BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập – Tự do – Hạnh phúc
Số: /QĐ-BTTTT	*Hà Nội, ngày tháng năm 2022*

QUYẾT ĐỊNH
Ban hành Yêu cầu an toàn cơ bản đối với Phần mềm nội bộ

BỘ TRƯỞNG BỘ THÔNG TIN VÀ TRUYỀN THÔNG

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

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 24/2020/TT-BTTTT ngày 09 tháng 9 năm 2020 của Bộ Thông tin và Truyền thông quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

Theo đề nghị của Cục trưởng Cục An toàn thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Yêu cầu an toàn cơ bản đối với Phần mềm nội bộ.

Điều 2. Khuyến nghị cơ quan, tổ chức nghiên cứu, phát triển, lựa chọn, sử dụng Phần mềm nội bộ đáp ứng các yêu cầu an toàn cơ bản theo Điều 1 Quyết định này.

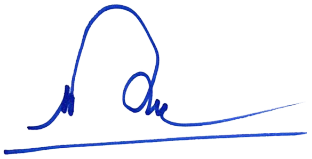
Điều 3. Cục An toàn thông tin chủ trì, phối hợp với các cơ quan, tổ chức liên quan hướng dẫn việc áp dụng các yêu cầu trong Yêu cầu an toàn cơ bản đối với Phần mềm nội bộ tại Điều 1 Quyết định này.

Điều 4. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 5. Chánh Văn phòng, Cục trưởng Cục An toàn thông tin, Thủ trưởng các đơn vị thuộc Bộ, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 5;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Cổng thông tin điện tử của Bộ;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG



Nguyễn Huy Dũng

YÊU CẦU AN TOÀN CƠ BẢN ĐỐI VỚI PHẦN MỀM NỘI BỘ

(Kèm theo Quyết định số /QĐ-BTTTT ngày tháng năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông)

I. THÔNG TIN CHUNG

1. Phạm vi áp dụng

Nội dung tại Quyết định này đưa ra các yêu cầu an toàn thông tin cơ bản đối với Phần mềm nội bộ nhằm đáp ứng các yêu cầu an toàn liên quan đến ứng dụng và dữ liệu theo Thông tư 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ Thông tin và Truyền thông và Tiêu chuẩn TCVN 11930:2017.

2. Đối tượng áp dụng

Cơ quan, tổ chức liên quan đến việc phát triển, kiểm thử Phần mềm nội bộ trong dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

3. Khái niệm và thuật ngữ

Trong tài liệu này các khái niệm được tham chiếu trong Tiêu chuẩn quốc gia TCVN 11930:2017.

Khái niệm Phần mềm nội bộ được hiểu như sau: Phần mềm nội bộ là phần mềm được xây dựng, phát triển, nâng cấp, mở rộng theo các yêu cầu riêng của tổ chức hoặc người sử dụng nhằm đáp ứng yêu cầu đặc thù của tổ chức hoặc người sử dụng đó.

II. YÊU CẦU AN TOÀN CƠ BẢN

1. Yêu cầu về tài liệu

Phần mềm nội bộ có tài liệu bao gồm các nội dung sau:

a) Hướng dẫn triển khai và thiết lập cấu hình;

b) Hướng dẫn sử dụng và quản trị;

c) Tài liệu thiết kế;

d) Mã nguồn sản phẩm (theo yêu cầu của bên đề nghị đánh giá).

2. Yêu cầu về quản lý điểm yếu an toàn thông tin

Trước khi thực hiện nghiệm thu và bàn giao, Phần mềm nội bộ không tồn tại lỗ hổng, điểm yếu được đánh giá và xác nhận bởi tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép hoặc tổ chức sự nghiệp nhà nước có chức năng,

nhiệm vụ phù hợp do chủ quản hệ thống thông tin chỉ định thực hiện theo quy định của pháp luật.

