul style="list-style-type: none"> - TLTK 1.

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Quản trị từ xa	- Thiết lập an toàn cho quản trị từ xa theo Quy tắc ATTT hệ điều hành máy chủ.	- Đảm bảo an toàn trong việc quản trị	Tham khảo theo Quy tắc cấu hình ATTT hệ điều hành máy chủ.	Tham khảo theo Quy tắc cấu hình ATTT hệ điều hành máy chủ.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 5.2 và kết quả nghiên cứu tình hình thực tiễn.

Điều 15. Quy tắc cấu hình ATTT cho hệ thống AD (Active Directory)

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham khảo
Yêu cầu về việc cài đặt hệ thống AD an toàn	<ul style="list-style-type: none"> - Cài đặt phiên bản hệ điều hành an toàn theo Quy tắc ATTT cho hệ điều hành máy chủ. - Cài đặt phiên bản Hệ thống AD an toàn. 	- Đảm bảo môi trường cài đặt an toàn	Phụ lục 10	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 10.	Tham chiếu tiêu chuẩn: TLTK 1.
Yêu cầu môi trường vận hành an toàn	<ul style="list-style-type: none"> - User remote quản trị hệ thống phải enable cơ chế xác thực đa nhân tố (token/OTP). - Sử dụng 1 máy riêng đảm bảo toàn bộ các quy tắc ATTT cho máy người dùng cuối để vận hành hệ thống . - Sử dụng các máy riêng để vận hành hệ thống, không dùng cho các công việc thông thường hàng ngày (Duyệt email, truy cập internet, đọc file văn bản MS Office/pdf. 	- Đảm bảo môi trường vận hành hệ thống an toàn	Phụ lục 10	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 10.	TLTK 3: Mục Implement administrative practices: Ensure administrative tasks are not performed on hosts used for standard user activities (for example, email and web browsing)
Yêu cầu bảo vệ tài khoản đặc	- Không sử dụng tài khoản đặc quyền, nhóm đặc quyền để remote desktop, đăng nhập trên	- Giảm thiểu nguy cơ bị mất các account đặc	Phụ lục 10	Kiểm tra cấu hình theo	Tham chiếu tiêu chuẩn: - TLTK 1.

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham khảo
quyền, nhóm đặc quyền	<p>máy tính người dùng, member server, xác thực LDAP, để chạy bash job, task scheduler, service trên máy người dùng hoặc member server nếu như không thực sự cần thiết.</p> <ul style="list-style-type: none"> - Chỉ sử dụng các tài khoản đặc quyền, tài khoản thuộc nhóm đặc quyền trong quá trình cài đặt. - Giới hạn các tài khoản thuộc nhóm có đặc quyền trên Group Policy áp dụng trên các Domain Controllers. Bất kỳ tài khoản nào được thêm vào các nhóm này trái phép sẽ bị tự động loại bỏ sau một khoảng thời gian. - Trường hợp các hệ thống yêu cầu bắt buộc phải sử dụng các account thuộc nhóm đặc quyền, tài khoản đặc quyền cần phải thiết lập Log on to cho các user sử dụng chỉ trên các máy này. 	quyền, account thuộc nhóm đặc quyền		hướng dẫn tại Phụ lục 10.	<ul style="list-style-type: none"> - TLTK 2. - TLTK 3: Mục Implement administrative practices: Domain admins (tier 0) cannot log on to enterprise servers (tier 1) and standard user workstations (tier 2).

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham khảo
	<p>- Mỗi quản trị viên cần có 1 account quản trị riêng. Không sử dụng chung account quản trị.</p> <p>- Tất cả các tài khoản user thường không có quyền join/unjoin domain. Sử dụng một nhóm tài khoản có quyền riêng biệt để join/unjoin domain. Tất cả các tài khoản thường không có quyền cài đặt phần mềm trên máy người dùng. Sử dụng một nhóm tài khoản có quyền riêng biệt để cài phần mềm trên máy người dùng. Người phụ trách hỗ trợ có thẩm quyền sẽ thực hiện việc quản lý các account này.</p>				
Yêu cầu thiết lập chống tấn công leo thang	<p>- Không cho phép các tài khoản Administrator AD được phép đăng nhập từ xa, đăng nhập dạng bash job, đăng nhập dạng services.</p> <p><i>Lưu ý: chỉ áp dụng với các tài khoản Administrator AD, không</i></p>	- Giảm thiểu nguy cơ bị tấn công leo thang	Phụ lục 10	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 10.	<p>Tham chiếu tiêu chuẩn:</p> <ul style="list-style-type: none"> - TLTK 1. - TLTK 2. - TLTK 3: Mục Implement administrative

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham khảo
	<p><i>áp dụng với các tài khoản thuộc nhóm Domain Admins, Enterprise Admins, Schema Admins.</i></p> <p>- Không cho phép các tài khoản Administrator AD, các nhóm Administrators, Domain Admins, Enterprise Admins, Schema Admins được phép đăng nhập qua remote desktop services.</p> <p>- Đối với các tài khoản thuộc nhóm Domain Admins, Enterprise Admins, Schema Admins, trừ tài khoản Administrator AD, thì tất cả các tài khoản còn lại phải giới hạn Logon to chỉ trên các máy DC.</p>				<p>practices: Logon restrictions can be enforced with: Logon restrictions can be enforced with Group Policy Logon Rights Restriction</p>
Yêu cầu thiết lập chống tấn công chéo	<p>- Không cho phép đăng nhập từ xa đối với: Các tài khoản Administrator AD, các nhóm Domain Admins, Enterprise Admins, Schema Admins. Tài</p>	<p>- Giảm thiểu nguy cơ bị tấn công chéo</p>	Phụ lục 10	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 10.	<p>Tham chiếu tiêu chuẩn:</p> <ul style="list-style-type: none"> - TLTK 1. - TLTK 2.

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham khảo
	<p>khoản local Administrator, nhóm Administrators.</p> <ul style="list-style-type: none"> - Không cho phép đăng nhập dạng bash job (task scheduler), đăng nhập dạng services đối với: Các tài khoản Administrator AD, các nhóm Domain Admins, Enterprise Admins, Schema Admins. Tài khoản local Administrator, nhóm Administrators. - Không cho phép đăng nhập locally đối với: Các nhóm Domain Admins, Enterprise Admins, Schema Admins. - Không cho phép đăng nhập remote desktop đối với: Các tài khoản Administrator AD, các nhóm Domain Admins, Enterprise Admins, Schema Admins. Tài khoản local Administrator, nhóm local Administrators. 				<p>- TLTK 3: Mục Implement administrative practices: Logon restrictions can be enforced with: Logon restrictions can be enforced with Group Policy Logon Rights Restriction</p>

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham khảo
Yêu cầu về việc lưu log đăng nhập	- Yêu cầu lưu log đăng nhập tối thiểu là 3 tháng.	- Lưu trữ thông tin cho việc forensic	Phụ lục 10	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 10.	Tham chiếu tiêu chuẩn: - TLTK 1. - TLTK 2.
Yêu cầu về việc đánh giá ATTT định kỳ	- Việc đánh giá ATTT cho hệ thống AD phải được thực hiện định kỳ	- Đảm bảo duy trì tiêu chuẩn ATTT	Phụ lục 10	N/A	Tham chiếu tiêu chuẩn: - TLTK 1.
Quản trị từ xa	- Thiết lập an toàn cho quản trị từ xa theo Quy tắc ATTT hệ điều hành máy chủ.	- Đảm bảo an toàn trong việc quản trị	Tham khảo theo Quy tắc cấu hình ATTT hệ điều hành máy chủ.	Tham khảo theo Quy tắc cấu hình ATTT hệ điều hành máy chủ.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 5.2 và kết quả nghiên cứu tình hình thực tiễn.

