**TCVN** **TIÊU CHUẨN QUỐC GIA**

# TCVN XXXX:XXXX

**Xuất bản lần 1**

# CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – YÊU CẦU CƠ BẢN VỀ AN TOÀN HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ

**HÀ NỘI – 2016**

**Mục lục**

## Lời nói đầu

TCVN xxxx đưa ra các yêu cầu an toàn cơ bản về an toàn hệ thống thông tin theo từng cấp độ.

TCVN xxxx:2015 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.

# Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ

## 1 Phạm vi áp dụng

Tiêu chuẩn này đưa ra các yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ. Yêu cầu an toàn cơ bản đưa ra các yêu cầu cần thiết, tối thiểu phải áp dụng để bảo đảm an toàn hệ thống thông tin theo cấp độ. Tổ chức có thể căn cứ vào yêu cầu thực tế của mình để xác định các yêu cầu an toàn bổ sung đáp ứng các mục tiêu đặt ra.

Tiêu chuẩn này có thể áp dụng cho tất cả các tổ chức. Sau khi, tổ chức đánh giá, xác định được cấp độ an toàn của hệ thống thông tin của mình sẽ căn cứ vào các yêu cầu an toàn cơ bản trong tiêu chuẩn này để thiết kế và áp dụng các biện pháp bảo đảm an toàn thông tin cho hệ thống thông tin của mình theo cấp độ đã xác định được.

Yêu cầu an toàn cơ bản bao gồm hai nhóm yêu cầu: yêu cầu về kỹ thuật và yêu cầu về quản lý. Nhóm yêu cầu về kỹ thuật giúp tổ chức, cá nhân có cơ sở thiết kế an toàn hệ thống thông tin của mình trong quá trình xây dựng hệ thống thông tin cũng như việc kiểm tra, đánh giá an toàn hệ thống thông tin của mình trong quá trình vận hành, khai thác, sử dụng. Nhóm các yêu cầu về quản lý giúp tổ chức, cá nhân có cơ sở để xây dựng các chính sách quản lý an toàn thông tin cho hệ thống của mình trong quá trình vận hành, khai thác, sử dụng.

Yêu cầu an toàn cơ bản đưa ra trong tiêu chuẩn này tập trung vào các yêu cầu bảo đảm an toàn mạng. Các yêu cầu an toàn khác như an toàn vật lý sẽ được tham khảo ở các tiêu chuẩn khác.

## 2 Tài liệu viện dẫn

TCVN ISO/IEC 27001:2007 ISO/IEC 27001:2005 “Công nghệ thông tin - Kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin – Các yêu cầu” (Information Technology – Security techniques – Information security management system – Requirements)

SP800-53 R4, Security and Privacy Controls for Federal Information Systems and Organizations

## 3 Thuật ngữ và định nghĩa

3.1

An toàn thông tin

Sự bảo vệ thông tin và hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

3.2

Hệ thống thông tin

Tập hợp thiết bị phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin.

3.3

Cấp độ an toàn hệ thống thông tin

Mức độ an toàn cần bảo đảm đối với một hệ thống thông tin; hệ thống thông tin càng quan trọng thì cấp độ an toàn thông tin càng cao.

3.4

Xâm phạm an toàn thông tin

Hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, làm sai lệch chức năng, phá hoại trái phép thông tin và hệ thống thông tin

3.5

Chủ quản hệ thống thông tin

Tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin của mình.

3.6

Mạng

Khái niệm chung dùng để chỉ mạng viễn thông, Internet và mạng máy tính.

3.7

Rủi ro an toàn thông tin

Những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin.

3.8

Đánh giá rủi ro an toàn thông tin

Việc phát hiện, phân tích, ước lượng mức độ tổn hại, mối đe dọa đối với thông tin và hệ thống thông tin.

3.7

Dịch vụ an toàn thông tin

Dịch vụ bảo vệ thông tin và hệ thống thông tin cho tổ chức, cá nhân.

3.10

Phần mềm độc hại

Phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

3.11

Tính khả dụng

Tính chất bảo đảm tính sẵn sàng của thông tin khi cần truy nhập và sử dụng theo yêu cầu.

3.12

Tính bí mật

Tính chất bảo đảm thông tin không bị tiết lộ, lộ lọt và sử dụng trái phép.

3.13

Tính nguyên vẹn

Tính chất bảo đảm thông tin không bị can thiệp, sửa đổi trái phép.

3.14

Sự cố mất an toàn thông tin

Việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính bảo mật, tính nguyên vẹn hoặc tính khả dụng.

3.15

Hệ thống quản lý an toàn thông tin

Một phần của hệ thống quản lý toàn diện, dựa trên các rủi ro có thể xuất hiện trong hoạt động của tổ chức để thiết lập, triển khai, điều hành, giám sát, soát xét, duy trì và cải tiến an toàn thông tin.

3.16

Mối đe dọa

Nguyên nhân tiềm ẩn gây ra sự cố không mong muốn, có thể gây tổn hại cho một hệ thống

hoặc tổ chức.

3.17

Chính sách quản lý an toàn

Quy định, quy tắc, quy trình quản lý, khai thác, vận hành và sử dụng hệ thống thông tin bảo đảm an toàn thông tin.

3.18

Khu vực hệ thống

Khu vực phòng máy chủ hoặc khu vực quản trị, vận hành và khai thác sử dụng hệ thống thông tin.

3.17

Thiết bị mạng chính

Thiết bị gây lên gián đoạn hoạt động của toàn bộ hệ thống khi xảy ra sự cố như: thiết bị chuyển mạch trung tâm, thiết bị định tuyến, tường lửa…

3.20

Hệ thống lọc phần mềm độc hại

Tập hợp phần cứng, phần mềm được kết nối vào mạng để phát hiện, ngăn chặn, lọc và thống kê phần mềm độc hại

3.21

Phần mềm phòng, chống mã độc

Phần mềm được cài đặt trên máy tính, có chức năng phát hiện, cảnh báo và xử lý phần mềm độc hại.

3.22

Hồ sơ cấp độ hệ thống

Hồ sơ, tài liệu liên quan đến việc đánh giá và xác định cấp đô an toàn hệ thống thông tin.

3.23

Khu vực xử lý trung tâm

Nơi được thiết lập để đặt, để, bảo vệ thiết bị mạng chính, máy chủ của hệ thống trong phòng máy chủ hoặc trung tâm dữ liệu.

3.24

Kết nối mạng bảo mật

Là kết nối mạng sử dụng các phương pháp mã hóa, xác thực và nguyên vẹn thông tin như SSH,SSL, VPN….

# 4 Tổng quan về bảo đảm an toàn hệ thống thông tin theo cấp độ

## 4.1 Yêu cầu kỹ thuật và yêu cầu quản lý cơ bản

Các yêu cầu của từng cấp độ được chia làm 2 nhóm yêu cầu bao gồm: yêu cầu về kỹ thuật và yêu cầu về quản lý.

Yêu cầu về kỹ thuật cơ bản bao gồm các yêu cầu về bảo đảm an toàn hạ tầng mạng, bảo mật máy chủ, ứng dụng bảo mật và an toàn dữ liệu. Để đạt được các yêu cầu kỹ thuật, hệ thống thông tin cần phải triển khai thiết lập hạ tầng kỹ thuật; thiết lập hệ thống phần cứng, phần mềm; cấu hình thiết lập các chính sách quản lý an toàn cần thiết cho hệ thống.

Yêu cầu về quản lý an toàn bao gồm các yêu cầu về chính sách quản lý an toàn, tổ chức quản lý an toàn, quản lý nhân lực, quản lý xây dựng hệ thống thông tin, quản lý vận hành hệ thống.

## 4.2 Ba loại yêu cầu cơ bản

Yêu cầu an toàn được chia ra làm 3 loại cơ bản. Loại yêu cầu bảo đảm an toàn thông tin chung cho cả hệ thống như yêu cầu môi trường vật lý, hạ tầng mạng được ký hiệu là G. Loại yêu cầu liên quan đến bảo mật thông tin dữ liệu như mã hóa dữ liệu, chống sửa xóa thay đổi thông tin được ký hiệu là S. Loại yêu cầu liên quan đến tính khả dụng của dữ liệu như khả năng phục hồi, sao lưu dự phòng được ký hiệu là A.

Trong tiêu chuẩn này các yêu cầu cơ bản được đánh nhãn theo các ký hiệu trên theo từng cấp độ an toàn của hệ thống thông tin.

# 5 Yêu cầu cơ bản cho cấp độ 1

## 5.1 Yêu cầu kỹ thuật

### 5.1.1 Bảo đảm an toàn hạ tầng mạng

#### 5.1.1.1 Thiết kế hệ thống (G1)

Yêu cầu bao gồm:

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, bao gồm cơ bản cơ bản các vùng mạng:

- Vùng mạng nội bộ (LAN)

- Vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác (Outside)

- Vùng mạng máy chủ công cộng (DMZ)

b) Phương án thiết kế bảo đảm các yêu cầu sau:

- Cung cấp khả năng truy nhập, quản trị hệ thống từ xa an toàn,

- Có biện pháp quản lý truy nhập và phòng chống xâm nhập.

#### 5.1.1.2 Kiểm soát truy nhập từ bên ngoài mạng (G1)

Yêu cầu bao gồm:

a) Thiết lập hệ thống chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương, khi truy nhập quản trị hệ thống, quản lý và sử dụng tài nguyên nội bộ trong hệ thống từ các mạng bên ngoài;

b) Kiểm soát truy nhập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép từ bên ngoài.

#### 5.1.1.3 Kiểm soát truy nhập từ bên trong mạng (S1)

Cho phép truy nhập ra bên ngoài các địa chỉ Internet, ứng dụng, dịch vụ theo yêu cầu nghiệp vụ; chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức.

#### 5.1.1.4 Phòng chống xâm nhập (G1)

a) Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng máy chủ công cộng;

b) Tự động cập nhật thời gian thực cơ sở dữ liệu, dấu hiệu phát hiện tấn công.

#### 5.1.1.5 Bảo vệ thiết bị hệ thống(G1)

Yêu cầu bao gồm:

a) Cấu hình chức năng xác thực trên các thiết bị hệ thống để xác thực người dùng sử dụng quản trị thiết bị trực tiếp hoặc từ xa;

b) Thiết lập hệ thống chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản trị thiết bị.

### 5.1.2 Bảo đảm an toàn máy chủ

#### 5.1.2.1 Xác thực (S1)

a) Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng sử dụng khi khi truy nhập, quản lý và sử dụng máy chủ;

b) Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng).

#### 5.1.2.2 Kiểm soát truy nhập (S1)

Thiết lập hệ thống chỉ chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản trị máy chủ từ xa thông qua môi trường mạng;

#### 5.1.2.3 Nhật ký hệ thống (G1)

Yêu cầu bao gồm:

a) Ghi nhật ký hệ thống bao gồm những thông tin cơ bản theo yêu cầu thực tế;

b) Đồng bộ thời gian giữa máy chủ với máy chủ thời gian;

#### 5.1.2.4 Phòng chống xâm nhập (G1)

Yêu cầu bao gồm:

a) Loại bỏ các tài khoản không sử dụng và các tài khoản không còn hợp lệ trên máy chủ;

b) Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng;

c) Thiết lập hệ thống chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi kết nối, truy nhập, quản trị máy chủ từ xa.

#### 5.1.2.5 Phòng chống phần mềm độc hại (G1)

Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm.

### 5.1.3 Bảo đảm an toàn ứng dụng

#### 5.1.3.1 Xác thực (S1)

Yêu cầu bao gồm:

a) Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi quản trị, cấu hình cấu hình ứng dụng và sử dụng ứng dụng (nếu ứng dụng cần quản lý truy nhập);

b) Lưu trữ mã hóa thông tin xác thực trên hệ thống.

#### 5.1.3.2 Kiểm soát truy nhập (S1)

Thiết lập hệ thống chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản trị ứng dụng từ xa thông qua môi trường mạng;

### 5.1.4 An toàn dữ liệu

#### 5.1.4.3 Sao lưu dự phòng (A1)

Thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, sơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

Có hệ thống/phương tiện sao lưu dự phòng độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để lưu trữ dự phòng.

## 5.2 Yêu cầu quản lý

### 5.2.1 Chính sách an toàn thông tin

#### 5.2.1.1. Chính sách an toàn thông tin (G1)

Bao gồm các yêu cầu sau:

a) Xây dựng chính sách an toàn thông tin cơ bản cho người sử dụng bao gồm:

- Chính sách truy nhập mạng và tài nguyên trên Internet

- Cài đặt và sử dụng máy tính an toàn

b) Xây dựng chính sách an toàn thông tin cho người quản trị bao gồm:

- Quản lý an toàn mạng

- Quản lý an toàn máy chủ và ứng dụng.

### 5.2.2 Tổ chức bảo đảm an toàn thông tin

#### 5.2.2.1 Liên lạc với những cơ quan/tổ chức có thẩm quyền (G1)

Yêu cầu bao gồm:

a) Xác định và lưu thông tin các cơ quan có chức năng quản lý và thực thi công tác bảo đảm an toàn thông tin;

b) Xác định và lưu thông tin các cơ quan trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin

#### 5.2.2.2 Liên lạc với các nhóm chuyên gia (G1)

Yêu cầu bao gồm:

a) Xác định và lưu thông tin các chuyên gia/nhóm chuyên gia trong lĩnh vực an toàn thông tin;

b) Xác định và lưu thông tin cơ quan, tổ chức cung cấp dịch vụ an toàn thông tin.

### 5.2.3. Quản lý xây dựng hệ thống thông tin (G1)

#### 5.2.3.1.Xác định cấp độ an toàn hệ thống thông tin

Yêu cầu bao gồm:

a) Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin;

b) Có tài liệu mô tả các thành phần của hệ thống thông tin bao gồm: các vùng mạng chức năng; hệ thống thiết bị mạng, thiết bị bảo mật; hệ thống máy chủ hệ thống; hệ thống máy chủ ứng dụng; dịch vụ và các thành phần khác trong hệ thống thông tin;

c) Có tài liệu mô tả, giải thích tính phù hợp của cấp độ đề xuất.

#### 5.2.3.2 Thiết kế an toàn hệ thống thông tin

Yêu cầu bao gồm:

a) Có tài liệu mô tả thiết kế hệ thống thông tin;

b) Có tài liệu thiết kế phương án bảo đảm an toàn thông tin theo yêu cầu thiết kế hệ thống.

#### 5.2.4 Quản lý vận hành hệ thống

##### 5.2.4.1 Quản lý an toàn mạng

Yêu cầu bao gồm:

a) Xây dựng chính sách quản lý an toàn mạng để quản lý kiểm soát truy nhập đi vào và từ hệ thống đi ra

b) Xây dựng quy trình quản lý, vận hành hoạt động bình thường của hệ thống.

##### 5.2.4.2 Quản lý an toàn máy chủ và ứng dụng

Yêu cầu bao gồm:

a) Xây dựng chính sách quản lý an toàn máy chủ và ứng dụng, bao gồm các yêu cầu cơ bản sau:

- Chính sách truy nhập và quản trị máy chủ và ứng dụng;

- Chính sách truy nhập mạng;

b) Xây dựng quy trình quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ.

## 6 Yêu cầu cơ bản cho cấp độ 2

### 6.1 Yêu cầu kỹ thuật

#### 6.1.1 Bảo đảm an toàn hạ tầng mạng

##### 6.1.1.1 Thiết kế hệ thống (G2)

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, bao gồm cơ bản cơ bản các vùng mạng:

- Vùng mạng nội bộ (LAN)

- Vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác (Outside)

- Vùng mạng máy chủ công cộng (DMZ)

- Vùng mạng máy chủ nội bộ (Server Farm)

- Vùng mạng máy chủ quản trị (Management)

b) Phương án thiết kế bảo đảm các yêu cầu sau:

- Thiết kế phân vùng mạng riêng cho mạng không dây (nếu có) tách biệt với các vùng mạng chức năng

- Cung cấp khả năng truy nhập, quản trị hệ thống từ xa an toàn

- Có biện pháp quản lý truy nhập và phòng chống xâm nhập.

##### 6.1.1.2 Kiểm soát truy nhập từ bên ngoài mạng (G2)

Yêu cầu bao gồm:

a) Thiết lập hệ thống chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương, khi truy nhập quản trị hệ thống, quản lý và sử dụng tài nguyên nội bộ trong hệ thống từ các mạng bên ngoài;

b) Kiểm soát truy nhập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép từ bên ngoài;

c) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng.

#### 6.1.1.3 Kiểm soát truy nhập từ bên trong mạng (S2)

Cho phép truy nhập ra bên ngoài các địa chỉ Internet, ứng dụng, dịch vụ theo yêu cầu nghiệp vụ; chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức.

#### 6.1.1.4 Nhật ký hệ thống (G2)

Yêu cầu bao gồm:

a) Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị;

b) Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống.

#### 6.1.1.7 Bảo vệ thiết bị hệ thống (G2)

Yêu cầu bao gồm:

a) Cấu hình chức năng xác thực trên các thiết bị hệ thống để xác thực người dùng sử dụng quản trị thiết bị trực tiếp hoặc từ xa;

b) Thiết lập hệ thống chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản trị thiết bị;

c) Cho phép hạn chế các địa chỉ IP, địa chỉ mạng có thể kết kết nối, quản trị thiết bị từ xa.

### 6.1.2 Bảo đảm an toàn máy chủ

#### 6.1.2.1 Xác thực (S2)

a) Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng sử dụng khi khi truy nhập, quản lý và sử dụng máy chủ;

b) Thiết lập chính sách an toàn mật khẩu cho máy chủ bao gồm các yêu cầu cơ bản sau:

- Yêu cầu thay đổi mật khẩu mặc định,

- Thiết lập thời gian yêu cầu thay đổi mật khẩu,

- Thiết lập thời gian mật khẩu hợp lệ,

- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự;

c) Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng).

#### 6.1.2.2 Kiểm soát truy nhập (S2)

Yêu cầu bao gồm:

a) Thiết lập hệ thống chỉ chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản trị máy chủ từ xa thông qua môi trường mạng;

b) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi máy chủ không nhận được yêu cầu từ người dùng.

#### 6.1.2.3 Nhật ký hệ thống (G2)

Yêu cầu bao gồm:

a) Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau:

- Thông tin kết nối mạng tới máy chủ (Firewall log)

- Thông tin đăng nhập vào máy chủ

- Lỗi phát sinh trong quá trình hoạt động

- Các thông tin khác cần ghi nhật ký theo yêu cầu thực tế (nếu có)

b) Đồng bộ thời gian giữa máy chủ với máy chủ thời gian;

c) Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 01 tháng.

#### 6.1.2.4 Phòng chống xâm nhập (G2)

Yêu cầu bao gồm:

a) Loại bỏ các tài khoản không sử dụng và các tài khoản không còn hợp lệ trên máy chủ;

b) Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng;

c) Có thiết lập cơ chế cập nhật, xử lý bản vá điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ.