3. Yêu cầu về chức năng Xác thực

3.1. Chức năng Xác thực đối với Phần mềm nội bộ bao gồm:

a) Xác thực người sử dụng khi truy cập, quản trị, cấu hình Phần mềm;

b) Có chức năng cho phép lưu trữ có mã hóa thông tin xác thực hệ thống sử dụng thuật toán hash từ SHA-256, SHA-512, SHA-3 và các thuật toán tương đương;

c) Có chức năng cho phép thiết lập chính sách mật khẩucủa tài khoản;

d) Có chức năng cho phép hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định;

đ) Có chức năng cho phép mã hóa thông tin xác thực trước khi gửi qua môi trường mạng;

e) Có chức năng cho phép sử dụng cơ chế xác thực đa nhân tố để xác thực người sử dụng.

3.2. Yêu cầu cụ thể đối với từng chức năng xác thực ở trên, khi Phần mềm được triển khai trên hệ thống thông tin theo từng cấp độ được tham chiếu chi tiết tại Mục 1, Phụ lục kèm theo.

4. Yêu cầu về chức năng Kiểm soát truy cập

4.1. Chức năng Kiểm soát truy cập đối với Phần mềm nội bộ bao gồm:

a) Có chức năng cho phép thiết lập giới hạn thời gian chờ (timeout);

b) Có chức năng cho phép giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị Phần mềm từ xa;

c) Có chức năng cho phép phân quyền và cấp quyền tối thiểu về truy cập, quản trị, sử dụng tài nguyên khác nhau của Phần mềm với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau;

d) Có chức năng cho phép thiết lập quyền tối thiểu (quyền truy cập, quản trị) cho tài khoản quản trị ứng dụng theo quyền hạn;

đ) Có chức năng cho phép thay đổi, tách biệt cổng quản trị ứng dụng với cổng cung cấp dịch vụ ứng dụng;

e) Có chức năng cho phép khóa tạm thời quản trị ứng dụng trong khoảng thời

gian ngoài giờ làm việc.

4.2. Yêu cầu cụ thể đối với từng chức năng Kiểm soát truy cập ở trên, khi Phần mềm được triển khai trên hệ thống thông tin theo từng cấp độ được tham chiếu chi tiết tại Mục 2, Phụ lục kèm theo.

5. Yêu cầu về chức năng Nhật ký hệ thống

5.1. Chức năng Nhật ký hệ thống đối với Phần mềm nội bộ bao gồm:

a) Có chức năng cho phép ghi nhật ký hệ thống gồm những thông tin:

i. Thời điểm sinh nhật ký;

ii. Phân nhóm nhật ký;

iii. Mô tả thao tác/lỗi;

iv. Đối tượng thực hiện thao tác/sinh lỗi;

v. Mức độ quan trọng.

b) Có chức năng cho phép quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung;

c) Có chức năng cho phép phân quyền truy cập, quản lý dữ liệu nhật ký hệ thống đối với các tài khoản có chức năng quản trị hệ thống khác nhau.

5.2. Yêu cầu cụ thể đối với từng chức năng Nhật ký hệ thống ở trên khi Phần mềm được triển khai trên hệ thống thông tin theo từng cấp độ được tham chiếu chi tiết tại Mục 3, Phụ lục kèm theo.

6. Yêu cầu về An toàn ứng dụng và mã nguồn

6.1. Yêu cầu về An toàn ứng dụng và mã nguồn đối với Phần mềm nội bộ bao gồm:

a) Có chức năng cho phép kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý;

b) Có chức năng cho phép bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF;

c) Có chức năng cho phép kiểm soát lỗi, thông báo lỗi từ ứng dụng;

d) Có chức năng cho phép bảo đảm không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng.

6.2. Yêu cầu cụ thể đối với từng chức năng An toàn ứng dụng và mã nguồn

ở trên khi Phần mềm được triển khai trên hệ thống thông tin theo từng cấp độ được tham chiếu chi tiết tại Mục 4, Phụ lục kèm theo.

7. Yêu cầu về chức năng Bảo mật thông tin liên lạc

7.1. Chức năng Bảo mật thông tin liên lạc đối với Phần mềm nội bộ bao gồm:

a) Có chức năng cho phép mã hóa thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trước khi truyền đưa, trao đổi qua môi trường mạng;

b) Có chức năng cho phép sử dụng chữ ký số được cung cấp bởi cơ quan có thẩm quyền để bảo vệ dữ liệu và chống chối bỏ (đối với các ứng dụng yêu cầu sử dụng chữ ký số).