Điều 16. Quy tắc cấu hình ATTT cho hệ thống Proxy

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Yêu cầu về việc cài đặt hệ thống Proxy Server an toàn	<ul style="list-style-type: none"> - Các máy chủ làm proxy server phải được thiết lập cấu hình chính sách bảo mật đảm bảo theo Quy tắc ATTT cho hệ điều hành máy chủ (Chỉ áp dụng nếu dùng proxy server). - Phiên bản phần mềm proxy server cài đặt phải là phiên bản vẫn duy trì các bản vá cập nhật bởi nhà phát triển, được cập nhật bản vá và đảm bảo không mắc các lỗ hổng bảo mật đã được công bố. - License các tính năng của hệ thống phải còn thời hạn sử dụng. 	<ul style="list-style-type: none"> - Đảm bảo cài đặt hệ thống proxy an toàn 	Phụ lục 11	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 11.	Tham chiếu tiêu chuẩn: - TLTK 1. - TLTK 2.
Yêu cầu môi trường vận hành an toàn	<ul style="list-style-type: none"> - User remote quản trị hệ thống phải enable cơ chế xác thực đa nhân tố (token/OTP). - Sử dụng 1 máy riêng đảm bảo toàn bộ các tiêu chuẩn ATTT cho máy người dùng cuối để vận hành hệ thống . - Sử dụng các máy riêng để vận hành hệ thống, không dùng cho các công việc thông thường hàng ngày (Duyệt email, 	<ul style="list-style-type: none"> - Đảm bảo môi trường vận hành hệ thống an toàn 	Phụ lục 11	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 11.	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	truy cập internet, đọc file văn bản MS Office/pdf.				
Yêu cầu về thiết lập hệ thống proxy	<ul style="list-style-type: none"> - Việc tích hợp hệ thống Proxy/ Web Security phải đảm bảo toàn bộ các dữ liệu gửi nhận nội bộ và gửi nhận ra ngoài đều đi qua hệ thống Proxy/Web Security. - Thực hiện chặn toàn bộ các kết nối trực tiếp từ người dùng ra internet trên firewall - Có giới hạn Firewall chỉ cho phép truy cập vào quản trị hệ thống proxy chỉ từ máy quản trị có thẩm quyền. Firewall chỉ mở các port theo nhu cầu tối thiểu đảm bảo hoạt động của hệ thống. Đóng toàn bộ các kết nối không cần thiết. - Thực hiện cấu hình trên firewall chỉ cho phép dải IP được phép truy cập đến. - Thực hiện cấu hình chặn trên hệ thống nếu có hỗ trợ. 	- Đảm bảo triển khai đúng mô hình	Phụ lục 11	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 11.	Tham chiếu tiêu chuẩn: - TLTK 1. - TLTK 2.
Yêu cầu đăng nhập, mật khẩu của Quản trị	<ul style="list-style-type: none"> - Giới hạn số lần nhập password không cho phép nhập sai quá 5 lần. - Giới hạn thời gian timeout của phiên kết nối quản trị tối đa là 15 phút. - Tất cả các tài khoản phải có mật khẩu. 	- Giảm thiểu nguy cơ bị dò quét mật khẩu	Phụ lục 11	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 11.	Tham chiếu tiêu chuẩn: - TLTK 1. - TLTK 2.

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
viên hệ thống Proxy	<ul style="list-style-type: none"> - Mật khẩu có độ dài tối thiểu 10 ký tự. - Mật khẩu bao gồm tối thiểu 3 trong 4 loại ký tự sau: chữ cái viết hoa (A - Z); chữ cái viết thường (a - z); chữ số (0 - 9); các ký tự khác trên bàn phím máy tính (` ~ ! @ # \$ % ^ & * () _ - + = { } [] \ : ; " ' < > , . ? /) và dấu cách. - Mật khẩu không chứa tên tài khoản. - Thời gian hiệu lực của mật khẩu đối với tài khoản cá nhân tối đa là 90 ngày. 				
Yêu cầu cấu hình đồng bộ thời gian	<ul style="list-style-type: none"> - Cấu hình tự động đồng bộ thời gian - Có cấu hình cập nhật thời gian theo giao thức NTP tới server NTP tập trung 	- Đảm bảo thời gian ghi log chính xác	Phụ lục 11	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 11.	Tham chiếu tiêu chuẩn: - TLTK 2.
Yêu cầu cấu hình SNMP	- Cấu hình đầy SNMP tới hệ thống SNMP tập trung	- Cấu hình SNMP để giám sát trạng thái hoạt động của hệ thống	Phụ lục 11	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 11.	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Yêu cầu về sử dụng mã hóa	<ul style="list-style-type: none"> - Có sử dụng tính năng SSL Inspection (nếu hệ thống hỗ trợ). - Cấu hình trên web security gateway bypass không giải mã các trang web tin cậy về về tài chính ngân hàng, các web chứa thông tin cá nhân của người dùng như các trang mạng xã hội, email. 	- Giám sát và phân tích các truy cập có sử dụng mã hóa	Phụ lục 11	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 11.	
Yêu cầu về ngăn chặn các C&C Server điều khiển mã độc	<ul style="list-style-type: none"> - Thực hiện cập nhật thường xuyên danh sách C&C. - Thực hiện chặn kết nối đến IP và domain của máy chủ điều khiển mã độc C&C theo các thông báo của bộ phận ATTT tại đơn vị 	- Ngăn chặn kết nối tới máy chủ điều khiển phát tán mã độc	Phụ lục 11	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 11.	
Yêu cầu về kiểm soát ứng dụng	<ul style="list-style-type: none"> - Có bật tính năng kiểm soát kết nối đến ứng dụng (nếu có hỗ trợ) - Thực hiện chặn kết nối đến các máy chủ điều khiển từ xa (như Teamviewer, Logmein, Ultraviewer). 	- Ngăn chặn kết nối các ứng dụng trái với quy định	Phụ lục 11	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 11.	
Yêu cầu về chặn lọc các website	- Có định nghĩa các loại trang web, các trang web độc hại, không phù hợp không được truy cập tới.	- Ngăn chặn việc truy cập các website trái quy	Phụ lục 11	Kiểm tra cấu hình theo hướng	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
(ULR Filtering)	<ul style="list-style-type: none"> - Có định nghĩa các loại trang web, các trang web có tính chất không phù hợp với công việc, không được truy cập hoặc giới hạn truy cập trong giờ làm việc hành chính. - Có cập nhật các loại trang web, danh sách trang web thường xuyên bao gồm các loại trang web được phép và không được phép truy cập tới. - Cấu hình chỉ được kết nối đến các trang web được phép truy cập. - Cấu hình chặn không cho kết nối tới các trang web không được phép truy cập 	định trong giờ làm việc		dẫn tại Phụ lục 11.	
Yêu cầu về chặn lọc virus	<ul style="list-style-type: none"> - Cập nhật thường xuyên các mẫu virus mới nhất. - Có bật tính năng quét virus, phát hiện file độc hại được tải xuống từ website. 	- Ngăn chặn virus tải xuống	Phụ lục 11	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 11.	
Yêu cầu chặn file upload	<ul style="list-style-type: none"> - Có thực hiện chặn người dùng upload tài liệu lên các trang chia sẻ dữ liệu trực tuyến, truy cập public email, mạng xã hội 	- Chống thất thoát dữ liệu	Phụ lục 11	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 11.	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Yêu cầu về lưu log hệ thống	<ul style="list-style-type: none"> - Lưu đầy đủ log truy cập của người dùng, thông tin log bao gồm địa chỉ IP nguồn, IP đích, tên user, thời gian, URL truy cập, method, mã trả về, content type trả về, User Agent, Referer. - Lưu đầy đủ log đăng nhập, tác động hệ thống. 	- Sử dụng forensic khi sự cố xảy ra	Phụ lục 11	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 11.	Tham chiếu tiêu chuẩn: - TLTK 1. - TLTK 2.
Quản trị từ xa	- Thiết lập an toàn cho quản trị từ xa theo Quy tắc ATTT hệ điều hành máy chủ.	- Đảm bảo an toàn trong việc quản trị	Tham khảo theo Quy tắc cấu hình ATTT hệ điều hành máy chủ.	Tham khảo theo Quy tắc cấu hình ATTT hệ điều hành máy chủ.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 5.2 và kết quả nghiên cứu tình hình thực tiễn.