#### 6.1.2.5 Phòng chống phần mềm độc hại (G2)

a) Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm;

b) Có phương án kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt lên máy chủ.

#### 6.1.2.5 Xử lý máy chủ khi chuyển giao (G2)

Có cơ chế xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng.

### 6.1.3 Bảo đảm an toàn ứng dụng

#### 6.1.3.1 Xác thực (S2)

Yêu cầu bao gồm:

a) Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi quản trị, cấu hình cấu hình ứng dụng và sử dụng ứng dụng (nếu ứng dụng cần quản lý truy nhập);

b) Thiết lập chính sách an toàn mật khẩu cho máy chủ bao gồm các yêu cầu cơ bản sau:

- Yêu cầu thay đổi mật khẩu mặc định,

- Thiết lập thời gian yêu cầu thay đổi mật khẩu,

- Thiết lập thời gian mật khẩu hợp lệ,

- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự;

c) Lưu trữ mã hóa thông tin xác thực trên hệ thống;

d) Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định.

#### 6.1.3.2 Kiểm soát truy nhập (S2)

Yêu cầu bao gồm:

a) Thiết lập hệ thống chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản trị ứng dụng từ xa thông qua môi trường mạng;

b) Thiết lập hệ thống cấm truy nhập trực vào trang quản trị, cổng quản trị ứng dụng từ các mạng bên ngoài mà cần thực hiện gián tiếp bằng cách sử dụng mạng riêng ảo hoặc các phương thức khác tương đương;

c) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng.

#### 6.1.3.3 Nhật ký hệ thống (G2)

Yêu cầu bao gồm:

a) Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau:

- Thông tin thông tin thời gian, địa chỉ, tài khoản (nếu có), nội dung truy nhập và sử dụng ứng dụng ứng dụng

- Thông tin các lỗi phát sinh trong quá trình hoạt động,

- Thông tin đăng nhập khi quản trị ứng dụng

b) Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 01 tháng.

#### 6.1.4 An toàn dữ liệu

##### 6.1.4.1 Bảo mật dữ liệu

Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ.

##### 6.1.4.2 Sao lưu dự phòng (A2)

a) Lưu trữ dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, sơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ;

b) Phân loại và quản lý các dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau.

### 6.2 Yêu cầu quản lý

#### 6.2.1 Chính sách an toàn thông tin

##### 6.2.1.1. Chính sách an toàn thông tin

Bao gồm các yêu cầu sau:

a) Xây dựng chính sách an toàn thông tin cơ bản cho người sử dụng bao gồm:

- Truy nhập, sử dụng tài nguyên trên nội bộ

- Chính sách truy nhập mạng và tài nguyên trên Internet

- Cài đặt và sử dụng máy tính an toàn

b) Xây dựng chính sách an toàn thông tin cho người quản trị bao gồm:

- Quản lý an toàn mạng

- Quản lý an toàn máy chủ và ứng dụng

- Quản lý an toàn dữ liệu

**- Quản lý an toàn dữ liệu.**

#### 6.2.2 Tổ chức bảo đảm an toàn thông tin

##### 6.2.2.1 Liên lạc với những cơ quan/tổ chức có thẩm quyền Yêu cầu bao gồm:

Yêu cầu bao gồm:

a) Xác định và lưu thông tin các cơ quan có chức năng quản lý và thực thi công tác bảo đảm an toàn thông tin;

b) Xác định và lưu thông tin các cơ quan trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin;

c) Cử đầu mối liên hệ/đại diện tổ chức với cơ quan/tổ chức có thẩm quyền.

#### 6.2.2.2 Liên lạc với các nhóm chuyên gia

Yêu cầu bao gồm:

a) Xác định và lưu thông tin các chuyên gia/nhóm chuyên gia trong lĩnh vực an toàn thông tin;

b) Xác định và lưu thông tin cơ quan, tổ chức cung cấp dịch vụ an toàn thông tin.

c) Cử đầu mối liên hệ/đại diện tổ chức với các nhóm chuyên gia.

### 6.2.3. Bảo đảm nguồn nhân lực

#### 6.2.3.1 Chấm dứt hoặc thay đổi công việc

a) Có quy định về quản lý các quy trình, thủ tục cán bộ thôi việc, quy trình nghỉ việc của cán bộ cần tuân thủ theo quy trình, thủ tục đã quy định;

b) Có quy trình vô hiệu hóa tất cả các quyền truy cập thông tin riêng của tổ chức, quyền truy cập, quản trị hệ thống sau khi có cán bộ thôi việc;

c) Có quy trình thu hồi tất cả các văn bản, giấy tờ, các thẻ tín dụng, các thẻ truy cập, thông tin được lưu trên các phương tiện điện tử; các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác của tổ chức do cán bộ quản lý và sử dụng.

### 6.2.4. Quản lý xây dựng hệ thống thông tin

#### 6.2.4.1. Xác định cấp độ an toàn hệ thống thông tin

Yêu cầu bao gồm:

a) Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin;

b) Có tài liệu mô tả các thành phần của hệ thống thông tin bao gồm: các vùng mạng chức năng; hệ thống thiết bị mạng, thiết bị bảo mật; hệ thống máy chủ hệ thống; hệ thống máy chủ ứng dụng; dịch vụ và các thành phần khác trong hệ thống thông tin;

c) Có tài liệu mô tả, giải thích tính phù hợp của cấp độ đề xuất.

#### 6.2.4.2 Thiết kế an toàn hệ thống thông tin

Yêu cầu bao gồm:

a) Có tài liệu mô tả thiết kế hệ thống thông tin;

b) Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ;

c) Có tài liệu thiết kế phương án bảo đảm an toàn thông tin theo yêu cầu thiết kế hệ thống.

### 6.2.5 Quản lý vận hành hệ thống

#### 6.2.5.1 Quản lý an toàn mạng

Yêu cầu bao gồm:

a) Xây dựng chính sách quản lý an toàn mạng, bao gồm các yêu cầu cơ bản sau:

- Chính sách quản lý kiểm soát truy nhập đi vào và từ hệ thống đi ra

- Chính sách truy nhập và quản lý cấu hình hệ thống

b) Xây dựng quy trình quản lý, vận hành hoạt động bình thường của hệ thống;

c) Xây dựng quy trình cập nhật; sao lưu, dự phòng các tệp tin cấu hình hệ thống và quy trình khôi phục hệ thống sau khi xảy ra sự cố.

#### 6.2.5.2 Quản lý an toàn máy chủ và ứng dụng

Yêu cầu bao gồm:

a) Xây dựng chính sách quản lý an toàn máy chủ và ứng dụng, bao gồm các yêu cầu cơ bản sau:

- Chính sách về quản lý và sử dụng máy chủ và ứng dụng an toàn,

- Chính sách truy nhập và quản trị máy chủ và ứng dụng,

- Chính sách truy nhập mạng,

- Chính sách sao lưu và dự phòng và khôi phục cấu hình hệ thống,

b) Xây dựng quy trình quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ.

c) Xây dựng quy trình cập nhật; sao lưu, dự phòng các tệp tin cấu hình hệ thống, tệp tin dự phòng hệ điều hành và các dữ liệu quan trọng khác và quy trình khôi phục sau khi xảy ra sự cố.

#### 6.2.5.3 Quản lý an toàn dữ liệu

Yêu cầu bao gồm:

a) Xây dựng chính sách sao lưu, dự phòng và phôi phục dữ liệu bao gồm: tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ.

b) Xây dựng danh sách thông tin, tệp tin và dữ liệu, phần mềm và các tài nguyên khác trên hệ thống cần dự phòng;

c) Xây dựng quy trình sao lưu dự phòng, định kỳ 01 tháng thực hiện quy trình sao lưu dự phòng.

# 7 Yêu cầu cơ bản cho cấp độ 3

## 7.1 Yêu cầu kỹ thuật

### 7.1.1 Bảo đảm an toàn hạ tầng mạng

#### 7.1.1.1 Thiết kế hệ thống (G3)

Yêu cầu bao gồm:

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, bao gồm cơ bản cơ bản các vùng mạng:

- Vùng mạng nội bộ (LAN)

- Vùng mạng biên (Outside)

- Vùng mạng máy chủ công cộng (DMZ)

- Vùng mạng máy chủ nội bộ (Server Farm)

- Vùng mạng cho máy chủ cơ sở dữ liệu (Database)

- Vùng mạng máy chủ quản trị (Management)

- Vùng mạng khác (nếu có) theo yêu cầu, mục đích của tổ chức

b) Phương án thiết kế bảo đảm các yêu cầu sau:

- Không triển khai các máy chủ cơ sở dữ liệu hoặc đặt cơ sở dữ liệu, máy chủ nội bộ trong vùng mạng máy chủ công cộng

- Thiết kế vùng mạng nội bộ thành các mạng chức năng theo yêu cầu nghiệp vụ (VLAN)

- Thiết kế phân vùng mạng riêng cho mạng không dây (nếu có) tách biệt với các vùng mạng chức năng

- Thiết lập một vùng mạng riêng (vùng mạng quản trị thiết bị) bao gồm các địa chỉ quản trị của các thiết bị hệ thống; kiểm soát, giám sát các truy nhập từ vùng mạng khác vào vùng mạng này

- Có biện pháp quản lý truy nhập và phòng chống xâm nhập

- Có phương án chặn lọc phần mềm độc hại trên môi trường mạng

- Các thiết bị mạng chính có thiết kế dự phòng bảo đảm tính khả dụng của hệ thống của hệ thống; năng lực của thiết bị đáp ứng theo quy mô hệ thống mạng, số lượng dịch vụ cung cấp và người dùng có trong hệ thống

- Có phương án truy nhập, quản trị hệ thống từ xa an toàn

- Có phương án phòng chống tấn công từ chối dịch vụ

- Có phương án giám sát tập trung hoạt động bình thường của hệ thống

- Có phương án giám sát tập trung sự kiện an toàn thông tin trên hệ thống

- Có phương án quản lý lưu trữ tập trung

- Có phương án quản lý đăng nhập tập trung

- Có phương án quản lý cập nhật bản vá, điểm yếu an toàn thông tin tập trung

- Có phương án quản lý tập trung các phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng trong hệ thống.

**7.1.1.2 Kiểm soát truy nhập từ bên ngoài mạng (G3)**

Yêu cầu bao gồm:

a) Thiết lập hệ thống chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản lý và sử dụng tài nguyên nội bộ trong hệ thống từ các mạng bên ngoài;

b) Kiểm soát truy nhập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép từ bên ngoài;

c) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng.

d) Phân quyền và cấp quyền truy nhập từ bên ngoài vào hệ thống theo theo từng người dùng hoặc nhóm người dùng căn cứ theo yêu cầu nghiệp vụ, yêu cầu quản lý;

đ) Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ hệ thống cung cấp theo quy mô và khả năng cung cấp của hệ thống.

**7.1.1.3 Kiểm soát truy nhập từ bên trong mạng (S3)**

Yêu cầu bao gồm:

a) Giới hạn các dịch vụ được cho phép truy nhập ra bên ngoài theo yêu cầu nghiệp vụ và các vùng mạng chức năng trong hệ thống, cấm toàn bộ các truy nhập không cần thiết khác tùy thuộc vào chính sách của tổ chức;

b) Có phương án quản lý các thiết bị đầu cuối, máy tính người dùng kết nối vào hệ thống mạng (theo địa chỉ vật lý, địa chỉ logic), chỉ cho phép thiết bị đầu cuối, máy tính người sử dụng hợp lệ kết nối vào hệ thống.

**7.1.1.4 Nhật ký hệ thống (G3)**

Yêu cầu bao gồm:

a) Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị;

b) Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống;

c) Thông tin về truy cập ứng dụng dịch vụ cần ghi nhật ký bao gồm:

- Thời gian kết nối,

- Thông tin kết nối mạng (địa chỉ IP, cổng kết nối),

- Hành động đối với kết nối (cho phép, ngăn chặn),

- Thông tin các thiết bị đầu cuối kết nối vào hệ thống theo địa chỉ vật lý và logic,

- Thông tin cảnh báo từ các thiết bị;

d) Giới hạn tài nguyên cho chức năng ghi nhật ký trên thiết bị, để bảo đảm chức năng này không làm ảnh hưởng, gián đoạn hoạt động của thiết bị;

đ) Lưu trữ và quản lý tập trung nhật ký hệ thống trên hệ thống quản lý nhật ký hệ thống tập trung;

e) Lưu trữ nhật ký hệ thống của thiết bị tối thiểu 03 tháng.

**7.1.1.5 Phòng chống xâm nhập (G3)**

Yêu cầu bao gồm:

a) Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng máy chủ công cộng, máy chủ nội bộ, máy chủ cơ sở dữ liệu và vùng mạng nội bộ;

b) Tự động cập nhật thời gian thực cơ sở dữ liệu, dấu hiệu phát hiện tấn công;

c) Bảo đảm năng lực hệ thống bảo đảm đáp ứng đủ theo yêu cầu theo quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp;

đ) Có phương án tự động xử lý bảo đảm hoạt động bình thường của hệ thống khi hệ thống xảy ra sự cố.

**7.1.1.6 Phòng chống phần mềm độc hại trên môi trường mạng (G3)**

Yêu cầu bao gồm:

a) Có phương án phòng chống phần mềm độc hại trên môi trường mạng để bảo vệ vùng mạng nội bộ;

b) Tự động cập nhật thời gian thực cơ sở dữ liệu cho hệ thống phòng chống phần mềm độc hại.

c) Bảo đảm năng lực hệ thống bảo đảm đáp ứng đủ theo yêu cầu theo quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp.

**7.1.1.7 Bảo vệ thiết bị mạng (G3)**

Yêu cầu bao gồm:

a) Cấu hình chức năng xác thực trên các thiết bị hệ thống để xác thực người dùng sử dụng quản trị thiết bị trực tiếp hoặc từ xa;

b) Thiết lập hệ thống chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản trị thiết bị;

c) Cho phép hạn chế các địa chỉ IP, địa chỉ mạng có thể kết kết nối, quản trị thiết bị từ xa;

d) Hạn chế được số lần đăng nhập sai khi quản trị hoặc kết nối quản trị từ xa theo địa chỉ IP nguồn;

đ) Phân quyền truy nhập, quản trị thiết bị đối với các tài khoản quản trị có quyền hạn khác nhau.

### 7.1.2 Bảo đảm an toàn máy chủ

#### 7.1.2.1 Xác thực (S3)

a) Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng sử dụng khi khi truy nhập, quản lý và sử dụng máy chủ;

b) Thiết lập chính sách an toàn mật khẩu cho máy chủ bao gồm các yêu cầu cơ bản sau:

- Yêu cầu thay đổi mật khẩu mặc định,

- Thiết lập thời gian yêu cầu thay đổi mật khẩu,

- Thiết lập thời gian mật khẩu hợp lệ,

- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự;

c) Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng);

d) Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với một tài khoản nhất định;

đ) Thiết lập cấu hình để vô hiệu hóa tài khoản nếu tài khoản đó đăng nhập sai nhiều lần vượt số lần quy định;

e) Thông tin xác thực yêu cầu cần thay đổi định kỳ 03 tháng/lần);

g) Quản lý thông tin xác thực trên hệ thống quản lý tập trung.

#### 7.1.2.2 Kiểm soát truy nhập (S3)

Yêu cầu bao gồm:

a) Thiết lập hệ thống chỉ chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản trị máy chủ từ xa thông qua môi trường mạng;

b) Thay đổi cổng quản trị mặc định của máy chủ;

c) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi máy chủ không nhận được yêu cầu từ người dùng;

d) Giới hạn địa chỉ IP nguồn được phép truy nhập, quản trị máy chủ từ xa;

đ) Thiết lập hệ thống không truy nhập trực tiếp cổng quản trị, phần mềm quản trị máy chủ từ các mạng bên ngoài; thực hiện gián tiếp thông qua kết nối mạng riêng ảo hoặc các phương thức khác tương đương.

#### 7.1.2.3 Nhật ký hệ thống (G3)

Yêu cầu bao gồm:

a) Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau:

- Thông tin kết nối mạng tới máy chủ (Firewall log),

- Thông tin trạng thái hoạt động của máy chủ (CPU, RAM, Network…),

- Thông tin các lỗi phát sinh trong quá trình hoạt động,

- Thông tin đăng nhập và truy nhập tài nguyên trên máy chủ,

- Thông tin quản trị, thay đổi cấu hình trên máy chủ (thời gian, địa chỉ, tài khoản truy nhập và thao tác trên máy chủ và các thông tin quản trị khác cần ghi nhật ký (nếu có),

- Các thông tin khác cần ghi nhật ký theo yêu cầu thực tế (nếu có);

b) Đồng bộ thời gian giữa máy chủ với máy chủ thời gian của hệ thống;

c) Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống để không mất hoặc tràn nhật ký hệ thống;

d) Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý nhật ký hệ thống tập trung, gửi dữ liệu nhật ký hệ thống về hệ thống trung tâm theo thời gian thực;

đ) Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 03 tháng.

#### 7.1.2.4 Phòng chống xâm nhập (G3)

Yêu cầu bao gồm:

a) Loại bỏ các tài khoản không sử dụng và các tài khoản không còn hợp lệ trên máy chủ;

b) Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng;

c) Sử dụng tường lửa của hệ điều hành máy chủ để cấm các truy nhập trái phép tới máy chủ;

d) Có cơ chế cập nhật và xử lý bản vá, điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ từ hệ thống quản lý tập trung.

#### 7.1.2.5 Phòng chống phần mềm độc hại (G3)

Yêu cầu bao gồm:

a) Cài đặt phần mềm xử lý phần mềm độc hại (anti-virus) và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm;

b) Có phương án kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt lên máy chủ;

c) Quản lý tập trung (cập nhật, cảnh báo và quản lý) các phần mềm phòng chống mã độc trên máy chủ và các máy tính người sử dụng trong hệ thống.

#### 7.1.2.6 Xử lý máy chủ khi chuyển giao (S3)

Khi chuyển giao hoặc thay đổi mục đích sử dụng phải thực hiện:

a) Sao lưu, dự phòng thông tin, dữ liệu trên máy chủ, ảnh của hệ điều hành máy chủ;

b) Xóa toàn bộ dữ liệu lưu trữ trên máy chủ và xóa hệ điều hành máy chủ.