7.2. Yêu cầu cụ thể đối với từng chức năng Bảo mật thông tin liên lạc ở trên khi Phần mềm được triển khai trên hệ thống thông tin theo từng cấp độ được tham chiếu chi tiết tại Mục 5, Phụ lục kèm theo.

8. Yêu cầu về chức năng Sao lưu dự phòng

8.1. Chức năng Sao lưu dự phòng đối với Phần mềm nội bộ bao gồm:

a) Có chức năng cho phép tự động sao lưu dự phòng;

b) Có chức năng cho phép gán nhãn loại dữ liệu được lưu trữ theo quy tắc được thiết lập;

c) Có chức năng cho phép thiết lập cấu hình để gửi dữ liệu dự phòng về hệ thống lưu trữ tập trung.

8.2. Yêu cầu cụ thể đối với từng chức năng Sao lưu dự phòng ở trên khi Phần mềm được triển khai trên hệ thống thông tin theo từng cấp độ được tham chiếu chi tiết tại Mục 6, Phụ lục kèm theo.

PHỤ LỤC

YÊU CẦU AN TOÀN CƠ BẢN CHO PHẦN MỀM NỘI BỘ

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
1.	**Xác thực**						
1.1	Có chức năng xác thực người sử dụng khi truy cập, quản trị, cấu hình Phần mềm.	a) Có giao diện quản lý tài khoản người sử dụng.	x	x	x	x	x
		b) Yêu cầu xác thực người sử dụng khi truy cập quản trị, cấu hình Phần mềm.	x	x	x	x	x
		c) Yêu cầu xác thực người sử dụng khi truy truy cập sử dụng Phần mềm.	x	x	x	x	x
1.2	Có chức năng cho phép lưu trữ có mã hóa thông tin xác thực hệ thống.	Thông tin xác thực được lưu trữ có mã hóa trên Phần mềm sử dụng thuật toán hash từ SHA-256, SHA-512, SHA-3 và các thuật toán tương đương	x	x	x	x	x
1.3	Có chức năng cho phép thiết lập chính sách mật khẩu người sử dụng.	a) Có chức năng yêu cầu người dùng đặt mật khẩu mới khi đăng nhập lần đầu sử dụng mật khẩu mặc định.	x	x	x	x	x
		b) Có chức năng cho phép thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự.	x	x	x	x	x

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
		c) Có chức năng cho phép thiết lập thời gian yêu cầu thay đổi mật khẩu.		x	x	x	x
		d) Có chức năng cho phép thiết lập thời gian mật khẩu hợp lệ.		x	x	x	x
		đ) Khóa tài khoản và yêu cầu nhập mật khẩu mới khi mật khẩu của tài khoản đó hết hạn thời gian hợp lệ.		x	x	x	x
		e) Mở khóa tài khoản khi thay đổi mật khẩu thành công đối với trường hợp mật khẩu hết hạn thời gian hợp lệ.		x	x	x	x
1.4	Có chức năng cho phép hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định.	a) Có giao diện cho phép thiết lập chính sách về giới hạn số lần đăng nhập sai trong khoảng thời gian nhất định.		x	x	x	x
		b) Có chức năng cảnh báo tới người sử dụng khi vi phạm chính sách.		x	x	x	x
		c) Có chức năng tự động ngăn cản việc đăng nhập tự động khi vi phạm chính sách trên.		x	x	x	x

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
		đ) Có chức năng tự động vô hiệu hóa tài khoản nếu vi phạm chính sách trên.			x	x	x
1.5	Có chức năng cho phép mã hóa thông tin xác thực trước khi gửi qua môi trường mạng.	Chức năng bảo đảm mật khẩu được mã hóa trước khi gửi qua môi trường mạng.			x	x	x
1.6	Có chức năng cho phép sử dụng cơ chế xác thực đa nhân tố để xác thực người sử dụng.	a) Có giao diện cho phép quản trị viên quản lý chính sách về xác thực đa nhân tố.				x	x
		b) Tích hợp các bước xác thực đa nhân tố khi chính sách đối với trường hợp này được kích hoạt.				x	x
2.	**Kiểm soát truy cập**						
2.1	Có chức năng cho phép thiết lập giới hạn thời gian chờ (timeout).	a) Có chức năng cho phép thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi Phần mềm không nhận được yêu cầu từ người dùng.	x	x	x	x	x