Điều 17. Quy tắc cấu hình ATTT cho hệ thống quản lý Antivirus tập trung

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Yêu cầu về việc cài đặt Hệ thống antivirus tập trung an toàn	<ul style="list-style-type: none"> - Các thành phần của hệ thống Antivirus tập trung phải được cài đặt trên HĐH an toàn, đã được thiết lập cấu hình chính sách bảo mật đảm bảo theo Quy tắc ATTT cho hệ điều hành. - Phiên bản Antivirus server cài đặt phải là phiên bản vẫn duy trì các bản vá cập nhật bởi nhà sản xuất, được cập nhật bản vá và đảm bảo không mắc các lỗ hổng bảo mật đã được công bố. - Không sử dụng các account thuộc nhóm Domain Admins, Schema Admins hoặc Enterprise Admin cài đặt. 	- Đảm bảo môi trường cài đặt an toàn	Phụ lục 12	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 12.	Tham chiếu tiêu chuẩn: - TLTK 1. - TLTK 2.
Yêu cầu môi trường vận hành an toàn	<ul style="list-style-type: none"> - User remote quản trị hệ thống phải enable cơ chế xác thực đa nhân tố (token/OTP). - Sử dụng 1 máy riêng đảm bảo toàn bộ các tiêu chuẩn ATTT cho máy người dùng cuối để vận hành hệ thống . - Sử dụng các máy riêng để vận hành hệ thống, không dùng cho các công việc thông thường hàng ngày (Duyệt email, 	- Đảm bảo môi trường vận hành hệ thống an toàn	Phụ lục 12	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 12.	

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	truy cập internet, đọc file văn bản MSOffice/pdf.				
Yêu cầu về phân quyền quản trị hệ thống Antivirus tập trung	- Phân quyền vừa đủ cho các tài khoản quản trị viên hệ thống Antivirus tập trung được quản lý chính sách máy tính tương ứng.	- Nếu 1 hệ thống Antivirus tập trung phục vụ 1 tổ chức lớn thì cần phân quyền cho các quản trị viên đơn vị chỉ quản lý chính sách các máy tính của đơn vị mình.	Phụ lục 12	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 12.	Tham chiếu tiêu chuẩn: - TLTK 2.
Yêu cầu về thiết lập chính sách trên hệ thống antivirus tập trung	- Bật tính năng Real time protection trên toàn bộ các máy trạm cài agent Antivirus nếu hệ thống hỗ trợ - Định kỳ scan các máy client theo chu kỳ hợp lý		Phụ lục 12	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 12.	Tham chiếu tiêu chuẩn: - TLTK 2.

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Yêu cầu về cài đặt và update antivirus client	<ul style="list-style-type: none"> - Toàn bộ người dùng/server phải được cài đặt Antivirus client và được quản lý bởi hệ thống antivirus tập trung - Cập nhật mẫu virus từ về máy chủ Antivirus tập trung và Antivirus client tối thiểu 1 ngày/1 lần - Việc cập nhật từ internet về phải qua hệ thống proxy để kiểm soát các địa chỉ kết nối. - Cấu hình tự động update bản vá các ứng dụng trên máy chủ/máy trạm (nếu có). 	<ul style="list-style-type: none"> - Đảm bảo các máy tính client đều được cài đặt và cập nhật thường xuyên. 	Phụ lục 12	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 12.	Tham chiếu tiêu chuẩn: - TLTK 2.
Yêu cầu cấu hình self-defence cho antivirus client	<ul style="list-style-type: none"> - Cấu hình không cho người dùng thay đổi các tham số cấu hình antivirus client. - Cấu hình không cho người dùng gỡ, tắt bảo vệ của Antivirus client. 	<ul style="list-style-type: none"> - Đảm bảo người dùng không tự tắt hoặc gỡ bỏ antivirus client. 	Phụ lục 12	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 12.	Tham chiếu tiêu chuẩn: - TLTK 2.
Yêu cầu chặn thiết bị ngoại vi	<ul style="list-style-type: none"> - Bật tính năng kiểm soát thiết bị, cấu hình ngăn chặn các thiết bị ngoại vi (USB/CDROM/...) kết nối với máy trạm. 		Phụ lục 12	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 12.	Tham chiếu tiêu chuẩn: - TLTK 2.

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Yêu cầu cấu hình Firewall mềm	- Bật tường lửa của phần mềm Antivirus client, cấu hình tường lửa mềm chặn các kết nối chiều inbound đến máy trạm (PC).	- Đảm bảo máy tính người dùng không bị tấn công ngang hàng.	Phụ lục 12	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 12.	Tham chiếu tiêu chuẩn: - TLTK 2.
Yêu cầu sao lưu hệ thống antivirus tập trung	- Cấu hình sao lưu hệ thống antivirus tập trung hàng ngày, lưu tối thiểu 03 bản sao lưu gần nhất.	- Đảm bảo khôi phục hệ thống nếu có lỗi.	Phụ lục 12	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 12.	Tham chiếu tiêu chuẩn: - TLTK 2.
Cấu hình lưu log	- Lưu đầy đủ các log alert, log vận hành thay đổi của hệ thống Antivirus tập trung. - Log lưu trong thời gian 3 tháng - Log phải được đẩy về lưu tại hệ thống log tập trung/SIEM		Phụ lục 12	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 12.	Tham chiếu tiêu chuẩn: - TLTK 1. - TLTK 2.
Đánh giá ATTT định kỳ	- Đánh giá ATTT định kỳ tối thiểu 6 tháng 1 lần		Phụ lục 12	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 12.	Tham chiếu tiêu chuẩn: - TLTK 1.

Nội dung quy tắc	Yêu cầu	Mục đích	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Quản trị từ xa	- Thiết lập an toàn cho quản trị từ xa theo Quy tắc ATTT hệ điều hành máy chủ.	- Đảm bảo an toàn trong việc quản trị	Tham khảo theo Quy tắc cấu hình ATTT hệ điều hành máy chủ.	Tham khảo theo Quy tắc cấu hình ATTT hệ điều hành máy chủ.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 5.2 và kết quả nghiên cứu tình hình thực tiễn.