### 7.1.3 Bảo đảm an toàn ứng dụng

#### 7.1.3.1 Xác thực (S3)

Yêu cầu bao gồm:

a) Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi quản trị, cấu hình cấu hình ứng dụng và sử dụng ứng dụng (nếu ứng dụng cần quản lý truy nhập);

b) Thiết lập chính sách an toàn mật khẩu cho máy chủ bao gồm các yêu cầu cơ bản sau:

- Yêu cầu thay đổi mật khẩu mặc định,

- Thiết lập thời gian yêu cầu thay đổi mật khẩu,

- Thiết lập thời gian mật khẩu hợp lệ,

- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự;

c) Vô hiệu hóa hoặc thay đổi các thông tin các tài khoản mặc định (nếu có);

d) Lưu trữ mã hóa thông tin xác thực trên hệ thống;

đ) Mã hóa thông tin xác thực trước khi gửi qua môi trường mạng;

e) Thiết lập cấu hình ứng dụng để ngăn cản việc đăng nhập tự động;

g) Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định;

h) Quản lý thông tin xác thực trên hệ thống quản lý tập trung.

#### 7.1.3.2 Kiểm soát truy nhập (S3)

Yêu cầu bao gồm:

a) Thiết lập hệ thống chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản trị ứng dụng từ xa thông qua môi trường mạng;

b) Thiết lập hệ thống cấm truy nhập trực vào trang quản trị, cổng quản trị ứng dụng từ các mạng bên ngoài mà cần thực hiện gián tiếp bằng cách sử dụng mạng riêng ảo hoặc các phương thức khác tương đương;

c) Giới hạn địa chỉ IP quản trị được phép truy nhập, quản trị ứng dụng từ xa;

d) Thay đổi, tách biệt cổng kết nối quản trị ứng dụng với cổng cung cấp dịch vụ ứng dụng;

đ) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng;

e) Phân quyền truy nhập, quản trị, sử dụng tài nguyên khác nhau của ứng dụng với người sử dụng/ nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau.

#### 7.1.3.3 Nhật ký hệ thống (G3)

Yêu cầu bao gồm:

a) Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau:

- Thông tin thông tin thời gian, địa chỉ, tài khoản (nếu có), nội dung truy nhập và sử dụng ứng dụng ứng dụng,

- Thông tin các lỗi phát sinh trong quá trình hoạt động,

- Thông tin quản trị, thay đổi cấu hình ứng dụng,

b) Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý nhật ký hệ thống tập trung, gửi dữ liệu nhật ký hệ thống về hệ thống trung tâm theo thời gian thực;

c) Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 03 tháng.

#### 7.1.3.4 Bảo mật thông tin liên lạc (S3)

Yêu cầu bao gồm:

a) 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) Sử dụng giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương.

#### 7.1.3.5 Chống chối bỏ (G3)

Yêu cầu bao gồm:

a) Cung cấp chức năng chức thực, xác minh thông tin, nguồn gửi thông tin khi trao đổi thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) qua môi trường mạng;

b) Áp dụng cơ chế xác thực hai chiều khi trao đổi dữ liệu quan trọng qua môi trường mạng.

### 7.1.4 An toàn dữ liệu

#### 7.1.4.1 Nguyên vẹn dữ liệu (S3)

Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống bảo đảm tính nguyên vẹn.

#### 7.1.4.2 Bảo mật dữ liệu (S3)

Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ.

#### 7.1.4.3 Sao lưu dự phòng (A3)

a) Thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, sơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ;

b) Phân loại và quản lý các dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau;

c) Có hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng.

## 7.2 Yêu cầu quản lý

### 7.2.1 Chính sách an toàn thông tin

#### 7.2.1.1. Chính sách an toàn thông tin

Bao gồm các yêu cầu sau:

a) Xác định các mục tiêu, nguyên tắc bảo đảm an toàn thông tin;

b) Xác định trách nhiệm của đơn vị quản lý an toàn thông tin, các thành viên trong ban quản lý an toàn thông tin và các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin;

c) Xác định Chính sách an toàn thông tin bao gồm các nội dung cơ bản sau:

- Phạm vi quản lý về vật lý và logic của tổ chức;

- Các loại tài sản (tài liệu, dữ liệu, thiết bị, con người…);

- Các ứng dụng, dịch vụ hệ thống cung cấp;

- Nguồn nhân lực bảo đảm an toàn thông tin (Cấp Lãnh đạo, cán bộ quản lý, cán bộ kỹ thuật, nhân viên…);

d) Xây dựng chính sách an toàn thông tin cơ bản cho người sử dụng bao gồm:

- Truy nhập, sử dụng tài nguyên trên nội bộ

- Truy nhập mạng và tài nguyên trên Internet

- Cài đặt và sử dụng máy tính an toàn

- An toàn dữ liệu

đ) Xây dựng chính sách an toàn thông tin cho người quản trị bao gồm:

- Quản lý an toàn mạng

- Quản lý an toàn máy chủ và ứng dụng

- Quản lý an toàn dữ liệu

- Quản lý an toàn thiết bị đầu cuối

- Quản lý phòng chống phần mềm độc hại

- Quản lý điểm yếu an toàn thông tin

**7.2.1.2. Rà soát, sửa đổi**

Yêu cầu bao gồm:

Định kỳ 02 năm hoặc đột xuất (khi có thay đổi chính sách) kiểm tra lại chính sách quản lý an toàn để tìm ra điểm chưa hợp lý, thiếu sót cần phải chỉnh sửa hoặc bổ sung;

**7.2.2 Tổ chức bảo đảm an toàn thông tin**

**7.2.2.1 Đơn vị quản lý an toàn thông tin (G3)**

Yêu cầu bao gồm:

a) Thành lập đơn vị chuyên trách hoặc chỉ định đơn vị (hoặc bộ phần) có trách nhiệm quản lý về an toàn thông tin trong tổ chức (Đơn vị quản lý an toàn thông tin);

b) Chỉ định bộ phận có trách nhiệm quản lý, thực thi chính sách an toàn thông tin đã xây dựng.

**7.2.2.2 Liên lạc với những cơ quan/tổ chức có thẩm quyền**

Yêu cầu bao gồm:

a) Xác định và lưu thông tin các cơ quan có chức năng quản lý và thực thi công tác bảo đảm an toàn thông tin;

b) Xác định và lưu thông tin các cơ quan trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin;

c) Cử đầu mối liên hệ/đại diện tổ chức với cơ quan/tổ chức có thẩm quyền.

**7.2.2.3 Liên lạc với các nhóm chuyên gia**

Yêu cầu bao gồm:

a) Xác định và lưu thông tin các chuyên gia/nhóm chuyên gia trong lĩnh vực an toàn thông tin;

b) Xây dựng thỏa thuận phối hợp, quy chế làm việc giữa tổ chức với các chuyên gia/nhóm chuyên gia; cơ quan, tổ chức cung cấp dịch vụ an toàn thông tin;

c) Cử đầu mối liên hệ/đại diện tổ chức với các nhóm chuyên gia.

**7.2.3 Bảo đảm nguồn nhân lực**

**7.2.3.1.Trước khi tuyển dụng**

a) Có quy định về quy trình tuyển dụng cán bộ; thẩm tra về lý lịch, thân phận của cán bộ được tuyển dụng; có chuyên gia trong lĩnh vực đánh giá, kiểm tra trình độ chuyên môn phù hợp với vị trí tuyển dụng;

b) Các điều khoản và điều kiện tuyển dụng: đưa ra các điều khoản, điều kiện trong hợp đồng với nhân viên và nhà thầu; trách nhiệm của của các bên liên quan trong hợp đồng;

c) Cán bộ được tuyển dụng yêu cầu có trình độ chuyên môn phù hợp với vị trí tuyển dụng, hiểu biết và có kinh nghiệm tối thiểu 01 năm trong lĩnh vực an toàn thông tin.

**7.2.3.2 Trong quá trình làm việc**

Yêu cầu này bao gồm:

a) Tổ chức đào tạo nâng cao nhận thức về an toàn thông tin và kỹ năng an toàn cơ bản về an toàn thông tin trong quá trình làm việc trước khi làm việc chính thức trong tổ chức;

b) Có kế hoạch và tổ chức đào tạo về an toàn thông tin hàng năm cho 03 nhóm đối tượng bao gồm: cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống.

**7.2.3.3 Chấm dứt hoặc thay đổi công việc**

a) Có quy định về quản lý các quy trình, thủ tục cán bộ thôi việc, quy trình nghỉ việc của cán bộ cần tuân thủ theo quy trình, thủ tục đã quy định;

b) Có quy trình vô hiệu hóa tất cả các quyền truy cập thông tin riêng của tổ chức, quyền truy cập, quản trị hệ thống sau khi có cán bộ thôi việc;

c) Có quy trình thu hồi tất cả các văn bản, giấy tờ, các thẻ tín dụng, các thẻ truy cập, thông tin được lưu trên các phương tiện điện tử; các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác của tổ chức do cán bộ quản lý và sử dụng;

d) Có cam kết giữ bí mật thông tin liên quan đến tổ chức đối với cán bộ ở vị trí chủ chốt sau khi nghỉ việc.

**7.2.4 Quản lý xây dựng hệ thống thông tin**

**7.2.4.1 Xác định cấp độ an toàn hệ thống thông tin (G3)**

Yêu cầu bao gồm:

a) Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin;

b) Có tài liệu mô tả các thành phần của hệ thống thông tin bao gồm: các vùng mạng chức năng; hệ thống thiết bị mạng, thiết bị bảo mật; hệ thống máy chủ hệ thống; hệ thống máy chủ ứng dụng; dịch vụ và các thành phần khác trong hệ thống thông tin;

c) Có tài liệu mô tả loại thông tin các thành phần trong hệ thống thông tin xử lý bao gồm: thông tin công cộng, thông tin riêng, thông tin cá nhân, thông tin bí mật nhà nước và các loại thông tin khác (nếu có);

d) Có tài liệu mô tả loại hệ thống thông tin căn cứ theo chức năng phục vụ hoạt động nghiệp vụ bao gồm: hệ thống thông tin phục vụ hoạt động nội bộ, hệ thống thông tin phục vụ người dân, doanh

nghiệp, hệ thống cơ sở hạ tầng thông tin, hệ thống thông tin điều khiển công nghiệp, hệ thống thông tin khác (nếu có);

đ) Có tài liệu mô tả, giải thích tính phù hợp của cấp độ đề xuất;

e) Có ý kiến thẩm định của đơn vị chuyên môn trước khi phê duyệt cấp độ.

**7.2.4.2 Thiết kế an toàn hệ thống thông tin (G3)**

Yêu cầu bao gồm:

a) Có tài liệu mô tả thiết kế mô tả những thông tin sau:

- Thiết kế vật lý hệ thống thông tin (thiết bị, kết nối vật lý)

- Thiết kế logic hệ thống thông tin (các phân vùng mạng, chức năng);

- Ứng dụng, dịch vụ hệ thống (DNS, DHCP, NTP…)

- Ứng dụng, dịch vụ phục vụ hoạt động nghiệp vụ

b) Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ

c) Có tài liệu thiết kế phương án bảo đảm an toàn thông tin theo yêu cầu thiết kế hệ thống.

**7.2.4.3 Phát triển phần mềm thuê khoán**

Yêu cầu bao gồm:

a) Có tài liệu mô tả các chức năng, yêu cầu an toàn phần mềm cần đáp ứng;

b) Có tài liệu mô tả phương án, thiết kế, mô tả khả năng đáp ứng các yêu cầu đặt ra;

c) Phần mềm cần đáp ứng các tiêu chuẩn, quy chuẩn kỹ thuật theo quy định (nếu có);

d) Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm; thực hiện kiểm tra, đánh giá an toàn thông tin cho phần mềm trước khi sử dụng;

đ) Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

**7.2.4.4 Thử nghiệm và bàn giao hệ thống**

Yêu cầu bao gồm:

a) Có nội dung, kế hoạch thử nghiệm và nghiệm thu hệ thống;

b) Có bộ phận có trách nhiệm thực hiện nghiệm thu và kiểm thử hệ thống;

c) Có đơn vị độc lập (bên thứ 3) tư vấn và giám sát quá trình thực nghiệm và kiểm thử hệ thống;

d) Có báo cáo nghiệm thu được thẩm định và xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

***3.2.4.5 Các mối liên hệ với bên cung cấp dịch vụ an toàn thông tin***

Yêu cầu bao gồm:

a) Có quy định về các yêu cầu, các thỏa thuận, quyền hạn và trách nhiệm của bên cung cấp;

b) Có quy trình ký kết, thực hiện, duy trì và thay đổi các cam kết trong hợp đồng đối với các bên cung cấp;

c) Có thỏa thuận và cam kết trách nhiệm của mỗi bên trước khi được ký kết hợp đồng;

d) Bên cung cấp dịch vụ an toàn thông tin được cơ quan có thẩm quyền cấp phép.

**7.2.4.5 Các mối liên hệ với bên cung cấp dịch vụ an toàn thông tin**

Yêu cầu bao gồm:

a) Có quy định về các yêu cầu, các thỏa thuận, quyền hạn và trách nhiệm của bên cung cấp;

b) Có quy trình ký kết, thực hiện, duy trì và thay đổi các cam kết trong hợp đồng đối với các bên cung cấp;

c) Có thỏa thuận và cam kết trách nhiệm của mỗi bên trước khi được ký kết hợp đồng;

d) Bên cung cấp dịch vụ an toàn thông tin được cơ quan có thẩm quyền cấp phép;

**7.2.5 Quản lý vận hành hệ thống**

**7.2.5.1 Quản lý an toàn mạng**

Yêu cầu bao gồm:

a) Xây dựng chính sách quản lý an toàn mạng, bao gồm các yêu cầu cơ bản sau:

- Chính sách quản lý kiểm soát truy nhập đi vào và từ hệ thống đi ra

- Chính sách truy nhập và quản lý cấu hình hệ thống

- Chính sách bảo đảm an toàn dữ liệu qua môi trường mạng

- Chính sách sao lưu và dự phòng và khôi phục cấu hình hệ thống

b) Xây dựng quy trình quản lý, vận hành hoạt động bình thường của hệ thống;

c) Xây dựng quy trình cập nhật; sao lưu, dự phòng các tệp tin cấu hình hệ thống và quy trình khôi phục hệ thống sau khi xảy ra sự cố;

d) Xây dựng quy trình cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

**7.2.5.2 Quản lý an toàn máy chủ và ứng dụng**

Yêu cầu bao gồm:

a) Xây dựng chính sách quản lý an toàn máy chủ và ứng dụng, bao gồm các yêu cầu cơ bản sau:

- Chính sách về quản lý và sử dụng máy chủ và ứng dụng an toàn,

- Chính sách truy nhập và quản trị máy chủ và ứng dụng,

- Chính sách truy nhập mạng,

- Chính sách bảo đảm an toàn dữ liệu qua môi trường mạng,

- Chính sách sao lưu và dự phòng và khôi phục cấu hình hệ thống,

b) Xây dựng quy trình quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ;

c) Xây dựng quy trình cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng;

d) Xây dựng quy trình kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống;

đ) Xây dựng quy trình cập nhật; sao lưu, dự phòng các tệp tin cấu hình hệ thống, tệp tin dự phòng hệ điều hành và các dữ liệu quan trọng khác và quy trình khôi phục sau khi xảy ra sự cố;

e) Xây dựng quy trình cấu hình tối tưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ và dịch vụ và thực hiện quy trình trước khi đưa hệ thống vào sử dụng.

**7.2.5.3 Quản lý an toàn dữ liệu**

Yêu cầu bao gồm:

a) Xây dựng chính sách sao lưu, dự phòng và phôi phục dữ liệu bao gồm: tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ.

b) Xây dựng danh sách thông tin, tệp tin và dữ liệu, phần mềm và các tài nguyên khác trên hệ thống cần dự phòng;

c) Xây dựng quy trình sao lưu dự phòng và thực hiện quy trình sao lưu dự phòng khi có thay đổi trên hệ thống;

d) Xây dựng quy trình khôi phục dữ liệu dự phòng.

**7.2.5.4 Quản lý an toàn thiết bị đầu cuối**

Yêu cầu bao gồm:

a) Xây dựng chính sách quản lý an toàn thiết bị đầu cuối, bao gồm các yêu cầu cơ bản sau:

- Chính sách về quản lý và sử dụng các thiết bị đầu cuối an toàn;

- Chính sách kết nối thiết bị đầu cuối vào hệ thống;

- Chính sách kết nối, truy nhập và sử dụng thiết bị đầu cuối từ xa;

- Chính sách bảo đảm an toàn vật lý cho thiết bị đầu cuối;

b) Xây dựng quy trình quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối;

c) Xây dựng quy trình cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối vào hệ thống.

#### 7.2.5.5 Quản lý phòng chống phần mềm độc hại

Yêu cầu bao gồm:

a) Xây dựng quy định cho người sử dụng về việc cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng;

b) Xây dựng quy định về việc gửi nhận tệp tin từ môi trường mạng và qua các phương tiện lưu trữ di động;

d) Xây dựng quy định, quy trình về việc cài đặt, cập nhật và sử dụng phần mềm diệt virus; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động;

đ) Định kỳ 01 tháng (hoặc khi phát hiện hoạt động không bình thường của hệ thống) thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống.

#### 7.2.5.6 Quản lý điểm yếu an toàn thông tin

Yêu cầu bao gồm:

a) Xây dựng danh mục, phiên bản, chức năng cho các thành phần có trong hệ thống (thiết bị mạng, bảo mật; hệ điều hành; máy chủ; ứng dụng, dịch vụ và các thành phần khác trong hệ thống có thể tồn tại điểm yếu an toàn thông tin và các thông tin);

b) Xây dựng danh sách nguồn cung cấp điểm yếu an toàn thông tin; phân nhóm và mức độ của điểm yếu cho các thành phần trong hệ thống đã xác định;

c) Xây dựng danh sách đầu mối các nhóm chuyên ra, bên cung cấp dịch vụ hỗ trợ, cung cấp dịch vụ xử lý, khắc phục điểm yếu an toàn thông tin;

d) Có quy định về việc cập nhật thông tin, cơ chế cảnh báo các điểm yếu an toàn thông tin cho các bộ phận có trách nhiệm tương ứng.