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
		b) Hiển thị thông báo, đóng phiên kết nối đã hết hạn thời gian timeout và yêu cầu đăng nhập lại.		x	x	x	x
2.2	Có chức năng cho phép giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị Phần mềm từ xa.	a) Có giao diện cho phép quản trị viên quản lý chính sách về giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị Phần mềm từ xa.		x	x	x	x
		b) Có chức năng thực thi chính sách về giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị Phần mềm từ xa ở trên.		x	x	x	x
2.3	Có chức năng cho phép phân quyền và cấp quyền tối thiểu truy cập, quản trị, sử dụng tài nguyên khác nhau của Phần mềm với người sử dụng/ nhóm người sử dụng	a) Có giao diện cho phép quản trị viên quản lý chính sách về phân quyền tài khoản theo từng nhóm tài khoản.			x	x	x
		b) Phân loại nhóm tài khoản theo ít nhất 03 nhóm: i. Tài khoản người sử dụng thông thường;			x	x	x

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
	có chức năng, yêu cầu nghiệp vụ khác nhau.	ii. Tài khoản quản trị mức sử dụng; iii. Tài khoản quản trị mức phát triển, vận hành.					
		c) Có chức năng thực thi chính sách phân quyền và cấp quyền tối thiểu truy cập, quản trị, sử dụng tài nguyên khác nhau ở trên.			x	x	x
2.4	Có chức năng cho phép thiết lập quyền tối thiểu (quyền truy cập, quản trị) cho tài khoản quản trị ứng dụng theo quyền hạn.	a) Có giao diện cho phép quản trị viên thiết lập quyền cho các tài khoản.			x	x	x
		b) Có chức năng thực thi chính sách phân quyền cho các tài khoản ở trên.			x	x	x
2.5	Có chức năng cho phép thay đổi, tách biệt cổng quản trị ứng dụng với cổng cung cấp dịch vụ ứng dụng.	c) Có giao diện cho phép quản trị viên quản lý chính sách về cổng quản trị ứng dụng và cổng cung cấp dịch vụ ứng dụng.					x
		b) Có chức năng thực thi chính sách tách biệt cổng quản trị ứng dụng					x

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
		với cổng cung cấp dịch vụ ứng dụng ở trên.					
2.6	Có chức năng cho phép khóa tạm thời quản trị ứng dụng trong khoảng thời gian ngoài giờ làm việc.	a) Có giao diện cho phép quản trị viên quản lý chính sách về khoảng thời gian được phép thực hiện thao tác quản trị.					x
		b) Có chức năng thực thi chính sách về khoảng thời gian được phép thực hiện thao tác quản trị hệ thống ở trên.					x
3.	**Nhật ký hệ thống**						
3.1	Có chức năng cho phép ghi nhật ký hệ thống gồm những thông tin.	a) Phần mềm cung cấp chức năng ghi nhật ký hệ thống.	x	x	x	x	x
		b) Nhật ký hệ thống được phân loại theo ít nhất 05 nhóm: i. Nhật ký truy cập Phần mềm; ii. Nhật ký đăng nhập khi quản trị Phần mềm; iii. Nhật ký các lỗi phát sinh trong quá trình hoạt động;			x	x	x