Điều 18. Quy tắc cấu hình ATTT cho hệ thống VPN tập trung

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Đảm bảo tính xác thực	Các hệ thống VPN phải sử dụng các phương pháp xác thực. Không sử dụng các hệ thống VPN không có xác thực	Xác thực bằng mật khẩu và kết hợp một trong các phương thức xác thực tập trung như: - Xác thực qua hệ thống điều khiển truy cập TACACS (Terminal Access Controller Access-Control System). - Xác thực qua hệ thống RADIUS (Remote Authentication Dial In User Service). - Xác thực LADP.	Phụ lục 13	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 13.	Tham chiếu một phần các tiêu chuẩn: - TLTK 1.
Nâng mức bảo mật lên mức cao nhất được hỗ trợ	Hệ thống VPN phải sử dụng các giao thức, tiêu chuẩn mã hóa, thuật toán an toàn. Đề xuất sử dụng mức bảo mật cao nhất.	- Sử dụng giao thức TLS1.1 trở lên. - Mã hóa AES (128, 192, 256) - Sử dụng khóa RSA có độ dài ít nhất 2048 bit. - Thuật giải băm SHA256 trở lên. - Sử dụng trao đổi khóa thuộc nhóm ECDH, không dùng RSA key exchange.	Phụ lục 13	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 13.	Tham chiếu một phần các tiêu chuẩn: - CIS Control V7.1 mục 18.5

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Kiểm soát kết nối qua tường lửa	Hệ thống phải được kiểm soát kết nối chặt chẽ, tuân thủ theo quy định về mở kết nối của đơn vị và EVN.	<ul style="list-style-type: none"> - Đối với các kết nối từ VPN client đến hệ thống VPN: + Chỉ cho phép mở các port chạy dịch vụ VPN. - Đối với các kết nối từ dải IP VPN đến các hệ thống nội bộ: Chặn hết đến các port quản trị, port kết nối đến database... + Chỉ cho phép mở vào các trang thông tin cơ bản của đơn vị + Mở đúng đến IP của dịch vụ cần kết nối. 	Phụ lục 13	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 13.	Tham chiếu một phần các tiêu chuẩn: - TLTK 1. - TLTK 2.
Tắt các tính năng hỗ trợ không đảm bảo an toàn	Chỉ bật các tính năng hỗ trợ đã đảm bảo an toàn và thống kê các tính năng này trong checklist để đánh giá chỉ bật lên khi có yêu cầu sử dụng	Một số hệ thống VPN có hỗ trợ các tính năng không đảm bảo an toàn (Ví dụ: “SSL Legacy Renegotiation Support option”)	Phụ lục 13	Kiểm tra cấu hình theo hướng dẫn tại Phụ lục 13.	
Yêu cầu môi trường vận hành an toàn	- User remote quản trị hệ thống phải enable cơ chế xác	- Đảm bảo môi trường vận hành hệ thống an toàn	Phụ lục 13	Kiểm tra cấu hình theo hướng	

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
(với hệ thống phần mềm VPN triển khai trên các máy chủ)	<p>thực đa nhân tố (token/OTP).</p> <p>- Sử dụng 1 máy riêng đảm bảo toàn bộ các quy tắc ATTT cho máy người dùng cuối để vận hành hệ thống.</p> <p>- Sử dụng các máy riêng để vận hành hệ thống, không dùng cho các công việc thông thường hàng ngày (Duyệt email, truy cập internet, đọc file văn bản MS Office/pdf).</p>			dẫn tại Phụ lục 13.	
Quản trị từ xa	Thiết lập an toàn cho quản trị từ xa theo Quy tắc ATTT hệ điều hành máy chủ.	- Đảm bảo an toàn trong việc quản trị	Tham khảo theo Quy tắc cấu hình ATTT hệ điều hành máy chủ.	Tham khảo theo Quy tắc cấu hình ATTT hệ điều hành máy chủ.	Kế thừa tiêu chuẩn NIST SP 800-123: mục 5.2 và kết quả nghiên cứu tình hình thực tiễn.

CHƯƠNG V. BỘ QUY TẮC CẤU HÌNH ATTT CHO CÁC THIẾT BỊ MẠNG

Điều 19. Quy tắc cấu hình ATTT cho hệ thống firewall

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
1. Yêu cầu chung					
Đưa các thiết bị về trạng thái cấu hình mặc định trước khi triển khai tích hợp vào mạng lưới	Đưa các thiết bị về trạng thái cấu hình mặc định trước khi thực hiện khai báo các cấu hình mới để tích hợp vào mạng lưới	Tránh việc tồn tại các cấu hình thừa, không cần thiết trên thiết bị gây ra các nguy cơ tiềm ẩn mất ATTT	Phụ lục 14	Kiểm tra quy trình triển khai thực tế	
Đảm bảo sử dụng firmware, phần mềm và bản vá không tồn tại lỗi ATTT	Đảm bảo sử dụng firmware, phần mềm và bản vá không có các lỗ hổng ATTT nghiêm trọng đã được công bố trong các CVE	Tránh bị khai thác các lỗ hổng ATTT nghiêm trọng của các thiết bị.	Phụ lục 14	Kiểm tra trong giao diện quản trị thiết bị	Kế thừa tiêu chuẩn: - CIS Control V7.1 - TLTK 1. - TLTK 2.
	Có phương án khắc phục các lỗ hổng tiềm ẩn của thiết bị				
Đảm bảo tính ổn định của hệ thống	Thống nhất phiên bản hệ điều hành cho tất cả các thiết bị mạng (cùng	Đảm bảo hệ thống hoạt động ổn định, đồng bộ, đơn giản		Kiểm tra chính sách quản lý, tài	

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	thuộc một dòng thiết bị) trong cùng phân lớp trên mạng	trong vận hành khai thác		liệu thống kê các thiết bị.	
Yêu cầu phát hiện và chống tấn công từ internet	Phải đặt IPS/IDS tại các vùng mạng mà monitor được tất cả các traffic in/out internet Phải đặt Firewall giữa kết nối từ Internet vào mạng nội bộ, đảm bảo toàn bộ traffic in/out internet phải đi qua Firewall	IPS/IDS đặt tại vùng mạng mà toàn bộ traffic in/out tới các hệ thống cần bảo vệ đi qua thì mới phát hiện đủ và đúng các tấn công xâm nhập trái phép tới các hệ thống đó	Phụ lục 14	Kiểm tra mô hình mạng thực tế.	Kế thừa tiêu chuẩn: - CIS Control V7.1 - TLTK 1. - TLTK 2.
Yêu cầu phát hiện và chống tấn công từ nội bộ	Phải đặt IPS/IDS tại các vùng mạng mà monitor được tất cả traffic in/out các hệ thống cần bảo vệ Phải đặt Firewall giữa kết nối từ các hệ thống khác tới hệ thống cần bảo vệ, đảm bảo toàn bộ traffic in/out của vùng mạng cần bảo vệ đi qua Firewall		Phụ lục 14	Kiểm tra mô hình mạng thực tế.	Kế thừa tiêu chuẩn: - CIS Control V7.1 - TLTK 1. - TLTK 2.