# 8 Yêu cầu cơ bản cho cấp độ 4

## 8.1 Yêu cầu kỹ thuật

### 8.1.1 Bảo đảm an toàn hạ tầng mạng

#### 8.1.1.1 Thiết kế hệ thống (G4)

Yêu cầu bao gồm:

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, bao gồm cơ bản cơ bản các vùng mạng:

- Vùng mạng nội bộ (LAN)

- Vùng mạng biên (Outside)

- Vùng mạng máy chủ công cộng (DMZ)

- Vùng mạng máy chủ nội bộ (Server Farm)

- Vùng mạng cho máy chủ cơ sở dữ liệu (Database)

- Vùng mạng máy chủ quản trị (Management)

- Vùng mạng khác (nếu có) theo yêu cầu, mục đích của tổ chức;

b) Phương án thiết kế bảo đảm các yêu cầu sau:

- Không triển khai các máy chủ cơ sở dữ liệu hoặc đặt cơ sở dữ liệu, máy chủ nội bộ trong vùng mạng máy chủ công cộng

- Thiết kế vùng mạng nội bộ thành các mạng chức năng theo yêu cầu nghiệp vụ (VLAN)

- Thiết kế phân vùng mạng riêng cho mạng không dây (nếu có) tách biệt với các vùng mạng chức năng

- Thiết lập một vùng mạng riêng (vùng mạng quản trị thiết bị) bao gồm các địa chỉ quản trị của các thiết bị hệ thống; có biện pháp quản lý, giám sát các truy nhập từ vùng mạng khác vào vùng mạng này

- Có biện pháp quản lý truy nhập và phòng chống xâm nhập

- Có phương án chặn lọc phần mềm độc hại trên môi trường mạng

- Có phương án bảo vệ máy chủ cơ sở dữ liệu chuyên dụng

- Các thiết bị mạng chính có thiết kế dự phòng nóng (HA hoặc AA) bảo đảm tính khả dụng của hệ thống của hệ thống; năng lực của thiết bị đáp ứng theo quy mô hệ thống mạng, số lượng dịch vụ cung cấp và người dùng có trong hệ thống

- Có phương án truy nhập, quản trị hệ thống từ xa an toàn

- Có phương án phòng chống tấn công từ chối dịch vụ

- Có phương án giám sát tập trung hoạt động bình thường của hệ thống

- Có phương án giám sát tập trung sự kiện an toàn thông tin trên hệ thống

- Có phương án quản lý lưu trữ tập trung

- Có phương án quản lý tập trung các phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng trong hệ thống

- Có phương án quản lý cập nhật bản vá, điểm yếu an toàn thông tin tập trung

- Có phương án quản lý mạng không dây tập trung

- Có phương án quản lý đăng nhập tập trung

- Có phương án quản lý tài khoản đặc quyền

#### 8.1.1.2 Kiểm soát truy nhập từ bên ngoài mạng (G4)

Yêu cầu bao gồm:

a) Thiết lập hệ thống chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản lý và sử dụng tài nguyên nội bộ trong hệ thống từ các mạng bên ngoài;

b) Kiểm soát truy nhập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép từ bên ngoài;

c) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng.

d) Phân quyền và cấp quyền truy nhập từ bên ngoài vào hệ thống theo theo từng người dùng hoặc nhóm người dùng căn cứ theo yêu cầu nghiệp vụ, yêu cầu quản lý;

đ) Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ hệ thống cung cấp theo quy mô và khả năng cung cấp của hệ thống

e) Kiểm soát truy nhập từ bên ngoài mạng theo thời gian quy định của tổ chức.

#### 8.1.1.3 Kiểm soát truy nhập từ bên trong mạng (S4)

Yêu cầu bao gồm:

a) Cho phép truy nhập ra bên ngoài các địa chỉ Internet, ứng dụng, dịch vụ theo yêu cầu nghiệp vụ; chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức;

b) Có phương án quản lý tập trung các thiết bị đầu cuối kết nối vào hệ thống, bao gồm các chức năng cơ bản sau:

- Quản lý theo địa chỉ vật lý, địa chỉ logic,

- Tài khoản người sử dụng,

- Chính sách cài đặt và thiết lập cấu hình bảo mật trên thiết bị,

- Các chính sách khác của hệ thống (nếu có)

c) Triển khai hệ thống giám sát, phát hiện và ngăn chặn truy cập từ bên trong mạng đến các địa chỉ Internet bị cấm truy cập theo chính sách của tổ chức.

#### 8.1.1.4 Nhật ký hệ thống (G4)

Yêu cầu bao gồm:

a) Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị;

b) Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống;

c) Thông tin về truy cập ứng dụng dịch vụ cần ghi nhật ký bao gồm:

- Thời gian kết nối

- Thông tin kết nối mạng (địa chỉ IP, cổng kết nối)

- Hành động đối với kết nối (cho phép, ngăn chặn)

- Thao tác người sử dụng khi kết nối thành công

- Thông tin các thiết bị đầu cuối kết nối vào hệ thống theo địa chỉ vật lý và logic

- Thông tin và thao tác người quản trị cấu hình, thay đổi hệ thống

- Thông tin cảnh báo từ các thiết bị

d) Giới hạn tài nguyên cho chức năng ghi nhật ký trên thiết bị, để bảo đảm chức năng này không làm ảnh hưởng, gián đoạn hoạt động của thiết bị;

đ) Lưu trữ và quản lý tập trung nhật ký hệ thống trên hệ thống quản lý nhật ký hệ thống tập trung;

e) Lưu trữ dự phòng dữ liệu nhật ký hệ thống trên hệ thống lưu trữ riêng biệt;

g) Lưu trữ nhật ký hệ thống của thiết bị tối thiểu 06 tháng.

**8.1.1.5 Phòng chống xâm nhập (G4)**

Yêu cầu bao gồm:

a) Có phương án phòng chống xâm nhập chuyên dụng để bảo vệ các vùng mạng máy chủ công cộng, máy chủ nội bộ, máy chủ cơ sở dữ liệu và vùng mạng nội bộ;

b) Tự động cập nhật thời gian thực cơ sở dữ liệu, dấu hiệu phát hiện tấn công;

c) Bảo đảm năng lực hệ thống bảo đảm đáp ứng đủ theo yêu cầu theo quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp;

đ) Có phương án tự động xử lý bảo đảm hoạt động bình thường của hệ thống khi hệ thống xảy ra sự cố;

e) Có phương án dự phòng nóng hệ thống.

**8.1.1.6 Phòng chống phần mềm độc hại trên môi trường mạng(G4)**

Yêu cầu bao gồm:

a) Thiết lập hệ thống phòng chống phần mềm độc hại chuyên dụng để bảo vệ các vùng mạng máy chủ và vùng mạng nội bộ;

b) Tự động cập nhật thời gian thực cơ sở dữ liệu cho hệ thống phòng chống phần mềm độc hại.

c) Bảo đảm năng lực hệ thống bảo đảm đáp ứng đủ theo yêu cầu theo quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp;

d) Có phương án tự động xử lý bảo đảm hoạt động bình thường của hệ thống khi hệ thống xảy ra sự cố;

đ) Có phương án dự phòng nóng hệ thống.

#### 8.1.1.7 Bảo vệ thiết bị hệ thống (G4)

Yêu cầu bao gồm:

a) Cấu hình chức năng xác thực trên các thiết bị hệ thống để xác thực người dùng sử dụng quản trị thiết bị trực tiếp hoặc từ xa;

b) Thiết lập hệ thống chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản trị thiết bị;

c) Cho phép hạn chế các địa chỉ IP, địa chỉ mạng có thể kết kết nối, quản trị thiết bị từ xa;

d) Hạn chế được số lần đăng nhập sai khi quản trị hoặc kết nối quản trị từ xa theo địa chỉ IP nguồn;

đ) Phân quyền truy nhập, quản trị thiết bị đối với các tài khoản quản trị có quyền hạn khác nhau;

e) Nâng cấp, xử lý điểm yếu, lỗ hổng bảo mật của thiết bị hệ thống trước khi đưa vào sử dụng;

g) Cấu hình tối ưu, tăng cường bảo mật cho hệ thống thiết bị hệ thống trước khi đưa vào sử dụng.

### 8.1.2 Bảo đảm an toàn máy chủ

#### 8.1.2.1 Xác thực (S4)

a) Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng sử dụng khi khi truy nhập, quản lý và sử dụng máy chủ;

b) Thiết lập chính sách an toàn mật khẩu cho máy chủ bao gồm các yêu cầu cơ bản sau:

- Yêu cầu thay đổi mật khẩu mặc định

- Thiết lập thời gian yêu cầu thay đổi mật khẩu

- Thiết lập thời gian mật khẩu hợp lệ

- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự

c) Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng);

d) Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với một tài khoản nhất định;

đ) Thiết lập cấu hình để vô hiệu hóa tài khoản nếu tài khoản đó đăng nhập sai nhiều lần vượt số lần quy định;

e) Thông tin xác thực yêu cầu cần thay đổi định kỳ 03 tháng/lần;

g) Thiết lập hệ thống để chỉ cho phép đăng nhập vào hệ thống vào khoảng thời gian hợp lệ (theo quy định của tổ chức;

h) Quản lý thông tin xác thực trên hệ thống quản lý tập trung.

#### 8.1.2.2 Kiểm soát truy nhập (S4)

Yêu cầu bao gồm:

a) Thiết lập hệ thống chỉ chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản trị máy chủ từ xa thông qua môi trường mạng;

b) Thay đổi cổng quản trị mặc định của máy chủ;

c) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi máy chủ không nhận được yêu cầu từ người dùng;

d) Giới hạn địa chỉ IP nguồn được phép truy nhập, quản trị máy chủ từ xa;

đ) Thiết lập hệ thống không truy nhập trực tiếp cổng quản trị, phần mềm quản trị máy chủ từ các mạng bên ngoài; thực hiện gián tiếp thông qua kết nối mạng riêng ảo hoặc các phương thức khác tương đương;

e) Phân quyền truy nhập, quản trị, sử dụng tài nguyên khác nhau trên máy chủ với người sử dụng/ nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau.

#### 8.1.2.3 Nhật ký hệ thống (G4)

Yêu cầu bao gồm:

a) Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau:

- Thông tin kết nối mạng tới máy chủ (Firewall log),

- Thông tin trạng thái hoạt động của máy chủ (CPU, RAM, Network…),

- Thông tin các lỗi phát sinh trong quá trình hoạt động,

- Thông tin đăng nhập và truy nhập tài nguyên trên máy chủ,

- Thông tin quản trị, thay đổi cấu hình trên máy chủ (thời gian, địa chỉ, tài khoản truy nhập và thao tác trên máy chủ và các thông tin quản trị khác cần ghi nhật ký (nếu có),

- Các thông tin khác cần ghi nhật ký theo yêu cầu thực tế (nếu có);

b) Đồng bộ thời gian giữa máy chủ với máy chủ thời gian của hệ thống;

c) Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống để không mất hoặc tràn nhật ký hệ thống;

d) Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý nhật ký hệ thống tập trung, gửi dữ liệu nhật ký hệ thống về hệ thống trung tâm theo thời gian thực;

đ) Lưu dữ liệu nhật ký hệ thống trên hệ thống lưu trữ riêng biệt; lưu trữ có mã hóa đối với dữ liệu nhật ký hệ thống của máy chủ quan trọng;

e) Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 12 tháng.

#### 8.1.2.4 Phòng chống xâm nhập (G4)

Yêu cầu bao gồm:

a) Loại bỏ các tài khoản không sử dụng và các tài khoản không còn hợp lệ trên máy chủ;

b) Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng;

c) Sử dụng tường lửa của hệ điều hành máy chủ để cấm các truy nhập trái phép tới máy chủ;

d) Có cơ chế cập nhật và xử lý bản vá, điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ từ hệ thống quản lý tập trung;

đ) Thực hiện nâng cấp, xử lý điểm yếu, lỗ hổng bảo mật trên máy chủ trước khi đưa vào sử dụng;

e) Thực hiện cấu hình tối ưu, tăng cường bảo mật cho máy chủ trước khi đưa vào sử dụng.

#### 8.1.2.5 Phòng chống phần mềm độc hại (G4)

Yêu cầu bao gồm:

a) Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm;

b) Có phương án kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt lên máy chủ;

c) Quản lý tập trung (cập nhật, cảnh báo và quản lý) các phần mềm phòng chống mã độc trên máy chủ và các máy tính người sử dụng trong hệ thống;

d) Có cơ chế kiểm tra, xử lý mã độc của các phương tiện lưu trữ di động (USB, đĩa flash…) trước khi kết nối với máy chủ.

#### 8.1.2.6 Xử lý máy chủ khi chuyển giao (S4)

Khi chuyển giao hoặc thay đổi mục đích sử dụng phải thực hiện:

a) Sao lưu, dự phòng thông tin, dữ liệu trên máy chủ, ảnh của hệ điều hành máy chủ;

b) Xóa toàn bộ dữ liệu lưu trữ trên máy chủ và xóa hệ điều hành máy chủ;

c) Sử dụng các biên pháp kỹ thuật hoặc thiết bị chuyên dụng để bảo đảm dữ liệu không thể khôi phục sau khi xóa.

### 8.1.3 Bảo đảm an toàn ứng dụng

#### 8.1.3.1 Xác thực (S4)

Yêu cầu bao gồm:

a) Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi quản trị, cấu hình cấu hình ứng dụng và sử dụng ứng dụng (nếu ứng dụng cần quản lý truy nhập);

b) Thiết lập chính sách an toàn mật khẩu cho máy chủ bao gồm các yêu cầu cơ bản sau:

- Yêu cầu thay đổi mật khẩu mặc định,

- Thiết lập thời gian yêu cầu thay đổi mật khẩu,

- Thiết lập thời gian mật khẩu hợp lệ,

- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự;

c) Vô hiệu hóa hoặc thay đổi các thông tin các tài khoản mặc định (nếu có);

d) Lưu trữ mã hóa thông tin xác thực trên hệ thống;

đ) Mã hóa thông tin xác thực trước khi gửi qua môi trường mạng;

e) Thiết lập cấu hình ứng dụng để ngăn cản việc đăng nhập tự động;

g) Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định;

h) Quản lý thông tin xác thực trên hệ thống quản lý tập trung;

i) Vô hiệu hóa tài khoản nếu đăng nhập sai nhiều lần vượt số lần quy định;

k) Thông tin xác thực yêu cầu cần thay đổi định kỳ 03 tháng/lần.

**8.1.3.2 Kiểm soát truy nhập (S4)**

Yêu cầu bao gồm:

a) Thiết lập hệ thống chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản trị ứng dụng từ xa thông qua môi trường mạng;

b) Thiết lập hệ thống cấm truy nhập trực vào trang quản trị, cổng quản trị ứng dụng từ các mạng bên ngoài mà cần thực hiện gián tiếp bằng cách sử dụng mạng riêng ảo hoặc các phương thức khác tương đương;

c) Giới hạn địa chỉ IP quản trị được phép truy nhập, quản trị ứng dụng từ xa;

d) Thay đổi, tách biệt cổng kết nối quản trị ứng dụng với cổng cung cấp dịch vụ ứng dụng;

đ) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng;

e) Phân quyền truy nhập, quản trị, sử dụng tài nguyên khác nhau của ứng dụng với người sử dụng/ nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau;

g) Cấp quyền tối thiểu (quyền truy nhập, quản trị) cho tài khoản quản trị ứng dụng theo quyền hạn;

h) Thiết lập quyền tối thiểu (chỉ cấp quyền truy cập cơ sở dữ liệu) cho tài khoản kết nối cơ sở dữ liệu;

k) Giới hạn số lượng các kết nối đồng thời (kết nối khởi tạo và đã thiết lập) đối với các ứng dụng, dịch vụ máy chủ cung cấp.

#### 8.1.3.3 Nhật ký hệ thống (G4)

Yêu cầu bao gồm:

a) Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau:

- Thông tin thông tin thời gian, địa chỉ, tài khoản (nếu có), nội dung truy nhập và sử dụng ứng dụng ứng dụng,

- Thông tin các lỗi phát sinh trong quá trình hoạt động,

- Thông tin quản trị, thay đổi cấu hình ứng dụng,

b) Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý nhật ký hệ thống tập trung, gửi dữ liệu nhật ký hệ thống về hệ thống trung tâm theo thời gian thực;

c) Lưu dữ liệu nhật ký hệ thống trên hệ thống lưu trữ riêng biệt; lưu trữ có mã hóa đối với dữ liệu nhật ký hệ thống của máy chủ quan trọng;

d) Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 06 tháng.

#### 8.1.3.4 Bảo mật thông tin liên lạc (S4)

Yêu cầu bao gồm:

a) 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) Sử dụng giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương;

c) Sử dụng kết hợp các giao thức với phương pháp mã hóa dữ liệu để tạo thành 02 lớp bảo vệ dữ liệu 2 khi truyền qua môi trường mạng.

#### 8.1.3.5 Chống thoái thác (G4)

Yêu cầu bao gồm:

a) Cung cấp chức năng chức thực, xác minh thông tin, nguồn gửi thông tin khi trao đổi dữ liệu nhạy cảm qua môi trường mạng;

b) Áp dụng cơ chế xác thực hai chiều khi trao đổi dữ liệu quan trọng qua môi trường mạng;

b) Sử dụng thiết bị lưu trữ chuyên dụng để lưu trữ thông tin xác thực.

### 8.1.4 An toàn dữ liệu

#### 8.1.4.1 Nguyên vẹn dữ liệu (S4)

Yêu cầu bao gồm:

a) Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống bảo đảm tính nguyên vẹn;

b) Có phương án giám sát, cảnh báo khi có thay đổi thông tin, dữ liệu lưu trên hệ thống lưu trữ/phương tiện lưu trữ.

#### 8.1.4.2 Bảo mật dữ liệu (S4)

Yêu cầu bao gồm:

a) Lưu trữ có mã hóa các thông tin, dữ liệu không công khai trên hệ thống lưu trữ/phương tiện lưu trữ;

b) Thiết lập phân vùng lưu trữ mã hóa, chỉ cho phép người có quyền, trách nhiệm truy nhập, lưu trữ dữ liệu trên phân vùng mã hóa.

#### 8.1.4.3 Sao lưu dự phòng (A4)

a) Thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, sơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ;

b) Phân loại và quản lý các dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau;

c) Có hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng;

d) Sử dụng cơ chế tự động sao lưu dự phòng đối với thông tin/dữ liệu thay đổi thường xuyên hoặc cập nhật bản sao lưu dự phòng khi thay đổi;

đ) Sử dụng hệ thông sao lưu dự phòng hỗ trợ chức năng dự phòng dự phòng nóng (online), dự phòng nguội (offline) và các chức năng dự phòng khác (theo yêu cầu thực tế);

e) Sử dụng hệ thông sao lưu dự phòng có khả năng chịu lỗi, cho phép khôi phục dữ liệu nóng khi một thành phần trong hệ thống xảy ra sự cố.