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
		iv. Nhật ký quản lý tài khoản; v. Nhật ký thay đổi cấu hình Phần mềm					
3.2	Có chức năng cho phép quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung.	a) Có giao diện cho phép quản trị viên quản lý chính sách về nhật ký hệ thống.			x	x	x
		b) Cho phép quản trị viên cấu hình khoảng thời gian lưu trữ nhật ký qua giao diện trên.			x	x	x
		c) Lưu trữ nhật ký với ít nhất 05 thông tin: i. Thời điểm sinh nhật ký; ii. Phân nhóm nhật ký; iii. Mô tả thao tác/lỗi; iv. Đối tượng thực hiện thao tác/sinh lỗi; v. Mức độ quan trọng.			x	x	x
3.3	Có chức năng cho phép phân quyền truy cập, quản lý dữ liệu nhật ký hệ thống đối với các tài	a) Có giao diện cho phép quản trị viên quản lý chính sách về phân quyền tài khoản theo từng nhóm tài khoản quản trị.					x

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
	khoản có chức năng quản trị hệ thống khác nhau.	b) Có chức năng thực thi chính sách phân quyền ở trên.					x
4.	**An toàn ứng dụng và mã nguồn**						
4.1	Có chức năng cho phép kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý.	Có chức năng thực thi việc kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý	x	x	x	x	x
4.2	Có chức năng cho phép bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF	Phần mềm được kiểm tra, đánh giá, kiểm thử xâm nhập theo tiêu chuẩn OWASP và không tồn tại điểm yếu cho phép kẻ tấn công khai thác thông qua các dạng tấn công: SQL Injection, OS command injection, RFI, LFI, Xpath Injection, XSS, CSRF.			x	x	x
4.3	Có chức năng cho phép kiểm soát lỗi, thông báo lỗi từ ứng dụng.	a) Có chức năng kiểm soát lỗi, chỉ hiển thị các thông báo lỗi được kiểm soát đến người dùng và không hiển thị các lỗi bên trong hệ thống.			x	x	x

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
		b) Có chức năng hiển thị thông báo lỗi đến người sử dụng.			x	x	x
4.4	Có chức năng cho phép bảo đảm không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng.	a) Thông tin xác thực, bí mật không được đưa trực tiếp vào mã nguồn ứng dụng mà phải được thiết lập thông qua giao diện cấu hình hệ thống.		x	x	x	x
5.	**Bảo mật thông tin liên lạc**						
5.1	Có chức năng cho phép mã hóa thông tin, dữ liệu trước khi truyền đưa, trao đổi qua môi trường mạng (đối với các ứng dụng yêu cầu sử dụng chữ ký số).	Có chức năng cho phép mã hóa dữ liệu trước khi truyền đưa, trao đổi qua môi trường mạng sử dụng chữ ký số.			x	x	x
6.	**Sao lưu dự phòng**						
6.1	Có chức năng cho phép tự động sao lưu dự phòng.	a) Có giao diện cho phép quản trị viên thiết lập chính sách về sao lưu dự phòng cơ sở dữ liệu và cấu hình hệ thống.			x	x	x
		b) Có chức năng cho phép thực hiện việc sao			x	x	x

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
		lưu dự phòng theo chính sách ở trên.					
6.2	Có chức năng cho phép phép gán nhãn loại dữ liệu được lưu trữ theo quy tắc được thiết lập.	a) Có giao diện cho phép quản trị viên quản lý chính sách về phân loại dữ liệu được lưu trữ theo từng nhóm dữ liệu.				x	x
		b) Có chức năng cho phép lưu trữ dữ liệu theo tên định dạng đối với từng loại dữ liệu tại mục trên.				x	x
6.3	Có chức năng cho phép thiết lập cấu hình để gửi dữ liệu dự phòng về hệ thống lưu trữ tập trung.	a) Có giao diện cho phép quản trị viên thiết lập cấu hình để gửi dữ liệu dự phòng về hệ thống lưu trữ tập trung.					x
		b) Có chức năng cho phép thực hiện sao lưu dự phòng thủ công cơ sở dữ liệu và cấu hình hệ thống lên hệ thống lưu trữ tập trung.					x
		c) Có chức năng cho phép thực hiện sao lưu dự phòng tự động cơ sở dữ liệu và cấu hình hệ thống lên hệ thống lưu trữ tập trung.					x

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
		d) Có chức năng cho phép khôi phục dữ liệu, cấu hình hệ thống từ dữ liệu được lưu trữ trên hệ thống lưu trữ tập trung.					x