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
2. Cấu hình an ninh lớp 1					
Yêu cầu Đóng/Tắt/Shutdow n các cổng (port) không sử dụng	Shutdown tất cả các port không sử dụng trên thiết bị, chỉ bật lên khi có yêu cầu sử dụng	Để ngăn chặn các các thiết bị lạ cắm vào mạng, gây loop, ảnh hưởng đến các giao thức trong mạng và các rủi ro về ATTT	Phụ lục 14	Kiểm tra cấu hình thiết bị.	Tham chiếu một phần tiêu chuẩn: CIS Control V7.1
Yêu cầu mô tả kết nối rõ ràng	Cổng đang bật phải có mô tả kết nối rõ ràng xác định được thông đầu nối của thiết bị đầu xa	Để xác định thông tin về các thiết bị kết nối đầu xa, đảm bảo được sự tin cậy của các kết nối, phục hồi kết nối trong trường hợp bị tấn công làm lỗi phần cứng	Phụ lục 14	Kiểm tra cấu hình thiết bị.	
3. Cấu hình an ninh lớp 2					

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Yêu cầu không sử dụng VLAN default	Bỏ cấu hình VLAN default (thường là VLAN 1) trên các interface	Bỏ cấu hình VLAN default (thường là VLAN 1) trên các interface	Phụ lục 14	Kiểm tra cấu hình thiết bị.	Tham chiếu một phần các tiêu chuẩn: - TLTK 1. - TLTK 2.
Yêu cầu cấu hình chính xác các cổng trunk, cổng access theo đúng thiết kế	Cấu hình chính xác các cổng trunk, cổng access theo đúng thiết kế đã phê duyệt. Đối với cổng trunk phải giới hạn những vlan được phép đi cổng trunk, không cho phép vlan default đi qua	Cấu hình chính xác các cổng trunk, cổng access theo đúng thiết kế đã phê duyệt. Đối với cổng trunk phải giới hạn những vlan được phép đi cổng trunk, không cho phép vlan default đi qua	Phụ lục 14	Kiểm tra cấu hình thiết bị.	
4. Cấu hình an ninh lớp 3					
Xác thực cho các giao thực lớp 3	Các giao thức dự phòng gateway (VRRP, HSRP, GLBP, NSRP...) phải	Để tránh các thiết bị giả mạo kết nối vào	Phụ lục 14	Kiểm tra cấu hình thiết bị.	Tham chiếu một phần các tiêu chuẩn:

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	cấu hình xác thực giữa các thiết bị	mạng mà không cần xác thực với các thiết bị đã có.			- TLTK 1. - TLTK 2.
	Các giao thức IGP (RIP/OSPF/ISIS...) phải thiết lập chuỗi xác thực có mã hóa giữa các thiết bị			Kiểm tra cấu hình thiết bị.	
	Sử dụng chuỗi xác thực mạnh theo chính sách của EVN			Kiểm tra cấu hình thiết bị.	
Yêu cầu kiểm soát định tuyến chính xác	Thực hiện định tuyến (tĩnh/động) chính xác các dải mạng cần tham gia vào quá trình định tuyến. Không định tuyến thừa hoặc định tuyến các dải mạng lớn hơn nhu cầu	Để tối ưu bảng định tuyến, tránh các thông tin định tuyến không cần thiết sẽ tiềm ẩn các nguy cơ mất ATTT		Kiểm tra cấu hình thiết bị.	
	Với các giao thức định tuyến động: Thực hiện chặn quảng bá thông tin định tuyến ra ngoài các port không cần thiết			Kiểm tra cấu hình thiết bị.	

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	(Port đầu xuống khách hàng, thiết bị đầu cuối...)				
Yêu cầu cấu hình bảo mật cho các phiên eBGP với các đối tác, khách hàng bên ngoài	Chặn việc quảng bá/nhận quảng bá các dải IP không hợp lệ và không được định tuyến trên mạng Internet toàn cầu (Các dải IP private, các dải IP dành riêng cho mục đích đặc biệt (ngiên cứu/dự phòng/kiểm thử/...), các dải IP nhỏ hơn subnet /24 với IPv4 và /48 với IPv6...).	Đảm bảo an ninh bảo mật cho phiên eBGP peering với các đối tác, khách hàng bên ngoài. Tuân thủ quy định định tuyến quốc tế.		Kiểm tra cấu hình thiết bị.	
	Giới hạn số lượng các BGP prefix nhận quảng bá từ đối tác/khách hàng.			Kiểm tra cấu hình thiết bị.	
	Chặn việc quảng bá bản tin BGP Update chứa thông tin private AS number ra các đối tác/khách hàng quốc tế.			Kiểm tra cấu hình thiết bị.	

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	Trên các interface đầu nối sử dụng để thiết lập eBGP: Thực hiện filter TCP port 179 (chỉ cho phép các bản tin BGP đến từ địa chỉ BGP neighbor của đối tác/khách hàng, chặn tất cả các bản tin BGP đến từ địa chỉ IP khác)			Kiểm tra cấu hình thiết bị.	
5. Cấu hình quản trị					
Yêu cầu về sao lưu cấu hình	Lưu cấu hình trước khi tác động và định kỳ tối thiểu 01 lần/tuần. Lưu tối thiểu 02 bản gần nhất. Không lưu bản sao lưu trên máy tính cá nhân của quản trị viên	Sao lưu cấu hình đảm bảo phục hồi trong trường hợp sự cố hoặc tấn công thay đổi cấu hình	Phụ lục 14	Kiểm tra cấu hình thiết bị, quy trình tác động hệ thống.	Tham chiếu một phần các tiêu chuẩn: - TLTK 1. - TLTK 2. - CIS Control V7.1
Yêu cầu về quản lý tài khoản	Sử dụng hệ thống AAA để quản lý tài khoản người dùng tập trung	Đối với các thiết bị hỗ trợ khai báo AAA	Phụ lục 14	Kiểm tra cấu hình thiết bị.	Tham chiếu một phần các tiêu chuẩn: - TLTK 1.

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	(xác thực, phân quyền, ghi lịch sử tác động) Tối đa 02 tài khoản quản trị local dùng cho trường hợp khẩn cấp				- TLTK 2. - CIS Control V7.1
	Quản trị viên phải sử dụng tài khoản được cấp riêng, phân quyền phù hợp trên local/AAA	Đảm bảo xác định được đối tượng tác động vào thiết bị đúng chức năng và quyền hạn		Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - TLTK 1.
	Đổi mật khẩu mặc định các tài khoản local của thiết bị	Đảm bảo không bị truy cập trái phép bằng account/password mặc định		Kiểm tra cấu hình thiết bị.	
	Thiết lập chính sách mật khẩu mạnh cho các tài khoản trên local/AAA: - Mật khẩu local trên thiết bị phải được cấu hình mã hóa hoặc ẩn đi trong file cấu hình	Đảm bảo mật khẩu mạnh chống tấn công dò quét mật khẩu		Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - TLTK 1.