## 8.2 Yêu cầu quản lý

### 8.2.1 Chính sách an toàn thông tin

#### 8.2.1.1. Chính sách an toàn thông tin

Yêu cầu này bao gồm:

a) Xác định các mục tiêu, nguyên tắc bảo đảm an toàn thông tin;

b) Xác định trách nhiệm của đơn vị quản lý an toàn thông tin, các thành viên trong ban quản lý an toàn thông tin và các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin;

c) Xác định phạm vi quản lý an toàn bao gồm các nội dung cơ bản sau:

- Phạm vi quản lý về vật lý và logic của tổ chức;

- Các loại tài sản (tài liệu, dữ liệu, thiết bị, con người…);

- Các ứng dụng, dịch vụ hệ thống cung cấp;

- Nguồn nhân lực bảo đảm an toàn thông tin (Cấp Lãnh đạo, cán bộ quản lý, cán bộ kỹ thuật, nhân viên…);

d) Xây dựng chính sách an toàn thông tin cơ bản cho người sử dụng bao gồm:

- Truy nhập, sử dụng tài nguyên trên nội bộ

- Truy nhập mạng và tài nguyên trên Internet

- Cài đặt và sử dụng máy tính an toàn

- An toàn dữ liệu

- Sử dụng và quản lý tài sản

đ) Xây dựng chính sách an toàn thông tin cho người quản trị bao gồm:

- Quản lý an toàn mạng

- Quản lý an toàn máy chủ và ứng dụng

- Quản lý an toàn dữ liệu

- Quản lý an toàn thiết bị đầu cuối

- Quản lý thiết bị hệ thống

- Quản lý giám sát an toàn thông tin

- Quản lý phòng chống phần mềm độc hại

- Quản lý điểm yếu an toàn thông tin

- Quản lý sự cố an toàn thông tin

- Quản lý phương án ứng cứu khẩn cấp

**8.2.1.2 Xây dựng và công bố (G4)**

Yêu cầu này bao gồm:

a) Được xây dựng thống nhất và được quản lý theo từng phiên bản;

b) Được thẩm định, thông qua trước khi triển khai áp dụng;

c) Công bố trước 01 tháng khi áp dụng;

d) Tổ chức tuyên truyền, bổ biến cho toàn bộ cán bộ, cán bộ trong tổ chức.

**8.2.1.3. Rà soát, sửa đổi (G4)**

Yêu cầu bao gồm:

a) Định kỳ 12 tháng hoặc đột xuất (khi có thay đổi chính sách) kiểm tra lại chính sách quản lý an toàn để tìm ra điểm chưa hợp lý, thiếu sót cần phải chỉnh sửa hoặc bổ sung;

b) Có hồ sơ lưu lại lại những thông tin về những trong việc triển khai, áp dụng chính sách quản lý an toàn thông tin, phản hồi của đối tượng áp dụng chính sách.

### 8.2.2 Tổ chức bảo đảm an toàn thông tin

#### 8.2.2.1 Đơn vị quản lý an toàn thông tin (G4)

Yêu cầu bao gồm:

a) Thành lập đơn vị chuyên trách hoặc chỉ định đơn vị (hoặc bộ phần) có trách nhiệm quản lý về an toàn thông tin trong tổ chức (Đơn vị quản lý an toàn thông tin);

b) Phân định vai trò và trò và trách nhiệm, cơ chế phối hợp của các bộ phận, thành viên trong Đơn vị quản lý an toàn thông tin;

c) Chỉ định bộ phận chuyên trách có trách nhiệm xây dựng và quản lý chính sách an toàn thông tin.

d) Chỉ định bộ phận có trách nhiệm thực thi chính sách an toàn thông tin đã xây dựng.

#### 8.2.2.2 Liên lạc với những cơ quan/tổ chức có thẩm quyền

Yêu cầu bao gồm:

a) Xác định và lưu thông tin các cơ quan có chức năng quản lý và thực thi công tác bảo đảm an toàn thông tin;

b) Xác định và lưu thông tin các cơ quan trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin;

c) Xây dựng quy chế, thỏa thuận phối hợp giữa tổ chức với các cơ quan chức năng;

d) Cử đầu mối liên hệ/đại diện tổ chức trong việc tổ chức thực hiện quy chế, thỏa thuận.

#### 8.2.2.3 Liên lạc với các nhóm chuyên gia

Yêu cầu bao gồm:

a) Xác định và lưu thông tin các chuyên gia/nhóm chuyên gia trong lĩnh vực an toàn thông tin;

b) Xác định và lưu thông tin cơ quan, tổ chức cung cấp dịch vụ an toàn thông tin;

c) Xây dựng thỏa thuận phối hợp, quy chế làm việc giữa tổ chức với các chuyên gia/nhóm chuyên gia; cơ quan, tổ chức cung cấp dịch vụ an toàn thông tin.

### 8.2.3. Bảo đảm nguồn nhân lực (G4)

#### 8.2.3.1.Trước khi tuyển dụng

Yêu cầu bao gồm:

a) Có quy định về quy trình tuyển dụng cán bộ; thẩm tra về lý lịch, thân phận của cán bộ được tuyển dụng; có chuyên gia trong lĩnh vực đánh giá, kiểm tra trình độ chuyên môn phù hợp với vị trí tuyển dụng;

b) Các điều khoản và điều kiện tuyển dụng: đưa ra các điều khoản, điều kiện trong hợp đồng với nhân viên và nhà thầu; trách nhiệm của của các bên liên quan trong hợp đồng;

c) Cán bộ được tuyển dụng yêu cầu có trình độ chuyên môn phù hợp với vị trí tuyển dụng, hiểu biết và có kinh nghiệm tối thiểu 02 năm trong lĩnh vực an toàn thông tin;

d) Có bản thỏa thuận riêng và ký xác nhận với cán bộ được tuyển dụng vào các vị trí quan trọng như: quyền, trách nhiệm, phạm vi, thời gian và các thỏa thuận khác liên quan.

**8.2.3.2 Trong quá trình làm việc**

Yêu cầu này bao gồm:

a) Tổ chức đào tạo nâng cao nhận thức về an toàn thông tin và kỹ năng an toàn cơ bản về an toàn thông tin trong quá trình làm việc trước khi làm việc chính thức trong tổ chức;

b) Có kế hoạch và định kỳ 01 năm tổ chức đào tạo về an toàn thông tin hàng năm cho 03 nhóm đối tượng bao gồm: cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống;

c) Có tiêu chí đánh giá kỹ năng, kiến thức chuyên môn, cũng như nhận thức về an toàn thông tin đối với cán bộ ở các vị trí;

đ) Định kỳ 01 năm tiến hành kiểm tra kỹ năng, kiến thức chuyên môn, cũng như nhận thức về an toàn thông tin đối với cán bộ ở các vị trí.

**8.2.3.2 Chấm dứt hoặc thay đổi công việc**

a) Có quy định về quản lý các quy trình, thủ tục cán bộ thôi việc, quy trình nghỉ việc của cán bộ cần tuân thủ theo quy trình, thủ tục đã quy định;

b) Có quy trình vô hiệu hóa tất cả các quyền truy cập thông tin riêng của tổ chức, quyền truy cập, quản trị hệ thống sau khi có cán bộ thôi việc;

c) Có quy trình thu hồi tất cả các văn bản, giấy tờ, các thẻ tín dụng, các thẻ truy cập, thông tin được lưu trên các phương tiện điện tử; các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác của tổ chức do cán bộ quản lý và sử dụng;

d) Cán bộ nghỉ việc phải có đơn và thông báo trước 03 tháng;

đ) Có cam kết giữ bí mật thông tin liên quan đến tổ chức đối với cán bộ ở vị trí chủ chốt sau khi nghỉ việc.

### 8.2.4 Quản lý xây dựng hệ thống thông tin

#### 8.2.4.1 Xác định cấp độ an toàn hệ thống thông tin (G4)

Yêu cầu bao gồm:

a) Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin;

b) Có tài liệu mô tả các thành phần của hệ thống thông tin bao gồm: các vùng mạng chức năng; hệ thống thiết bị mạng, thiết bị bảo mật; hệ thống máy chủ hệ thống; hệ thống máy chủ ứng dụng; dịch vụ và các thành phần khác trong hệ thống thông tin;

c) Có tài liệu mô tả loại thông tin các thành phần trong hệ thống thông tin xử lý bao gồm: thông tin công cộng, thông tin riêng, thông tin cá nhân, thông tin bí mật nhà nước và các loại thông tin khác (nếu có);

d) Có tài liệu mô tả loại hệ thống thông tin căn cứ theo chức năng phục vụ hoạt động nghiệp vụ bao gồm: hệ thống thông tin phục vụ hoạt động nội bộ, hệ thống thông tin phục vụ người dân, doanh nghiệp, hệ thống cơ sở hạ tầng thông tin, hệ thống thông tin điều khiển công nghiệp, hệ thống thông tin khác (nếu có);

đ) Có tài liệu mô tả, giải thích tính phù hợp của cấp độ đề xuất;

e) Có ý kiến thẩm định của đơn vị chuyên môn trước khi phê duyệt cấp độ;

g) Định kỳ 02 năm xác định lại cấp độ an toàn hệ thống thông tin hoặc khi có thay đổi, nâng cấp, mở rộng hệ thống.

#### 8.2.4.2 Thiết kế an toàn hệ thống thông tin (G4)

Yêu cầu bao gồm:

a) Có tài liệu mô tả thiết kế mô tả những thông tin sau:

- Thiết kế vật lý hệ thống thông tin (thiết bị, kết nối vật lý)

- Thiết kế logic hệ thống thông tin (các phân vùng mạng, chức năng);

- Ứng dụng, dịch vụ hệ thống (DNS, DHCP, NTP…)

- Ứng dụng, dịch vụ phục vụ hoạt động nghiệp vụ

b) Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ

c) Có tài liệu thiết kế phương án bảo đảm an toàn thông tin theo yêu cầu thiết kế hệ thống;

d) Có bộ phận chuyên môn, tổ chuyên gia đánh giá, thẩm định hồ sơ thiết kế hệ thống thông tin, các biện pháp bảo đảm an toàn thông tin trước khi triển khai thực hiện;

đ) Định kỳ 01 năm kiểm tra tính hợp lý trong thiết kế và các biện pháp bảo đảm an toàn thông tin cho hệ thống hoặc khi mở rộng, nâng cấp hệ thống thông tin.

**8.2.4.3 Phát triển phần mềm thuê khoán**

Yêu cầu bao gồm:

a) Có tài liệu mô tả các chức năng, yêu cầu an toàn phần mềm cần đáp ứng;

b) Có tài liệu mô tả phương án, thiết kế, mô tả khả năng đáp ứng các yêu cầu đặt ra;

c) Phần mềm cần đáp ứng các tiêu chuẩn, quy chuẩn kỹ thuật theo quy định (nếu có);

d) Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm; thực hiện kiểm tra, đánh giá an toàn thông tin cho phần mềm trước khi sử dụng;

đ) Kiểm thử phần mềm trên môi trường thử nghiệm và được nghiệm thu trước 01 tháng trước khi đưa vào sử dụng;

e) Có bên thứ 3 thực hiện kiểm tra, đánh giá độc lập an toàn thông tin cho phần mềm;

g) Có cam kết của bên phát triển về bảo đảm tính bí mật và độc quyền của phần mềm phát triển.

**8.2.4.4 Thử nghiệm và bàn giao hệ thống**

Yêu cầu bao gồm:

a) Có nội dung, kế hoạch thử nghiệm và nghiệm thu hệ thống;

b) Có bộ phận có trách nhiệm thực hiện nghiệm thu và kiểm thử hệ thống;

c) Có đơn vị độc lập (bên thứ 3) tư vấn và giám sát quá trình thực nghiệm và kiểm thử hệ thống;

đ) Có báo cáo nghiệm thu được thẩm định và xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng;

e) Có xác nhận của cơ quan chức năng về hợp chuẩn, hợp quy của hệ thống thông tin trước khi đưa vào sử dụng.

**8.2.4.5 Các mối liên hệ với bên cung cấp dịch vụ an toàn thông tin**

Yêu cầu bao gồm:

a) Có quy định về các yêu cầu, các thỏa thuận, quyền hạn và trách nhiệm của bên cung cấp;

b) Có quy trình ký kết, thực hiện và duy trì các cam kết trong hợp đồng đối với các bên cung cấp;

c) Có thỏa thuận và cam kết trách nhiệm của mỗi bên trước khi được ký kết hợp đồng;

d) Bên cung cấp dịch vụ an toàn thông tin được cơ quan có thẩm quyền cấp phép;

đ) Bên cung cấp dịch vụ an toàn thông tin được cơ quan có thẩm quyền chỉ định.

### 8.2.5 Quản lý vận hành hệ thống

#### 8.2.5.1 Quản lý an toàn mạng

Yêu cầu bao gồm:

a) Xây dựng chính sách quản lý an toàn mạng, bao gồm các yêu cầu cơ bản sau:

- Chính sách kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng

- Chính sách quản lý kiểm soát truy nhập đi vào và từ hệ thống đi ra

- Chính sách truy nhập và quản lý cấu hình hệ thống

- Chính sách bảo đảm an toàn dữ liệu qua môi trường mạng

- Chính sách sao lưu và dự phòng và khôi phục cấu hình hệ thống

- Chính sách ghi nhật ký hệ thống và giám sát an toàn thông tin

b) Xây dựng quy trình quản lý, vận hành hoạt động bình thường của hệ thống;

c) Xây dựng quy trình cập nhật; sao lưu, dự phòng các tệp tin cấu hình hệ thống;

d) Xây dựng quy trình cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác;

đ) Xây dựng quy trình khôi phục hệ thống sau khi xảy ra sự cố; định kỳ 01 năm thực hiện diễn tập theo quy trình.

#### 8.2.5.2 Quản lý an toàn máy chủ và ứng dụng

Yêu cầu bao gồm:

a) Xây dựng chính sách quản lý an toàn máy chủ và ứng dụng, bao gồm các yêu cầu cơ bản sau:

- Chính sách về quản lý và sử dụng máy chủ và ứng dụng an toàn,

- Chính sách truy nhập và quản trị máy chủ và ứng dụng,

- Chính sách truy nhập mạng,

- Chính sách bảo đảm an toàn dữ liệu qua môi trường mạng,

- Chính sách sao lưu và dự phòng và khôi phục cấu hình hệ thống,

- Chính sách ghi nhật ký hệ thống và giám sát an toàn thông tin;

b) Xây dựng quy trình cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng;

c) Xây dựng quy trình quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ;

d) Xây dựng quy trình cấu hình tối tưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ và dịch vụ và thực hiện quy trình trước khi đưa hệ thống vào sử dụng;

đ) Xây dựng quy trình kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống;

e) Xây dựng quy trình cập nhật; sao lưu, dự phòng các tệp tin cấu hình hệ thống, tệp tin dự phòng hệ điều hành và các dữ liệu quan trọng khác cần lưu sao lư dự phòng (nếu có);

g) Xây dựng quy trình khôi phục hệ điều hành, ứng dụng, dịch vụ sau khi xảy ra sự cố.

**8.2.5.3 Quản lý an toàn dữ liệu**

Yêu cầu bao gồm:

a) Xây dựng chính sách quản lý an toàn dữ liệu, bao gồm các yêu cầu cơ bản sau:

- Yêu cầu an toàn đối với phương pháp mã hóa;

- Quản lý và sử dụng khóa bí mật;

- Phân loại, quản lý dữ liệu bí mật;

- Cơ chế mã hóa và kiểm tra tính toàn vẹn của dữ liệu;

- Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ;

- Sao lưu, dự phòng và phôi phục dữ liệu (tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ).

b) Xây dựng danh sách thông tin, tệp tin và dữ liệu, phần mềm và các tài nguyên khác trên hệ thống cần dự phòng;

c) Xây dựng quy trình sao lưu dự phòng, định kỳ 01 tuần (hoặc khi có thay đổi trên hệ thống cần sao lưu dự phòng) thực hiện quy trình sao lưu dự phòng;

d) Xây dựng quy trình khôi phục dữ liệu dự phòng;

đ) Xây dựng quy trình kiểm tra, vận hành và bảo trì hệ thống sao lưu dự phòng.

**8.2.5.4 Quản lý an toàn thiết bị đầu cuối**

Yêu cầu bao gồm:

a) Xây dựng chính sách quản lý an toàn thiết bị đầu cuối, bao gồm các yêu cầu cơ bản sau:

- Chính sách về quản lý và sử dụng các thiết bị đầu cuối an toàn;

- Chính sách kết nối thiết bị đầu cuối vào hệ thống;

- Chính sách kết nối, truy nhập và sử dụng thiết bị đầu cuối từ xa;

- Chính sách bảo đảm an toàn vật lý cho thiết bị đầu cuối;

b) Xây dựng quy trình quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối;

c) Xây dựng quy trình cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối vào hệ thống;

d) Xây dựng quy trình cấu hình tối tưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng;

đ) Xây dựng quy trình kiểm tra, đánh giá an toàn thông tin xử lý điểm yếu, lỗ hổng bảo mật cho thiết bị đầu cuối.

**8.2.5.5 Quản lý thiết bị hệ thống**

Yêu cầu bao gồm:

a) Xây dựng chính sách truy nhập, quản lý và cấu hình thiết bị;

b) Quy định về các điều kiện bảo đảm an toàn vật lý cho thiết bị;

c) Xây dựng quy trình lắp đặt, cài đặt kết nối và gỡ bỏ thiết bị khỏi hệ thống;

d) Xây dựng quy trình quản lý, vận hành khai thác hoạt động bình thường của thiết bị;

đ) Xây dựng quy trình bảo dưỡng, bảo trì thiết bị;

e) Xây dựng hướng dẫn cách sử dụng, quản lý, vận hành thiết bị các thiết bị đầu cuối và các thiết bị dự phòng;

g) Chỉ định bộ phận có trách nhiệm quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị và thiết bị dự phòng).

**8.2.5.6 Quản lý phòng chống phần mềm độc hại**

Yêu cầu bao gồm:

a) Xây dựng quy định cho người sử dụng về việc cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng;

b) Xây dựng quy định về việc gửi nhận tệp tin từ môi trường mạng và qua các phương tiện lưu trữ di động;

d) Xây dựng quy định, quy trình về việc cài đặt, cập nhật và sử dụng phần mềm diệt virus; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động;

đ) Định kỳ 01 tháng (hoặc khi phát hiện hoạt động không bình thường của hệ thống) thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống.

**8.2.5.7 Quản lý giám sát an toàn thông tin**

Yêu cầu bao gồm:

a) Xây dựng chích sách giám sát an toàn thông tin bao gồm các yêu cầu cơ bản sau:

- Chính sách truy nhập và quản lý hệ thống giám sát;

- Quy định về việc kết nối; gửi dữ liệu từ các thiết bị được giám sát về hệ thống giám sát;

- Quy định về những loại thông tin cần được giám sát;

- Quy định về việc lưu trữ và bảo đảm an toàn thông tin giám sát (nhật ký hệ thống);

- Quy định về việc đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát.

b) Xây dựng quy trình, quy định việc kết nối đối tượng giám vào hệ thống giám sát;

c) Xây dựng quy trình quản lý vận hành hệ thống giám sát, hệ thống tập trung (nếu có);

d) Xây dựng quy trình theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin;

đ) Chỉ định bộ phận có trách nhiệm giám sát hệ thống thông tin.

**8.2.5.8 Quản lý điểm yếu an toàn thông tin**

Yêu cầu bao gồm:

a) Xây dựng danh mục, phiên bản, chức năng cho các thành phần có trong hệ thống (thiết bị mạng, bảo mật; hệ điều hành; máy chủ; ứng dụng, dịch vụ và các thành phần khác trong hệ thống có thể tồn tại điểm yếu an toàn thông tin và các thông tin);

b) Xây dựng danh sách nguồn cung cấp điểm yếu an toàn thông tin; phân nhóm và mức độ của điểm yếu cho các thành phần trong hệ thống đã xác định;

c) Xây dựng danh sách đầu mối các nhóm chuyên ra, bên cung cấp dịch vụ hỗ trợ, cung cấp dịch vụ xử lý, khắc phục điểm yếu an toàn thông tin;

d) Có quy định về việc cập nhật thông tin, cơ chế cảnh báo các điểm yếu an toàn thông tin cho các bộ phận có trách nhiệm tương ứng;

đ) Xây dựng quy trình, phương án xử lý, khắc phục điểm yếu an toàn thông tin theo các nhóm hạ tầng mạng; hệ điều hành; ứng dụng và dịch vụ và các nhóm khác nếu cần quản lý;

e) Xây dựng các phương án xử lý tạm thời khi điểm yếu an toàn thông tin không/chưa có khả năng xử lý;

g) Xây dựng quy trình khôi phục lại hệ thống sau khi xử lý điểm yếu an toàn thông tin thất bại;

h) Chỉ định bộ phận có trách nhiệm quản lý điểm yếu an toàn thông tin.

**8.2.5.9 Quản lý sự cố an toàn thông tin**

Yêu cầu bao gồm:

a) Xây dựng danh sách, tiêu chí và phân loại các sự cố an toàn thông tin theo các nhóm sự cố: sự cố an toàn vật lý, sự cố an toàn mạng, sự cố an toàn máy chủ, sự cố an toàn dịch vụ;

b) Xây dựng danh sách đầu mối các nhóm chuyên ra, bên cung cấp dịch vụ hỗ trợ, cung cấp dịch vụ xử lý, khắc phục sự cố an toàn thông tin;

c) Xây dựng phương án khắc phục, xử lý các loại sự cố an toàn thông tin tương ứng;

đ) Xây dựng quy trình phát hiện và cảnh báo sự cố an toàn thông tin;

e) Xây dựng quy trình khắc phục, xử lý sự cố an toàn thông tin bao gồm: tiếp nhận sự cố, xác minh/xác nhận sự cố, phân loại sự cố, báo cáo sự cố, thu thập thông tin để phục vụ phân tích sự cố, phân tích sự cố; xử lý sự cố, tổng hợp báo cáo, lưu hồ sơ sự cố;

g) Xây dựng quy trình điều tra, phân tích và thu thập chứng cứ;

h) Quy định về việc lưu hồ sơ quá trình xử lý, tổng kết bài học kinh nghiệm; đưa ra biện pháp ngăn chặn sự cố tái phát sinh; cần lưu hồ sơ toàn quá trình thực hiện;

i) Xây dựng quy trình riêng đối với những sự cố nghiêm trọng cần xử lý đặc biệt (ví dụ: sự cố gây gián đoạn hoạt động toàn hệ thống hoặc lộ lọt thông tin bí mật..) và chỉ định bộ phận chuyên trách thực hiện;

k) Xây dựng phương án báo cáo cơ quan chức năng (theo các quy định của nhà nước) trong trường hợp cần hỗ trợ điều phối, xử lý;

l) Chỉ định bộ phận chó trách nhiệm quản lý và thực thi xử lý sự cố an toàn thông tin

**8.2.5.10 Quản lý phương án ứng cứu khẩn cấp**

Yêu cầu bao gồm:

a) Xác định, xây dựng tiêu chí phân loại sự cố an toàn thông tin cần xử lý theo phương án ứng cứu khẩn cấp;

b) Chỉ định và phân trách nhiệm cho bộ phận và thành phần tham gia phương án ứng cứu khẩn cấp;

c) Quy định về phương án phân bổ tài nguyên (con người, tài chính, phương tiện, biện pháp kỹ thuật…) cho phương án ứng cứu khẩn cấp;

d) Xây dựng phương án ứng cứu khẩn cấp theo từng cấp độ ứng cứu khẩn cấp;

đ) Xây dựng quy trình thực hiện phương án ứng cứu khẩn cấp;

e) Định kỳ hàng năm, tổ chức đào tạo, nâng cao kỹ năng cho cán bộ chuyên trách có trách nhiệm thực hiện phương án ứng cứu khẩn cấp;

g) Định kỳ hàng năm tổ chức diễn tập phương án ứng cứu khẩn cấp;

h) Định kỳ (hoặc đột xuất theo yêu cầu thực tế) kiểm tra, rà soát và cập nhật phương án ứng cứu khẩn cấp cho phù hợp với yêu cầu và tình hình thực tế.

# 9 Yêu cầu cơ bản cho cấp độ 5

## 9.1 Yêu cầu kỹ thuật

### 9.1.1 Bảo đảm an toàn hạ tầng mạng

#### 9.1.1.1 Thiết kế hệ thống (G5)

Yêu cầu bao gồm:

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, bao gồm cơ bản cơ bản các vùng mạng:

- Vùng mạng nội bộ (LAN)

- Vùng mạng biên (Outside)

- Vùng mạng máy chủ công cộng (DMZ),

- Vùng mạng máy chủ nội bộ (Server Farm)

- Vùng mạng cho máy chủ cơ sở dữ liệu (Database)

- Vùng mạng máy chủ quản trị (Management)

- Vùng mạng khác (nếu có) theo yêu cầu, mục đích của tổ chức;

b) Phương án thiết kế bảo đảm các yêu cầu sau:

- Không triển khai các máy chủ cơ sở dữ liệu hoặc đặt cơ sở dữ liệu, máy chủ nội bộ trong vùng mạng máy chủ công cộng

- Thiết kế vùng mạng nội bộ thành các mạng chức năng theo yêu cầu nghiệp vụ (VLAN)

- Thiết kế phân vùng mạng riêng cho mạng không dây (nếu có) tách biệt với các vùng mạng chức năng

- Thiết lập một vùng mạng riêng (vùng mạng quản trị thiết bị) bao gồm các địa chỉ quản trị của các thiết bị hệ thống; kiểm soát, giám sát các truy nhập từ vùng mạng khác vào vùng mạng này

- Có biện pháp quản lý truy nhập và phòng chống xâm nhập

- Có phương án chặn lọc phần mềm độc hại trên môi trường mạng

- Có phương án bảo vệ máy chủ cơ sở dữ liệu chuyên dụng

- Thiết kế các thiết bị mạng có thiết kế dự phòng nóng (HA hoặc AA) bảo đảm tính khả dụng của hệ thống của hệ thống; năng lực của thiết bị đáp ứng theo quy mô hệ thống mạng, số lượng dịch vụ cung cấp và người dùng có trong hệ thống

- Có phương án truy nhập, quản trị hệ thống từ xa an toàn

- Có phương án phòng chống tấn công từ chối dịch vụ

- Có phương án giám sát tập trung hoạt động bình thường của hệ thống

- Có phương án giám sát tập trung sự kiện an toàn thông tin trên hệ thống

- Có phương án quản lý lưu trữ tập trung

- Có phương án quản lý tập trung các phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng trong hệ thống

- Có phương án quản lý cập nhật bản vá, điểm yếu an toàn thông tin tập trung

- Có phương án quản lý mạng không dây tập trung

- Có phương án quản lý đăng nhập tập trung

- Có phương án quản lý tài khoản đặc quyền

- Có phương án quản lý chính sách bảo mật tập trung

- Có phương án kiểm soát/ giám sát kết nối mạng giữa các mạng trong mạng nội bộ

- Có phương án dự phòng ở vị trí địa lý khác nhau; yêu cầu có 02 kết nối độc lập giữa hệ thống chính và hệ thống dự phòng, phục vụ việc trao đổi, đồng bộ và sao lưu dự phòng dữ liệu.

**9.1.1.2 Kiểm soát truy nhập từ bên ngoài mạng (G5)**

Yêu cầu bao gồm:

a) Thiết lập hệ thống chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản lý và sử dụng tài nguyên nội bộ trong hệ thống từ các mạng bên ngoài;

b) Kiểm soát truy nhập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép từ bên ngoài;

c) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng.

d) Phân quyền và cấp quyền truy nhập từ bên ngoài vào hệ thống theo theo từng người dùng hoặc nhóm người dùng căn cứ theo yêu cầu nghiệp vụ, yêu cầu quản lý;

đ) Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ hệ thống cung cấp theo quy mô và khả năng cung cấp của hệ thống

e) Kiểm soát truy nhập từ bên ngoài mạng theo thời gian quy định của tổ chức;

g) Kiểm soát truy nhập từ bên ngoài theo địa chỉ nguồn truy cập (theo chính sách của tổ chức nếu có).

**9.1.1.3 Kiểm soát truy nhập từ bên trong mạng (S5)**

Yêu cầu bao gồm:

a) Cho phép truy nhập ra bên ngoài các địa chỉ Internet, ứng dụng, dịch vụ theo yêu cầu nghiệp vụ; chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức;

b) Có phương án quản lý tập trung các thiết bị đầu cuối kết nối vào hệ thống, bao gồm các chức năng cơ bản sau:

- Quản lý theo địa chỉ vật lý, địa chỉ logic,

- Tài khoản người sử dụng,

- Chính sách cài đặt và thiết lập cấu hình bảo mật trên thiết bị,

- Các chính sách khác của hệ thống (nếu có)

c) Triển khai hệ thống giám sát, phát hiện và ngăn chặn truy cập từ bên trong mạng đến các địa chỉ Internet bị cấm truy cập theo chính sách của tổ chức

d) Giới hạn truy nhập theo thời gian (theo chính sách truy nhập của tổ chức nếu có);

đ) Có phương án quản lý tập trung việc truy nhập, sử dụng tài nguyên của máy tính người sử dụng.

**9.1.1.4 Nhật ký hệ thống (G5)**

Yêu cầu bao gồm:

a) Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị;

b) Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống;

c) Thông tin về truy cập ứng dụng dịch vụ cần ghi nhật ký bao gồm:

- Thời gian kết nối

- Thông tin kết nối mạng (địa chỉ IP, cổng kết nối)

- Hành động đối với kết nối (cho phép, ngăn chặn)

- Thao tác người sử dụng khi kết nối thành công

- Thông tin các thiết bị đầu cuối kết nối vào hệ thống theo địa chỉ vật lý và logic

- Thông tin và thao tác người quản trị cấu hình, thay đổi hệ thống

- Thông tin cảnh báo từ các thiết bị

d) Giới hạn tài nguyên cho chức năng ghi nhật ký trên thiết bị, để bảo đảm chức năng này không làm ảnh hưởng, gián đoạn hoạt động của thiết bị;

đ) Lưu trữ và quản lý tập trung nhật ký hệ thống trên hệ thống quản lý nhật ký hệ thống tập trung;

e) Lưu trữ dự phòng dữ liệu nhật ký hệ thống trên hệ thống lưu trữ riêng biệt;

g) Phân quyền truy nhập chỉ cho phép tài khoản có chức năng quản lý nhật ký hệ thống có quyền truy nhập quản lý dữ liệu nhật ký hệ thống;

h) Lưu trữ nhật ký hệ thống của thiết bị tối thiểu 12 tháng.

#### 9.1.1.5 Phòng chống xâm nhập (G5)

Yêu cầu bao gồm:

a) Có phương án phòng chống xâm nhập chuyên dụng để bảo vệ các vùng mạng máy chủ công cộng, máy chủ nội bộ, máy chủ cơ sở dữ liệu và vùng mạng nội bộ;

b) Tự động cập nhật thời gian thực cơ sở dữ liệu, dấu hiệu phát hiện tấn công;

c) Bảo đảm năng lực hệ thống bảo đảm đáp ứng đủ theo yêu cầu theo quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp;

đ) Có phương án tự động xử lý bảo đảm hoạt động bình thường của hệ thống khi hệ thống xảy ra sự cố;

e) Có phương án dự phòng nóng hệ thống.

#### 9.1.1.6 Phòng chống phần mềm độc hại trên môi trường mạng (G5)

Yêu cầu bao gồm:

a) Thiết lập hệ thống phòng chống phần mềm độc hại chuyên dụng để bảo vệ các vùng mạng máy chủ và vùng mạng nội bộ;

b) Tự động cập nhật thời gian thực cơ sở dữ liệu cho hệ thống phòng chống phần mềm độc hại.

c) Bảo đảm năng lực hệ thống bảo đảm đáp ứng đủ theo yêu cầu theo quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp;

d) Có phương án tự động xử lý bảo đảm hoạt động bình thường của hệ thống khi hệ thống xảy ra sự cố;

đ) Có phương án dự phòng nóng hệ thống.

#### 9.1.1.7 Bảo vệ thiết bị hệ thống (G5)

Yêu cầu bao gồm:

a) Cấu hình chức năng xác thực trên các thiết bị hệ thống để xác thực người dùng sử dụng quản trị thiết bị trực tiếp hoặc từ xa;

b) Thiết lập hệ thống chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản trị thiết bị;

c) Cho phép hạn chế các địa chỉ IP, địa chỉ mạng có thể kết kết nối, quản trị thiết bị từ xa;

d) Hạn chế được số lần đăng nhập sai khi quản trị hoặc kết nối quản trị từ xa theo địa chỉ IP nguồn;

đ) Phân quyền truy nhập, quản trị thiết bị đối với các tài khoản quản trị có quyền hạn khác nhau;

e) Nâng cấp, xử lý điểm yếu, lỗ hổng bảo mật của thiết bị hệ thống trước khi đưa vào sử dụng;

g) Cấu hình tối ưu, tăng cường bảo mật cho hệ thống thiết bị hệ thống trước khi đưa vào sử dụng;

h) Thiết lập hệ thống quản lý tài khoản đặc quyền để quản lý, giám sát tập trung việc quản trị, cấu hình các thiết bị.

### 9.1.2 Bảo đảm an toàn máy chủ

#### 9.1.2.1 Xác thực (S5)

a) Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng sử dụng khi khi truy nhập, quản lý và sử dụng máy chủ;

b) Thiết lập chính sách an toàn mật khẩu cho máy chủ bao gồm các yêu cầu cơ bản sau:

- Yêu cầu thay đổi mật khẩu mặc định,

- Thiết lập thời gian yêu cầu thay đổi mật khẩu,

- Thiết lập thời gian mật khẩu hợp lệ,

- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự;

c) Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng);

d) Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với một tài khoản nhất định;

đ) Thiết lập cấu hình để vô hiệu hóa tài khoản nếu tài khoản đó đăng nhập sai nhiều lần vượt số lần quy định;

e) Thông tin xác thực yêu cầu cần thay đổi định kỳ 03 tháng/lần;

g) Sử dựng cơ chế xác thực đa nhân tố để xác thực người sử dụng khi truy nhập vào các máy chủ quan trọng trong hệ thống;

h) Thiết lập hệ thống để chỉ cho phép đăng nhập vào hệ thống vào khoảng thời gian hợp lệ (theo quy định của tổ chức);

i) Áp dụng giải pháp xác thực mạnh và quản lý tập trung thông tin xác thực trên hệ thống.

#### 9.1.2.2 Kiểm soát truy nhập (S5)

Yêu cầu bao gồm:

a) Thiết lập hệ thống chỉ chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản trị máy chủ từ xa thông qua môi trường mạng;

b) Thay đổi cổng quản trị mặc định của máy chủ;

c) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi máy chủ không nhận được yêu cầu từ người dùng;

d) Giới hạn địa chỉ IP nguồn được phép truy nhập, quản trị máy chủ từ xa;

đ) Thiết lập hệ thống không truy nhập trực tiếp cổng quản trị, phần mềm quản trị máy chủ từ các mạng bên ngoài; thực hiện gián tiếp thông qua kết nối mạng riêng ảo hoặc các phương thức khác tương đương;

e) Phân quyền truy nhập, quản trị, sử dụng tài nguyên khác nhau trên máy chủ với người sử dụng/ nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau;

g) Cấp quyền tối thiểu (quyền truy nhập, quản trị) cho tài khoản quản trị máy chủ theo quyền hạn;

h) Kiểm soát truy nhập máy chủ theo khoảng thời gian hợp lệ (theo chính sách của tổ chức nếu có).

**9.1.2.3 Nhật ký hệ thống (G5)**

Yêu cầu bao gồm:

a) Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau:

- Thông tin kết nối mạng tới máy chủ (Firewall log),

- Thông tin trạng thái hoạt động của máy chủ (CPU, RAM, Network…),

- Thông tin các lỗi phát sinh trong quá trình hoạt động,

- Thông tin đăng nhập và truy nhập tài nguyên trên máy chủ,

- Thông tin quản trị, thay đổi cấu hình trên máy chủ (thời gian, địa chỉ, tài khoản truy nhập và thao tác trên máy chủ và các thông tin quản trị khác cần ghi nhật ký (nếu có),

- Các thông tin khác cần ghi nhật ký theo yêu cầu thực tế (nếu có);

b) Đồng bộ thời gian giữa máy chủ với máy chủ thời gian của hệ thống;

c) Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống để không mất hoặc tràn nhật ký hệ thống;

d) Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý nhật ký hệ thống tập trung, gửi dữ liệu nhật ký hệ thống về hệ thống trung tâm theo thời gian thực;

đ) Lưu dữ liệu nhật ký hệ thống trên hệ thống lưu trữ riêng biệt; lưu trữ có mã hóa đối với dữ liệu nhật ký hệ thống của máy chủ quan trọng;

e) Phân quyền truy nhập chỉ cho phép tài khoản quản trị cao nhất hoặc tài khoảng có chức năng quản lý nhật ký hệ thống có quyền truy nhập quản lý dữ liệu nhật ký hệ thống;

g) Thiết lập hệ thống quản lý tài khoản đặc quyền để ghi nhật ký hệ thống việc truy nhập và quản trị máy chủ;

h) Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 12 tháng.

#### 9.1.2.4 Phòng chống xâm nhập (G5)

Yêu cầu bao gồm:

a) Loại bỏ các tài khoản không sử dụng và các tài khoản không còn hợp lệ trên máy chủ;

b) Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng;

c) Sử dụng tường lửa của hệ điều hành máy chủ để cấm các truy nhập trái phép tới máy chủ;

d) Có cơ chế cập nhật và xử lý bản vá, điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ từ hệ thống quản lý tập trung;

đ) Thực hiện nâng cấp, xử lý điểm yếu, lỗ hổng bảo mật trên máy chủ trước khi đưa vào sử dụng;

e) Thực hiện cấu hình tối ưu, tăng cường bảo mật cho máy chủ trước khi đưa vào sử dụng;

g) Cài đặt phần mềm phòng chống xâm nhập cho máy chủ (Host based IDS) và kiểm tra tính toàn vẹn của các tệp tin hệ thống.