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	Khóa sau 5 lần đăng nhập sai, thời gian khóa tài khoản do đăng nhập sai là 10 phút	Để chống tấn công dò quét mật khẩu		Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - TLTK 1.
Yêu cầu về kết nối quản trị	Quản trị thiết bị qua VLAN quản trị dành riêng	Đảm bảo người quản trị kết nối tới thiết bị theo đúng IP và VLAN quy hoạch	Phụ lục 14	Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - CIS Control V7.1
	Quản trị thiết bị qua kết nối trực tiếp Console hoặc kết nối từ xa an toàn, có mã hóa (SSHv2, HTTPS...)	Đảm bảo giao thức kết nối có mã hóa mạnh (nếu thiết bị hỗ trợ)		Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - TLTK 1. - CIS Control V7.1
	Tắt các giao thức quản trị từ xa không an toàn (Telnet, HTTP...)				
	Thời gian timeout của các phiên kết nối quản trị tối đa là 15 phút	Đảm bảo thời gian cho người quản trị tác động vào thiết bị và sẽ bị time-		Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - TLTK 1. - CIS Control V7.1

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
		out khi không sử dụng mà người quản trị không chủ động ngắt			
	Giới hạn chỉ cho phép quản trị từ các IP theo danh sách đăng kí	Đảm bảo chỉ những người quản trị được quyền mới truy cập được vào thiết bị theo quy định		Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - TLTK 1. - TLTK 2.
Yêu cầu cấu hình NTP	Thiết bị phải được đồng bộ thời gian theo tối thiểu 01 máy chủ thời gian (NTP server)	Đề đồng bộ thời gian thực	Phụ lục 14	Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - TLTK 1. - TLTK 2. - CIS Control V7.1
Yêu cầu cấu hình Log	Thiết bị phải được thiết lập bật chế độ ghi log và cấu hình lưu log tập trung tối thiểu 06 tháng cho các hệ thống cấp độ	Trong trường hợp không có hệ thống lưu log tập trung thực hiện thiết lập lưu trên local	Phụ lục 14	Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - TLTK 1. - TLTK 2. - CIS Control V7.1

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	3 theo quy định của Bộ TT&TT.				
Yêu cầu cấu hình SNMP	SNMP phiên bản v2c, v3	Để giám sát trạng thái hoạt động với SNMP v2c hoặc v3 với chế độ chỉ đọc được thông tin thiết bị, có xác thực riêng từ các máy chủ giám sát được phân quyền theo quy định	Phụ lục 14	Kiểm tra cấu hình thiết bị.	Tham chiếu một phần các tiêu chuẩn: - TLTK 1. - TLTK 2.
	SNMP theo chế độ read-only				
	Community string SNMP riêng				
	Xóa bỏ community string mặc định				
	Chỉ cho phép truy cập SNMP từ máy chủ giám sát				
6. Thiết lập các tính năng an ninh					
Yêu cầu bật tính năng phòng chống tấn công mạng trên các Firewall	Bật và cấu hình các tính năng phòng chống tấn công mạng phù hợp với hệ thống CNTT được Firewall bảo vệ (IPS/IDS, UTM, Screening, SSL Inspection (nếu thiết bị	Khi bật các tính năng này cần theo dõi và đánh giá performance của thiết bị	Phụ lục 14	Kiểm tra cấu hình trên các thiết bị Firewall	Kế thừa tiêu chuẩn: - TLTK 1.

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	hỗ trợ và theo chính sách của đơn vị)...				
Yêu cầu rule phát hiện và ngăn chặn các kết nối C&C	Khai báo phát hiện và ngăn chặn các kết nối C&C, các domain độc hại Khai báo rule ở vị trí có hiệu lực đầu tiên	Danh sách C&C và Domain theo khuyến nghị của Cục ATTT – Bộ TT&TT để tránh các máy nhiễm APT kết nối về máy chủ C&C	Phụ lục 14	Kiểm tra khai báo policy trên thiết bị Firewall	Tham chiếu một phần các tiêu chuẩn: - TLTK 1. - TLTK 2. - CIS Control V7.1.
Yêu cầu rule phát hiện và chặn người dùng quản trị ra Internet	Khai báo rule phát hiện và chặn người dùng quản trị ra Internet trực tiếp và qua Proxy, chỉ mở cho người dùng quản trị đến các hệ thống theo các port quản trị TCP-22 (SSH), (TCP-23 (Telnet), TCP-3389 (RDP), 1433 (MS-SQL),	Các kết nối từ người dùng quản trị ra internet hoặc qua proxy đều có tiềm ẩn nguy cơ kết nối tới máy chủ C&C chưa được phát hiện khi máy	Phụ lục 14	Kiểm tra khai báo policy trên thiết bị	Tham chiếu một phần tiêu chuẩn: - CIS Control V7.1.

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	TCP-1521->1527 (Oracle), TCP-3306 (Mysql), TCP-5432 (postgresql), TCP/UDP-161/162 (SMTP)...	người dùng quản trị bị tấn công APT mà các công cụ khác chưa kịp phát hiện và ngăn chặn. Người dùng quản trị chỉ được vào các hệ thống quản trị, mở port khác như người dùng thông thường			
Yêu cầu rule phát hiện và chặn kết nối port quản trị từ vùng có security level thấp sang vùng có security level cao	Khai báo rule phát hiện và chặn kết nối port quản trị từ vùng có security level thấp sang vùng có security level cao: - Internet: Level 1 - Wan: Level 2 - Office: Level 3 - DMZ: Level 4 - Server Farm: Level 5	Chỉ mở các rule quản trị từ vùng mạng Office (vùng mạng Văn phòng) vào DMZ và Server Farm khi có phê duyệt của lãnh đạo có thẩm quyền	Phụ lục 14	Kiểm tra khai báo policy trên thiết bị	Tham chiếu một phần tiêu chuẩn: - TLTK 1. - CIS Control V7.1

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	- ...	Đảm bảo các hệ thống có mức security level thấp hơn không thể quản trị được các hệ thống có mức security level cao hơn			
Yêu cầu rule khai báo Policy vừa đủ các địa chỉ nguồn, địa chỉ đích và port dịch vụ	<p>Với port quản trị:</p> <ul style="list-style-type: none"> - Mở chi tiết và cụ thể theo ip người dùng và hệ thống được cấp phép trên Firewall Office, Firewall WAN - Mở theo dải không quá subnet 24 trên Firewall Server Farm, Firewall DMZ <p>Với các port khác:</p> <ul style="list-style-type: none"> - Mở không quá subnet 16 - Mở không quá range 2000 port 	Đảm bảo việc chỉ người dùng quản trị hệ thống nào được truy cập hệ thống đó, không mở thừa nguồn, đích hoặc port dịch vụ để tránh bị tấn công thông qua các kết nối tunnel giữa các hệ thống. Mở không qua chi	Phụ lục 14	Kiểm tra khai báo policy trên thiết bị	Tham chiếu một phần tiêu chuẩn: - TLTK 2. - CIS Control V7.1

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	Với kết nối internet: - Được phép mở bất kỳ đích đến với kết nối đi internet	tiết để đảm bảo về tài nguyên và hiệu năng của Firewall/IPS/IDS			
Yêu cầu rule khai báo phải chứa các thông tin phục vụ kiểm tra và rà soát ATTT	<ul style="list-style-type: none"> - Khi mở rule cần chú ý mở đúng theo: Title, zone, tags,... - Các rule quan trọng phải bật lưu logs - Các rule cần phải có comment rõ ràng: ngày/tháng/năm mở rule - tên quản trị - rule mở cho mục đích gì - rule mở tạm thời thì cần có thời hạn cụ thể. 	Đảm bảo việc tra cứu lại nhanh và tiện lợi khi cần phải kiểm tra và rà soát các tác động vào thiết bị	Phụ lục 14	Kiểm tra khai báo policy trên thiết bị	Tham chiếu một phần tiêu chuẩn: - CIS Control V7.1
Yêu cầu IPS/IDS phải update bộ rule mới nhất và đầy đủ	IPS/IDS phải update bộ rule mới nhất và đầy đủ được ban hành trên website và hệ thống cập nhật của hãng	Cập nhật tri thức mới nhất của thiết bị để xử lý các lỗi Zero Day và One Day vừa được phát hiện	Phụ lục 14	Kiểm tra trên giao diện quản trị	Kế thừa tiêu chuẩn: - CIS Control V7.1

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
		trong bản cập nhật mới			
Yêu cầu thiết lập gửi mail cảnh báo	Thiết lập gửi mail cảnh báo về người quản trị khi có hành động phát hiện và chặn xâm nhập	Đảm bảo người quản trị theo dõi được hoạt động chặn/lọc của thiết bị (nếu thiết bị có hỗ trợ)	Phụ lục 14	Kiểm tra trên cấu hình thiết bị.	