#### 9.1.2.5 Phòng chống phần mềm độc hại (G5)

Yêu cầu bao gồm:

a) Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm;

b) Có phương án kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt lên máy chủ;

c) Quản lý tập trung (cập nhật, cảnh báo và quản lý) các phần mềm phòng chống mã độc trên máy chủ và các máy tính người sử dụng trong hệ thống;

d) Có cơ chế kiểm tra, xử lý mã độc của các phương tiện lưu trữ di động (USB, đĩa flash…) trước khi kết nối với máy chủ;

đ) Thiết lập hệ thống có chức theo dõi, giám sát và cảnh báo thời gian thực các tiến trình mới xuất hiện, các tệp tin hệ thống bị thay đổi trên máy chủ.

#### 9.1.2.6 Xử lý máy chủ khi chuyển giao (S5)

Khi chuyển giao hoặc thay đổi mục đích sử dụng cần thực hiện:

a) Sao lưu, dự phòng thông tin, dữ liệu trên máy chủ, ảnh của hệ điều hành máy chủ;

b) Xóa toàn bộ dữ liệu lưu trữ trên máy chủ và xóa hệ điều hành máy chủ;

c) Sử dụng các biên pháp kỹ thuật để bảo đảm dữ liệu không thể khôi phục sau khi xóa.

### 9.1.3 Bảo đảm an toàn ứng dụng

#### 9.1.3.1 Xác thực (S5)

Yêu cầu bao gồm:

a) Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi quản trị, cấu hình cấu hình ứng dụng và sử dụng ứng dụng (nếu ứng dụng cần quản lý truy nhập);

b) Thiết lập chính sách an toàn mật khẩu cho máy chủ bao gồm các yêu cầu cơ bản sau:

- Yêu cầu thay đổi mật khẩu mặc định,

- Thiết lập thời gian yêu cầu thay đổi mật khẩu,

- Thiết lập thời gian mật khẩu hợp lệ,

- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự;

c) Vô hiệu hóa hoặc thay đổi các thông tin các tài khoản mặc định (nếu có);

d) Lưu trữ mã hóa thông tin xác thực trên hệ thống;

đ) Mã hóa thông tin xác thực trước khi gửi qua môi trường mạng;

e) Thiết lập cấu hình ứng dụng để ngăn cản việc đăng nhập tự động;

g) Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định;

h) Vô hiệu hóa tài khoản nếu đăng nhập sai nhiều lần vượt số lần quy định;

i) Thông tin xác thực yêu cầu cần thay đổi định kỳ 03 tháng/lần;

k) Áp dụng giải pháp xác thực mạnh và quản lý tập trung thông tin xác thực trên hệ thống.

**9.1.3.2 Kiểm soát truy nhập (S5)**

Yêu cầu bao gồm:

a) Thiết lập hệ thống chỉ cho phép sử dụng các giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản trị ứng dụng từ xa thông qua môi trường mạng;

b) Thiết lập hệ thống cấm truy nhập trực vào trang quản trị, cổng quản trị ứng dụng từ các mạng bên ngoài mà cần thực hiện gián tiếp bằng cách sử dụng mạng riêng ảo hoặc các phương thức khác tương đương;

c) Giới hạn địa chỉ IP quản trị được phép truy nhập, quản trị ứng dụng từ xa;

d) Thay đổi, tách biệt cổng kết nối quản trị ứng dụng với cổng cung cấp dịch vụ ứng dụng;

đ) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng;

e) Phân quyền truy nhập, quản trị, sử dụng tài nguyên khác nhau của ứng dụng với người sử dụng/ nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau;

g) Cấp quyền tối thiểu (quyền truy nhập, quản trị) cho tài khoản quản trị ứng dụng theo quyền hạn;

h) Thiết lập quyền tối thiểu (chỉ cấp quyền truy cập cơ sở dữ liệu) cho tài khoản kết nối cơ sở dữ liệu;

k) Giới hạn số lượng các kết nối đồng thời (kết nối khởi tạo và đã thiết lập) đối với các ứng dụng, dịch vụ máy chủ cung cấp;

l) Khóa tạm thời hoặc không cho truy nhập quản trị ứng dụng trong khoảng thời gian ngoài giờ làm việc.

**9.1.3.3 Nhật ký hệ thống (G5)**

Yêu cầu bao gồm:

a) Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau:

- Thông tin thông tin thời gian, địa chỉ, tài khoản (nếu có), nội dung truy nhập và sử dụng ứng dụng ứng dụng,

- Thông tin các lỗi phát sinh trong quá trình hoạt động,

- Thông tin quản trị, thay đổi cấu hình ứng dụng,

b) Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý nhật ký hệ thống tập trung, gửi dữ liệu nhật ký hệ thống về hệ thống trung tâm theo thời gian thực;

c) Lưu dữ liệu nhật ký hệ thống trên hệ thống lưu trữ riêng biệt; lưu trữ có mã hóa đối với dữ liệu nhật ký hệ thống của máy chủ quan trọng;

d) Phân quyền truy nhập chỉ cho phép tài khoản quản trị cao nhất hoặc tài khoảng có chức năng quản lý nhật ký hệ thống có quyền truy nhập quản lý dữ liệu nhật ký hệ thống;

đ) Thiết lập hệ thống quản lý tài khoản đặc quyền để ghi nhật ký hệ thống việc truy nhập và quản trị ứng dụng;

e) Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 12 tháng.

**9.1.3.4 Bảo mật thông tin liên lạc (S5)**

Yêu cầu bao gồm:

a) 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) Sử dụng giao thức mạng có chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương;

c) Sử dụng kết hợp các giao thức với phương pháp mã hóa dữ liệu để tạo thành 02 lớp bảo vệ dữ liệu 2 khi truyền qua môi trường mạng;

d) Sử dụng kênh vật lý riêng khi khi truyền đưa, trao đổi qua môi trường mạng đối với dữ liệu quan trọng;

đ) Sử dụng kênh mã hóa vật lý chuyên dụng đối với những loại dữ liệu đặc biết quan trọng.

#### 9.1.3.5 Chống chối bỏ (G5)

Yêu cầu bao gồm:

a) Cung cấp chức năng chức thực, xác minh thông tin, nguồn gửi thông tin khi trao đổi thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) qua môi trường mạng;

b) Áp dụng cơ chế xác thực hai chiều khi trao đổi dữ liệu quan trọng qua môi trường mạng;

c) Sử dụng thiết bị lưu trữ chuyên dụng để lưu trữ thông tin xác thực.

### 9.1.4 An toàn dữ liệu

#### 9.1.4.1 Nguyên vẹn dữ liệu (S5)

Yêu cầu bao gồm:

a) Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống bảo đảm tính nguyên vẹn;

b) Có phương án giám sát, cảnh báo khi có thay đổi thông tin, dữ liệu lưu trên hệ thống lưu trữ/phương tiện lưu trữ.

#### 9.1.4.2 Bảo mật dữ liệu (S5)

Yêu cầu bao gồm:

a) Lưu trữ có mã hóa các thông tin, dữ liệu không công khai trên hệ thống lưu trữ/phương tiện lưu trữ;

b) Thiết lập phân vùng lưu trữ mã hóa, chỉ cho phép người có quyền, trách nhiệm truy nhập, lưu trữ dữ liệu trên phân vùng mã hóa.

c) Phân quyền quản lý thông tin mã hóa dữ liệu (phương pháp, công cụ và mật khẩu mã hóa);

#### 9.1.4.3 Sao lưu dự phòng (A5)

a) Thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, sơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ;

b) Phân loại và quản lý các dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau;

c) Có hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng;

d) Sử dụng cơ chế tự động sao lưu dự phòng đối với thông tin/dữ liệu thay đổi thường xuyên hoặc cập nhật bản sao lưu dự phòng khi thay đổi;

đ) Sử dụng hệ thông sao lưu dự phòng hỗ trợ chức năng dự phòng dự phòng nóng (online), dự phòng nguội (offline) và các chức năng dự phòng khác (theo yêu cầu thực tế);

e) Sử dụng hệ thông sao lưu dự phòng có khả năng chịu lỗi, cho phép khôi phục dữ liệu nóng khi một thành phần trong hệ thống xảy ra sự cố;

g) Lưu trữ dự phòng các dữ liệu quan trọng trên hệ thống/phương tiện lưu trữ dự phòng ở vị trí vật lý khác nhau; bảo đảm môi trường bảo quản và phương pháp quản lý giống như với hệ thống chính;

h) Duy trì ít nhất 02 kết nối mạng từ hệ thống sao lưu dự phòng chính với hệ thống sao lưu dự phòng phụ.

## 9.2 Yêu cầu quản lý

### 9.2.1 Chính sách an toàn thông tin

#### 9.2.1.1. Chính sách an toàn thông tin

Bao gồm các yêu cầu sau:

a) Xác định các mục tiêu, nguyên tắc bảo đảm an toàn thông tin;

b) Xác định trách nhiệm của đơn vị quản lý an toàn thông tin, các thành viên trong ban quản lý an toàn thông tin và các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin;

c) Xác định phạm vi quản lý an toàn bao gồm các nội dung cơ bản sau:

- Phạm vi quản lý về vật lý và logic của tổ chức;

- Các loại tài sản (tài liệu, dữ liệu, thiết bị, con người…);

- Các ứng dụng, dịch vụ hệ thống cung cấp;

- Nguồn nhân lực bảo đảm an toàn thông tin (Cấp Lãnh đạo, cán bộ quản lý, cán bộ kỹ thuật, nhân viên…);

d) Xây dựng chính sách an toàn thông tin cơ bản cho người sử dụng bao gồm:

- Truy nhập, sử dụng tài nguyên trên nội bộ

- Truy nhập mạng và tài nguyên trên Internet

- Cài đặt và sử dụng máy tính an toàn

- An toàn dữ liệu

- Sử dụng và quản lý tài sản

đ) Xây dựng chính sách an toàn thông tin cho người quản trị bao gồm:

- Quản lý an toàn mạng

- Quản lý an toàn máy chủ và ứng dụng

- Quản lý an toàn dữ liệu

- Quản lý an toàn thiết bị đầu cuối

- Quản lý thiết bị hệ thống

- Quản lý giám sát an toàn thông tin

- Quản lý phòng chống phần mềm độc hại

- Quản lý điểm yếu an toàn thông tin

- Quản lý sự cố an toàn thông tin

- Quản lý phương án ứng cứu khẩn cấp

- Quản lý tài sản

- Quản lý thay đổi hệ thống

#### 9.2.1.2 Xây dựng và công bố (G5)

Yêu cầu này bao gồm:

a) Được xây dựng thống nhất và được quản lý theo từng phiên bản;

b) Được thẩm định, thông qua trước khi triển khai áp dụng;

c) Công bố trước 02 tháng khi áp dụng;

d) Tổ chức tuyên truyền, bổ biến cho toàn bộ cán bộ, cán bộ trong tổ chức;

đ) Xin ý kiến thẩm định về mặt chuyên môn, tính hợp pháp của chính sách quản lý an toàn thông tin trước khi công bố và áp dụng;

e) Quy định riêng việc xây dụng, công bố và áp dụng chính sách quản lý an toàn thông tin có tính đặc thù riêng hoặc bí mật.

#### 9.2.1.3. Rà soát, sửa đổi (G5)

Yêu cầu bao gồm:

a) Định kỳ 06 tháng hoặc đột xuất (khi có thay đổi chính sách) kiểm tra lại chính sách quản lý an toàn để tìm ra điểm chưa hợp lý, thiếu sót cần cần chỉnh sửa hoặc bổ sung;

b) Lưu lại lại những thông tin về những trong việc triển khai, áp dụng chính sách quản lý an toàn thông tin, phản hồi của đối tượng áp dụng chính sách.

c) Xin ý kiến thẩm định về mặt chuyên môn, tính hợp pháp của chính sách quản lý an toàn thông tin trước khi công bố và áp dụng.

### 9.2.2 Tổ chức bảo đảm an toàn thông tin

#### 9.2.2.1 Đơn vị quản lý an toàn thông tin (G5)

Yêu cầu bao gồm:

a) Thành lập đơn vị chuyên trách hoặc chỉ định đơn vị (hoặc bộ phần) có trách nhiệm quản lý về an toàn thông tin trong tổ chức (Đơn vị quản lý an toàn thông tin);

b) Phân định vai trò và trò và trách nhiệm, cơ chế phối hợp của các bộ phận, thành viên trong Đơn vị quản lý an toàn thông tin;

c) Chỉ định bộ phận chuyên trách có trách nhiệm xây dựng và quản lý chính sách an toàn thông tin.

d) Chỉ định bộ phận có trách nhiệm thực thi chính sách an toàn thông tin đã xây dựng.

đ) Bố trí cán bộ quản lý ở vị trí quan trọng phải là cán bộ chuyên trách, không được kiêm nhiệm mảng công việc khác;

e) Bố trí tối thiểu 02 cán bộ theo mỗi mảng công việc cần quản lý.

**9.2.2.2 Liên lạc với những cơ quan/tổ chức có thẩm quyền**

Yêu cầu bao gồm:

a) Xác định và lưu thông tin các cơ quan có chức năng quản lý và thực thi công tác bảo đảm an toàn thông tin;

b) Xác định và lưu thông tin các cơ quan trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin;

c) Xây dựng quy chế, thỏa thuận phối hợp giữa tổ chức với các cơ quan chức năng;

đ) Cử đầu mối liên hệ/đại diện tổ chức trong việc tổ chức thực hiện quy chế, thỏa thuận.

**9.2.2.3 Liên lạc với các nhóm chuyên gia**

Yêu cầu bao gồm:

a) Xác định và lưu thông tin các chuyên gia/nhóm chuyên gia trong lĩnh vực an toàn thông tin;

b) Xác định và lưu thông tin cơ quan, tổ chức cung cấp dịch vụ an toàn thông tin;

c) Xây dựng thỏa thuận phối hợp, quy chế làm việc giữa tổ chức với các chuyên gia/nhóm chuyên gia; cơ quan, tổ chức cung cấp dịch vụ an toàn thông tin.

**9.2.3. Bảo đảm nguồn nhân lực**

**9.2.3.1.Trước khi tuyển dụng**

Yêu cầu bao gồm:

a) Có quy định về quy trình tuyển dụng cán bộ; thẩm tra về lý lịch, thân phận của cán bộ được tuyển dụng; có chuyên gia trong lĩnh vực đánh giá, kiểm tra trình độ chuyên môn phù hợp với vị trí tuyển dụng;

b) Các điều khoản và điều kiện tuyển dụng: đưa ra các điều khoản, điều kiện trong hợp đồng với nhân viên và nhà thầu; trách nhiệm của của các bên liên quan trong hợp đồng;

c) Cán bộ được tuyển dụng yêu cầu có trình độ chuyên môn phù hợp với vị trí tuyển dụng, hiểu biết và có kinh nghiệm tối thiểu 03 năm trong lĩnh vực an toàn thông tin;

d) Có bản thỏa thuận riêng và ký xác nhận với cán bộ được tuyển dụng vào các vị trí quan trọng như: quyền, trách nhiệm, phạm vi, thời gian và các thỏa thuận khác liên quan;

đ) Xây dựng quy chế tuyển dụng riêng đối với những vị trì đặc biệt quan trọng hoặc tuyển dụng vào làm việc tại các ngành đặc biệt.

e) Thẩm tra, xác minh lý lịch của ứng viên tuyển dụng, của nhà thầu và bên thứ ba, bảo đảm sự phù hợp với pháp luật, qui định và đạo đức và phù hợp với các yêu cầu của công việc.

**9.2.3.2 Trong quá trình làm việc**

Yêu cầu này bao gồm:

a) Tổ chức đào tạo nâng cao nhận thức về an toàn thông tin và kỹ năng an toàn cơ bản về an toàn thông tin trong quá trình làm việc trước khi làm việc chính thức trong tổ chức;

b) Có kế hoạch và định kỳ 01 năm tổ chức đào tạo về an toàn thông tin hàng năm cho 03 nhóm đối tượng bao gồm: cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống;

c) Có tiêu chí đánh giá kỹ năng, kiến thức chuyên môn, cũng như nhận thức về an toàn thông tin đối với cán bộ ở các vị trí;

đ) Định kỳ 06 tháng tiến hành kiểm tra kỹ năng, kiến thức chuyên môn, cũng như nhận thức về an toàn thông tin đối với cán bộ ở các vị trí;

e) Có bên thứ 3 thực hiện kiểm tra, đánh giá độc lập.

**9.2.3.2 Chấm dứt hoặc thay đổi công việc**

a) Có quy định về quản lý các quy trình, thủ tục cán bộ thôi việc, quy trình nghỉ việc của cán bộ cần tuân thủ theo quy trình, thủ tục đã quy định;

b) Có quy trình vô hiệu hóa tất cả các quyền truy cập thông tin riêng của tổ chức, quyền truy cập, quản trị hệ thống sau khi có cán bộ thôi việc;

c) Có quy trình thu hồi tất cả các văn bản, giấy tờ, các thẻ tín dụng, các thẻ truy cập, thông tin được lưu trên các phương tiện điện tử; các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác của tổ chức do cán bộ quản lý và sử dụng;

d) Cán bộ nghỉ việc phải có đơn và thông báo trước 06 tháng;

đ) Có cam kết giữ bí mật thông tin liên quan đến tổ chức đối với cán bộ ở vị trí chủ chốt sau khi nghỉ việc;

e) Có quy chế thôi việc riêng cho những vị trì đặc biệt quan trọng hoặc tuyển dụng vào làm việc tại các ngành đặc biệt như cơ yếu.

### 9.2.4 Quản lý xây dựng hệ thống thông tin

#### 9.2.4.1 Xác định cấp độ an toàn hệ thống thông tin (G5)

Yêu cầu bao gồm:

a) Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin;

b) Có tài liệu mô tả các thành phần của hệ thống thông tin bao gồm: các vùng mạng chức năng; hệ thống thiết bị mạng, thiết bị bảo mật; hệ thống máy chủ hệ thống; hệ thống máy chủ ứng dụng; dịch vụ và các thành phần khác trong hệ thống thông tin;

c) Có tài liệu mô tả loại thông tin các thành phần trong hệ thống thông tin xử lý bao gồm: thông tin công cộng, thông tin riêng, thông tin cá nhân, thông tin bí mật nhà nước và các loại thông tin khác (nếu có);

d) Có tài liệu mô tả loại hệ thống thông tin căn cứ theo chức năng phục vụ hoạt động nghiệp vụ bao gồm: hệ thống thông tin phục vụ hoạt động nội bộ, hệ thống thông tin phục vụ người dân, doanh nghiệp, hệ thống cơ sở hạ tầng thông tin, hệ thống thông tin điều khiển công nghiệp, hệ thống thông tin khác (nếu có);

đ) Có tài liệu mô tả, giải thích tính phù hợp của cấp độ đề xuất;

e) Có ý kiến thẩm định của đơn vị chuyên môn trước khi phê duyệt cấp độ;

g) Định kỳ 01 năm xác định lại cấp độ an toàn hệ thống thông tin hoặc khi có thay đổi, nâng cấp, mở rộng hệ thống.