Điều 20. Quy tắc cấu hình ATTT cho thiết bị mạng

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
1. Yêu cầu chung					
Đưa các thiết bị về trạng thái cấu hình mặc định trước khi triển khai tích hợp vào mạng lưới	Đưa các thiết bị về trạng thái cấu hình mặc định trước khi thực hiện khai báo các cấu hình mới để tích hợp vào mạng lưới	Tránh việc tồn tại các cấu hình thừa, không cần thiết trên thiết bị gây ra các nguy cơ tiềm ẩn mất ATTT	Phụ lục 15	Kiểm tra quy trình triển khai thực tế	
Đảm bảo sử dụng firmware, phần mềm và bản vá không tồn tại lỗi ATTT	Đảm bảo sử dụng firmware, phần mềm và bản vá không có các lỗ hổng ATTT nghiêm trọng đã được công bố trong các CVE	Tránh bị khai thác các lỗ hổng ATTT nghiêm trọng của các thiết bị.	Phụ lục 15	Kiểm tra trong giao diện quản trị thiết bị	Kế thừa tiêu chuẩn: - TLTK 1. - TLTK 2. - CIS Control V7.1.
	Có phương án khắc phục các lỗ hổng tiềm ẩn của thiết bị				

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Đảm bảo tính ổn định của hệ thống	Thống nhất phiên bản hệ điều hành cho tất cả các thiết bị mạng (cùng thuộc một dòng thiết bị) trong cùng phân lớp trên mạng	Đảm bảo hệ thống hoạt động ổn định, đồng bộ, đơn giản trong vận hành khai thác		Kiểm tra chính sách quản lý, tài liệu thống kê các thiết bị.	
2. Cấu hình an ninh lớp 1					
Yêu cầu phải shutdown các port không sử dụng	Shutdown tất cả các port không sử dụng trên thiết bị, chỉ bật lên khi có yêu cầu sử dụng	Để ngăn chặn các thiết bị lạ kết nối vật lý vào mạng, gây loop, ảnh hưởng đến các giao thức trong mạng và các rủi ro về ATTT	Phụ lục 15	Kiểm tra cấu hình thiết bị.	Tham chiếu một phần tiêu chuẩn: CIS Control V7.1 mục 9.2
Yêu cầu mô tả kết nối rõ ràng	Cổng đang bật phải có mô tả kết nối rõ ràng xác định được thông	Để xác định thông tin về các thiết bị kết nối đầu xa, đảm bảo được sự tin	Phụ lục 15	Kiểm tra cấu hình thiết bị.	

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	tin đầu nối của thiết bị đầu xa	cây của các kết nối, phục hồi kết nối trong trường hợp bị tấn công làm lỗi phần cứng			
3. Cấu hình an ninh lớp 2					
Yêu cầu không sử dụng VLAN default	Bỏ cấu hình VLAN default (thường là vlan 1) trên các interface	Ngăn chặn các thiết bị lạ cắm vào mạng có thể sử dụng vlan default để kết nối vào mạng	Phụ lục 15	Kiểm tra cấu hình thiết bị.	Tham chiếu một phần các tiêu chuẩn: - TLTK 1. - TLTK 2.
Yêu cầu cấu hình chính xác các cổng trunk, cổng access theo đúng thiết kế	Cấu hình chính xác các cổng trunk, cổng access theo đúng thiết kế đã phê duyệt	Ngăn chặn các thiết bị kết nối vào mạng qua các vlan không được cho phép như vlan default và các vlan khác ngoài quy hoạch	Phụ lục 15	Kiểm tra thiết kế hệ thống, cấu hình thiết bị.	
	Đối với cổng trunk phải giới hạn những vlan được phép đi cổng		Phụ lục 15	Kiểm tra cấu hình thiết bị.	

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	trunk, không cho phép vlan default đi qua				
Đối với mạng Office phải sử dụng các giải pháp chống tấn công lớp 2	Cấu hình một trong các giải pháp: static mapping địa chỉ IP – địa chỉ MAC, port security, 802.1x	Kiểm soát chính xác thiết bị đầu cuối truy cập mạng	Phụ lục 15	Kiểm tra cấu hình thiết bị.	Tham chiếu một phần các tiêu chuẩn: - TLTK 1. - TLTK 2. - CIS Control V7.1.
	Cấu hình ARP Inspection	Để tránh tấn công ARP Poisoning nếu switch có hỗ trợ tính năng		Kiểm tra cấu hình thiết bị.	
	Cấu hình BPDU guard trên các port access	Để tránh loop mạng nếu switch có hỗ trợ tính năng		Kiểm tra cấu hình thiết bị.	
	Cấu hình isolate port người dùng để ngăn chặn việc các thiết bị kết nối	Để tránh tấn công ngang hàng		Kiểm tra cấu hình thiết bị.	

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	ngang hàng (các port tới gateway, máy in không cấu hình isolate)				
4. Cấu hình an ninh lớp 3					
Yêu cầu xác thực cho các giao thức lớp 3	Các giao thức dự phòng gateway (VRRP, HSRP, GLBP, NSRP...) phải cấu hình xác thực giữa các thiết bị	Để tránh các thiết bị giả mạo kết nối vào mạng mà không cần xác thực với các thiết bị đã có.	Phụ lục 15	Kiểm tra cấu hình thiết bị.	Tham chiếu một phần các tiêu chuẩn: - TLTK 1. - TLTK 2.
	Các giao thức IGP (RIP/OSPF/ISIS..) phải thiết lập chuỗi xác thực có mã hóa giữa các thiết bị			Kiểm tra cấu hình thiết bị.	
	BGP phải thiết lập chuỗi xác thực có mã hóa giữa các peer			Kiểm tra cấu hình thiết bị.	

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Yêu cầu kiểm soát định tuyến chính xác	Sử dụng chuỗi xác thực mạnh.			Kiểm tra cấu hình thiết bị.	
	Tắt các giao thức discovery mạng (ví dụ: như CDP của Cisco)	Để tránh thu thập thông tin mạng		Kiểm tra cấu hình thiết bị.	
	Thực hiện định tuyến (tĩnh/động) chính xác các dải mạng cần tham gia vào quá trình định tuyến. Không định tuyến thừa hoặc định tuyến các dải mạng lớn hơn nhu cầu	Để tối ưu bảng định tuyến, tránh các thông tin định tuyến không cần thiết sẽ tiềm ẩn các nguy cơ mất ATTT	Phụ lục 15	Kiểm tra cấu hình thiết bị.	
	Với các giao thức định tuyến động: Thực hiện chặn quảng bá thông tin định tuyến ra			Kiểm tra cấu hình thiết bị.	

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	ngoài các port không cần thiết (Port đầu xuống khách hàng, thiết bị đầu cuối...)				
Yêu cầu cấu hình bảo mật cho các phiên eBGP với các đối tác, khách hàng bên ngoài	Chặn việc quảng bá/nhận quảng bá các dải IP không hợp lệ và không được định tuyến trên mạng Internet toàn cầu (Các dải IP private, các dải IP dành riêng cho mục đích đặc biệt (nghiên cứu/dự phòng/kiểm thử/...), các dải IP nhỏ hơn subnet /24 với IPv4 và /48 với IPv6...).	Đảm bảo an ninh bảo mật cho phiên eBGP peering với các đối tác, khách hàng bên ngoài. Tuân thủ quy định định tuyến quốc tế.		Kiểm tra cấu hình thiết bị.	

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	Giới hạn số lượng các BGP prefix nhận quảng bá từ đối tác/khách hàng.			Kiểm tra cấu hình thiết bị.	
	Chặn việc quảng bá bản tin BGP Update chứa thông tin private AS number ra các đối tác/khách hàng quốc tế.			Kiểm tra cấu hình thiết bị.	
	Trên các interface đầu nối sử dụng để thiết lập eBGP: Thực hiện filter TCP port 179 (chỉ cho phép các bản tin BGP đến từ địa chỉ BGP neighbor của đối tác/khách hàng, chặn tất cả các			Kiểm tra cấu hình thiết bị.	

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	bản tin BGP đến từ địa chỉ IP khác)				
Yêu cầu tách bảng định tuyến giữa lớp dịch vụ và lớp giám sát thông qua VRF riêng	Thiết bị switch layer 3, router có các interface đầu public phải tách bảng định tuyến giữa lớp dịch vụ và lớp giám sát thông qua VRF riêng cho lưu lượng OAM	Đảm bảo việc phân tách giữa bảng định tuyến lớp dịch vụ và bảng định tuyến lớp giám sát để tránh việc khởi tạo các kết nối tấn công từ lớp dịch vụ đi đến lớp giám sát (Nếu thiết bị hỗ trợ cấu hình VRF)	Phụ lục 15	Kiểm tra cấu hình thiết bị.	Tham chiếu một phần tiêu chuẩn CIS Control V7.1
Yêu cầu bật tính năng DHCP Snooping	Mạng văn phòng sử dụng DHCP cho máy tính người dùng phải	Để tránh tấn công DHCP trong mạng	Phụ lục 15	Kiểm tra cấu hình thiết bị.	.

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	bật tính năng DHCP Snooping				
5. Cấu hình quản trị					
Yêu cầu về sao lưu cấu hình	Lưu cấu hình trước và sau khi tác động và định kì tối thiểu 01 lần/quý. Lưu tối thiểu 02 bản gần nhất. Không lưu bản sao lưu trên máy tính cá nhân của quản trị viên	Sao lưu cấu hình đảm bảo phục hồi trong trường hợp sự cố hoặc tấn công thay đổi cấu hình	Phụ lục 15	Kiểm tra cấu hình thiết bị.	Tham chiếu một phần các tiêu chuẩn: - TLTK 1. - TLTK 2. - CIS Control V7.1.
Yêu cầu về quản lý tài khoản	Khuyến nghị sử dụng hệ thống AAA để quản lý tài khoản người dùng tập trung (xác thực, phân quyền, ghi lịch sử tác động)	Đối với các thiết bị hỗ trợ khai báo AAA	Phụ lục 15	Kiểm tra cấu hình thiết bị.	Tham chiếu một phần các tiêu chuẩn: - TLTK 1. - TLTK 2. - CIS Control V7.1.

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	Tối đa 02 tài khoản quản trị local dùng cho trường hợp khẩn cấp				
	Quản trị viên phải sử dụng tài khoản được cấp riêng, phân quyền phù hợp trên local/AAA	Đảm bảo xác định được đối tượng tác động vào thiết bị đúng chức năng và quyền hạn		Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: TCVN 11930:2017 mục 7.2.1.7. đ)
	Đổi mật khẩu mặc định các tài khoản local của thiết bị	Đảm bảo không bị truy cập trái phép bằng account/password mặc định		Kiểm tra cấu hình thiết bị.	
	Thiết lập chính sách mật khẩu mạnh cho các tài khoản trên local/AAA:	Đảm bảo mật khẩu mạnh chống tấn công dò quét mật khẩu		Kiểm tra cấu hình thiết bị, chính	Kế thừa tiêu chuẩn: - TLTK 1.

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	- Mật khẩu local trên thiết bị phải được cấu hình mã hóa hoặc ẩn đi trong file cấu hình			sách hiện hành.	
	Khóa sau 5 lần đăng nhập sai, thời gian khóa tài khoản do đăng nhập sai là 10 phút	Để chống tấn công dò quét mật khẩu		Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - TLTK 1.
Yêu cầu về kết nối quản trị	Quản trị thiết bị qua VLAN quản trị dành riêng	Đảm bảo người quản trị kết nối tới thiết bị theo đúng ip và vlan quy hoạch	Phụ lục 15	Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - CIS Control V7.1.
	Quản trị thiết bị qua kết nối trực tiếp Console hoặc kết nối từ xa an toàn, có mã hóa (SSHv2, HTTPS...),	Đảm bảo giao thức kết nối có mã hóa mạnh (Nếu thiết bị hỗ trợ)		Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - TLTK 2. - CIS Control V7.1.

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	Tắt các giao thức quản trị từ xa không an toàn (Telnet, HTTP...)			Kiểm tra cấu hình thiết bị.	
	Thời gian timeout của các phiên kết nối quản trị tối đa là 15 phút.	Đảm bảo thời gian cho người quản trị tác động vào thiết bị và sẽ bị timeout khi không sử dụng mà người quản trị không chủ động ngắt		Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - TLTK 2. - CIS Control V7.1.
	Giới hạn chỉ cho phép quản trị từ các IP theo danh sách đăng ký	Đảm bảo chỉ những người quản trị được quyền mới truy cập được vào thiết bị theo quy định		Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - TLTK 1. - TLTK 2.

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
Yêu cầu cấu hình NTP	Đồng bộ thời gian theo tối thiểu 01 máy chủ thời gian (NTP server)	Để đồng bộ thời gian thực	Phụ lục 15	Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - TLTK 1. - TLTK 2. - CIS Control V7.1.
Yêu cầu cấu hình Log	Thiết bị phải được thiết lập bật chế độ ghi log và cấu hình lưu log tập trung tối thiểu 06 tháng cho các hệ thống cấp độ 3 theo quy định của bộ Thông tin Truyền thông	Trong trường hợp không có hệ thống lưu log tập trung thực hiện thiết lập lưu trên local	Phụ lục 15	Kiểm tra cấu hình thiết bị.	Kế thừa tiêu chuẩn: - TLTK 1. - TLTK 2. - CIS Control V7.1.
Yêu cầu cấu hình SNMP	SNMP phiên bản v2c, v3	Để giám sát trạng thái hoạt động với snmp v2c hoặc v3 với chế độ chỉ đọc được thông tin	Phụ lục 15	Kiểm tra cấu hình thiết bị.	Tham chiếu một phần các tiêu chuẩn: - TLTK 1. - TLTK 2.
	SNMP theo chế độ read-only				
	Community string SNMP riêng				

Nội dung quy tắc	Yêu cầu	Mô tả	Hướng dẫn tham khảo	Cách kiểm tra	Tài liệu tham chiếu
	Xóa bỏ community string mặc định	thiết bị, có xác thực riêng từ các máy chủ giám sát được phân quyền theo quy định			
	Chỉ cho phép truy cập SNMP từ máy chủ giám sát				