#### 9.2.4.2 Thiết kế an toàn hệ thống thông tin (G5)

Yêu cầu bao gồm:

a) Có tài liệu mô tả thiết kế mô tả những thông tin sau:

- Thiết kế vật lý hệ thống thông tin (thiết bị, kết nối vật lý)

- Thiết kế logic hệ thống thông tin (các phân vùng mạng, chức năng);

- Ứng dụng, dịch vụ hệ thống (DNS, DHCP, NTP…)

- Ứng dụng, dịch vụ phục vụ hoạt động nghiệp vụ

b) Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ

c) Có tài liệu thiết kế phương án bảo đảm an toàn thông tin theo yêu cầu thiết kế hệ thống;

d) Có bộ phận chuyên môn, tổ chuyên gia đánh giá, thẩm định hồ sơ thiết kế hệ thống thông tin, các biện pháp bảo đảm an toàn thông tin trước khi triển khai thực hiện;

đ) Định kỳ 06 tháng kiểm tra tính hợp lý trong thiết kế và các biện pháp bảo đảm an toàn thông tin cho hệ thống hoặc khi mở rộng, nâng cấp hệ thống thông tin.

#### 9.2.4.3 Phát triển phần mềm thuê khoán

Yêu cầu bao gồm:

a) Có tài liệu mô tả các chức năng, yêu cầu an toàn phần mềm cần đáp ứng;

b) Có tài liệu mô tả phương án, thiết kế, mô tả khả năng đáp ứng các yêu cầu đặt ra;

c) Phần mềm cần đáp ứng các tiêu chuẩn, quy chuẩn kỹ thuật theo quy định (nếu có);

d) Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm; thực hiện kiểm tra, đánh giá an toàn thông tin cho phần mềm trước khi sử dụng;

đ) Kiểm thử phần mềm trên môi trường thử nghiệm và được nghiệm thu trước 03 tháng trước khi đưa vào sử dụng;

e) Có bên thứ 3 thực hiện kiểm tra, đánh giá độc lập an toàn thông tin cho phần mềm;

g) Có cam kết của bên phát triển về bảo đảm tính bí mật và độc quyền của phần mềm phát triển.

#### 9.2.4.4 Thử nghiệm và bàn giao hệ thống

Yêu cầu bao gồm:

a) Có nội dung, kế hoạch thử nghiệm và nghiệm thu hệ thống;

b) Có bộ phận có trách nhiệm thực hiện nghiệm thu và kiểm thử hệ thống;

c) Có đơn vị độc lập (bên thứ 3) tư vấn và giám sát quá trình thực nghiệm và kiểm thử hệ thống;

đ) Có báo cáo nghiệm thu được thẩm định và xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng;

e) Có xác nhận của cơ quan chức năng về hợp chuẩn, hợp quy của hệ thống thông tin trước khi đưa vào sử dụng;

g) Thực hiện thử nghiệm và nghiệm thu hệ thống trước 01 tháng trước khi bàn giao và đưa vào sử dụng.

#### 9.2.4.5 Các mối liên hệ với bên cung cấp dịch vụ an toàn thông tin

Yêu cầu bao gồm:

a) Có quy định về các yêu cầu, các thỏa thuận, quyền hạn và trách nhiệm của bên cung cấp;

b) Có quy trình ký kết, thực hiện, duy trì và thay đổi các cam kết trong hợp đồng đối với các bên cung cấp;

c) Có thỏa thuận và cam kết trách nhiệm của mỗi bên trước khi được ký kết hợp đồng;

d) Bên cung cấp dịch vụ an toàn thông tin được cơ quan có thẩm quyền cấp phép;

đ) Bên cung cấp dịch vụ an toàn thông tin được cơ quan có thẩm quyền chỉ định.

### 9.2.5 Quản lý vận hành hệ thống

#### 9.2.5.1 Quản lý an toàn mạng

Yêu cầu bao gồm:

a) Xây dựng chính sách quản lý an toàn mạng, bao gồm các yêu cầu cơ bản sau:

- Chính sách kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng

- Chính sách quản lý kiểm soát truy nhập đi vào và từ hệ thống đi ra

- Chính sách truy nhập và quản lý cấu hình hệ thống

- Chính sách bảo đảm an toàn dữ liệu qua môi trường mạng

- Chính sách sao lưu và dự phòng và khôi phục cấu hình hệ thống

- Chính sách ghi nhật ký hệ thống và giám sát an toàn thông tin

b) Xây dựng quy trình quản lý, vận hành hoạt động bình thường của hệ thống;

c) Xây dựng quy trình cập nhật; sao lưu, dự phòng các tệp tin cấu hình hệ thống và quy trình khôi phục hệ thống sau khi xảy ra sự cố;

d) Xây dựng quy trình cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác;

đ) Xây dựng quy trình kiểm tra, đánh giá an toàn thông tin; xử lý điểm yếu, lỗ hổng bảo mật cho các thiết bị mạng, bảo mật; định kỳ 01 tháng (hoặc đột xuất khi cần thiết) thực hiện quy trình.

e) Xây dựng quy trình kết nối và gửi nhật ký hệ thống từ thiết bị mạng, bảo mật, thiết bị đầu cuối và các thiết bị khác trong hệ thống về hệ thống giám sát.

#### 9.2.5.2 Quản lý an toàn máy chủ và ứng dụng

Yêu cầu bao gồm:

a) Xây dựng chính sách quản lý an toàn máy chủ và ứng dụng, bao gồm các yêu cầu cơ bản sau:

- Chính sách về quản lý và sử dụng máy chủ và ứng dụng an toàn,

- Chính sách truy nhập và quản trị máy chủ và ứng dụng,

- Chính sách truy nhập mạng,

- Chính sách bảo đảm an toàn dữ liệu qua môi trường mạng,

- Chính sách sao lưu và dự phòng và khôi phục cấu hình hệ thống,

- Chính sách ghi nhật ký hệ thống và giám sát an toàn thông tin;

b) Xây dựng quy trình quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ;

c) Xây dựng quy trình cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng;

d) Xây dựng quy trình kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống;

đ) Xây dựng quy trình cập nhật; sao lưu, dự phòng các tệp tin cấu hình hệ thống, tệp tin dự phòng hệ điều hành và các dữ liệu quan trọng khác và quy trình khôi phục sau khi xảy ra sự cố;

e) Xây dựng quy trình cấu hình tối tưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ và dịch vụ và thực hiện quy trình trước khi đưa hệ thống vào sử dụng;

h) Xây dựng quy trình kiểm tra, đánh giá an toàn thông tin xử lý điểm yếu, lỗ hổng bảo mật cho hệ thống máy chủ và dịch vụ, bảo mật;

i) Xây dựng quy trình kết nối và gửi nhật ký hệ thống từ hệ điều hành, ứng dụng, dịch vụ về hệ thống giám sát.

**9.2.5.3 Quản lý an toàn dữ liệu**

Yêu cầu bao gồm:

a) Xây dựng chính sách quản lý an toàn dữ liệu, bao gồm các yêu cầu cơ bản sau:

- Yêu cầu an toàn đối với phương pháp mã hóa;

- Quản lý và sử dụng khóa bí mật;

- Phân loại, quản lý dữ liệu bí mật;

- Cơ chế mã hóa và kiểm tra tính toàn vẹn của dữ liệu;

- Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ;

- Sao lưu, dự phòng và phôi phục dữ liệu (tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ).

b) Xây dựng danh sách thông tin, tệp tin và dữ liệu, phần mềm và các tài nguyên khác trên hệ thống cần dự phòng;

c) Xây dựng quy trình sao lưu dự phòng, định kỳ 01 tuần (hoặc khi có thay đổi trên hệ thống cần sao lưu dự phòng) thực hiện quy trình sao lưu dự phòng;

d) Xây dựng quy trình khôi phục dữ liệu dự phòng;

đ) Xây dựng quy trình kiểm tra, vận hành và bảo trì hệ thống sao lưu dự phòng.

**9.2.5.4 Quản lý an toàn thiết bị đầu cuối**

Yêu cầu bao gồm:

a) Xây dựng chính sách quản lý an toàn thiết bị đầu cuối, bao gồm các yêu cầu cơ bản sau:

- Chính sách về quản lý và sử dụng các thiết bị đầu cuối an toàn;

- Chính sách kết nối thiết bị đầu cuối vào hệ thống;

- Chính sách kết nối, truy nhập và sử dụng thiết bị đầu cuối từ xa;

- Chính sách bảo đảm an toàn vật lý cho thiết bị đầu cuối;

b) Xây dựng quy trình quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối;

c) Xây dựng quy trình cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối vào hệ thống;

d) Xây dựng quy trình cấu hình tối tưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng;

đ) Xây dựng quy trình kiểm tra, đánh giá an toàn thông tin xử lý điểm yếu, lỗ hổng bảo mật cho thiết bị đầu cuối.

**9.2.5.5 Quản lý thiết bị hệ thống**

Yêu cầu bao gồm:

a) Xây dựng chính sách truy nhập, quản lý và cấu hình thiết bị;

b) Quy định về các điều kiện bảo đảm an toàn vật lý cho thiết bị;

c) Xây dựng quy trình lắp đặt, cài đặt kết nối và gỡ bỏ thiết bị khỏi hệ thống;

d) Xây dựng quy trình quản lý, vận hành khai thác hoạt động bình thường của thiết bị;

đ) Xây dựng quy trình bảo dưỡng, bảo trì thiết bị;

e) Xây dựng hướng dẫn cách sử dụng, quản lý, vận hành thiết bị các thiết bị đầu cuối và các thiết bị dự phòng;

g) Chỉ định bộ phận có trách nhiệm quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị và thiết bị dự phòng).

**9.2.5.6 Quản lý phòng chống phần mềm độc hại**

Yêu cầu bao gồm:

a) Xây dựng quy định cho người sử dụng về việc cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng;

b) Xây dựng quy định về việc gửi nhận tệp tin từ môi trường mạng và qua các phương tiện lưu trữ di động;

d) Xây dựng quy định, quy trình về việc cài đặt, cập nhật và sử dụng phần mềm diệt virus; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động;

đ) Định kỳ 01 tháng (hoặc khi phát hiện hoạt động không bình thường của hệ thống) thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống.

**9.2.5.7 Quản lý giám sát an toàn thông tin**

Yêu cầu bao gồm:

a) Xây dựng chích sách giám sát an toàn thông tin bao gồm các yêu cầu cơ bản sau:

- Chính sách truy nhập và quản lý hệ thống giám sát;

- Quy định về việc kết nối; gửi dữ liệu từ các thiết bị được giám sát về hệ thống giám sát;

- Quy định về những loại thông tin cần được giám sát;

- Quy định về việc lưu trữ và bảo đảm an toàn thông tin giám sát (nhật ký hệ thống);

- Quy định về việc đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát.

b) Xây dựng quy trình, quy định việc kết nối đối tượng giám vào hệ thống giám sát;

c) Xây dựng quy trình quản lý vận hành hệ thống giám sát, hệ thống tập trung (nếu có);

d) Xây dựng quy trình theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin;

đ) Chỉ định bộ phận có trách nhiệm giám sát hệ thống thông tin.

**9.2.5.8 Quản lý điểm yếu an toàn thông tin**

Yêu cầu bao gồm:

a) Xây dựng danh mục, phiên bản, chức năng cho các thành phần có trong hệ thống (thiết bị mạng, bảo mật; hệ điều hành; máy chủ; ứng dụng, dịch vụ và các thành phần khác trong hệ thống có thể tồn tại điểm yếu an toàn thông tin và các thông tin);

b) Xây dựng danh sách nguồn cung cấp điểm yếu an toàn thông tin; phân nhóm và mức độ của điểm yếu cho các thành phần trong hệ thống đã xác định;

c) Xây dựng danh sách đầu mối các nhóm chuyên ra, bên cung cấp dịch vụ hỗ trợ, cung cấp dịch vụ xử lý, khắc phục điểm yếu an toàn thông tin;

d) Có quy định về việc cập nhật thông tin, cơ chế cảnh báo các điểm yếu an toàn thông tin cho các bộ phận có trách nhiệm tương ứng;

đ) Xây dựng quy trình, phương án xử lý, khắc phục điểm yếu an toàn thông tin theo các nhóm hạ tầng mạng; hệ điều hành; ứng dụng và dịch vụ và các nhóm khác nếu cần quản lý;

e) Xây dựng các phương án xử lý tạm thời khi điểm yếu an toàn thông tin không/chưa có khả năng xử lý;

g) Xây dựng quy trình khôi phục lại hệ thống sau khi xử lý điểm yếu an toàn thông tin thất bại;

h) Chỉ định bộ phận có trách nhiệm quản lý điểm yếu an toàn thông tin.

**9.2.5.9 Quản lý sự cố an toàn thông tin**

Yêu cầu bao gồm:

a) Xây dựng danh sách, tiêu chí và phân loại các sự cố an toàn thông tin theo các nhóm sự cố: sự cố an toàn vật lý, sự cố an toàn mạng, sự cố an toàn máy chủ, sự cố an toàn dịch vụ;

b) Xây dựng danh sách đầu mối các nhóm chuyên ra, bên cung cấp dịch vụ hỗ trợ, cung cấp dịch vụ xử lý, khắc phục sự cố an toàn thông tin;

c) Xây dựng phương án khắc phục, xử lý các loại sự cố an toàn thông tin tương ứng;

đ) Xây dựng quy trình phát hiện và cảnh báo sự cố an toàn thông tin;

e) Xây dựng quy trình khắc phục, xử lý sự cố an toàn thông tin bao gồm: tiếp nhận sự cố, xác minh/xác nhận sự cố, phân loại sự cố, báo cáo sự cố, thu thập thông tin để phục vụ phân tích sự cố, phân tích sự cố; xử lý sự cố, tổng hợp báo cáo, lưu hồ sơ sự cố;

g) Xây dựng quy trình điều tra, phân tích và thu thập chứng cứ;

h) Quy định về việc lưu hồ sơ quá trình xử lý, tổng kết bài học kinh nghiệm; đưa ra biện pháp ngăn chặn sự cố tái phát sinh; cần lưu hồ sơ toàn quá trình thực hiện;

i) Xây dựng quy trình riêng đối với những sự cố nghiêm trọng cần xử lý đặc biệt (ví dụ: sự cố gây gián đoạn hoạt động toàn hệ thống hoặc lộ lọt thông tin bí mật..) và chỉ định bộ phận chuyên trách thực hiện;

k) Xây dựng phương án báo cáo cơ quan chức năng (theo các quy định của nhà nước) trong trường hợp cần hỗ trợ điều phối, xử lý;

l) Chỉ định bộ phận chó trách nhiệm quản lý và thực thi xử lý sự cố an toàn thông tin.

**9.2.5.10 Quản lý phương án ứng cứu khẩn cấp**

Yêu cầu bao gồm:

a) Xác định, xây dựng tiêu chí phân loại sự cố an toàn thông tin cần xử lý theo phương án ứng cứu khẩn cấp;

b) Chỉ định và phân trách nhiệm cho bộ phận và thành phần tham gia phương án ứng cứu khẩn cấp;

c) Quy định về phương án phân bổ tài nguyên (con người, tài chính, phương tiện, biện pháp kỹ thuật…) cho phương án ứng cứu khẩn cấp;

d) Xây dựng phương án ứng cứu khẩn cấp theo từng cấp độ ứng cứu khẩn cấp;

đ) Xây dựng quy trình thực hiện phương án ứng cứu khẩn cấp;

e) Định kỳ hàng năm, tổ chức đào tạo, nâng cao kỹ năng cho cán bộ chuyên trách có trách nhiệm thực hiện phương án ứng cứu khẩn cấp;

g) Định kỳ hàng năm tổ chức diễn tập phương án ứng cứu khẩn cấp;

h) Định kỳ (hoặc đột xuất theo yêu cầu thực tế) kiểm tra, rà soát và cập nhật phương án ứng cứu khẩn cấp cho phù hợp với yêu cầu và tình hình thực tế.

**9.2.5.11 Quản lý tài sản**

Yêu cầu bao gồm:

a) Xây dựng danh mục và phân loại tài sản, bao gồm các yêu cầu cơ bản sau:

- Mỗi tài sản cần có tài liệu bao gồm các thông tin cơ bản như: loại tài sản, người quản lý, vị trí, mức độ quan trọng của tài sản và trách nhiệm tương ứng;

- Phân loại tài sản căn cứ vào mức độ quan trọng của tài sản tiến hành quản lý theo phân loại tài sản, căn cứ vào giá trị, mức độ quan trọng của tài sản lựa chọn phương thức quản lý tương ứng;

- Phân loại tài sản thông tin căn cứ theo giá trị, mức độ quan trọng bao gồm các loại thông tin sau: thông tin công cộng, thông tin riêng, thông tin cá nhân, thông tin bí mật nhà nước và các loại thông tin khác (nếu có);

- Gắn nhãn thông tin căn cứ vào các loại thông tin hệ thống xử lý được xác định ở trên, mỗi loại thông tin cần gán nhãn tương ứng với loại thông tin đó. Việc gán nhãn thông tin có thể thực hiện bằng cách mỗ tả loại thông tin và lưu hồ sơ mô tả các loại thông tin đó.

b) Xây dựng chính sách quản lý và sử dụng tài sản trong tổ chức bao gồm các yêu cầu cơ bản sau:

- Bàn giao và thu hồi tài sản;

- Quy định về quản lý, bảo quản và sử dụng;

- Quy định các điều kiển bảo đảm an toàn cho tài sản trong quá trình sử dụng và bảo quản;

- Quy định về việc di dời; lăp đặt, sửa chữa, bảo trì, bảo dưỡng;

- Quy định về thanh lý và hủy bỏ tài sản.

c) Quản lý phương tiện lưu trữ bao gồm các yêu cầu cơ bản sau:

- Quy định về việc sửa chữa, tiêu hủy phương tiện lưu trữ như: cần tiến hành mã hóa nội dung phương tiện lưu trữ đưa ra khỏi môi trường làm việc; đối với phương tiện lưu trữ đưa ra sửa chữa hoặc tiêu hủy cần làm sạch dữ liệu nhạy cảm, bí mật trong đó; đối với phương tiện không thể làm sạch dữ liệu bắt buộc phải tiêu hủy thì cần được phê duyệt của bộ phận quản lý và có sự giám sát của bộ phận quản lý;

- Đối với dữ liệu nhạy cảm, bí mật cần được mã hóa trước khi lưu trữ; phân loại và quản lý các dữ liệu được lưu trữ theo từng loại thông tin khác nhau;

- Quy định riêng về việc lưu trữ, mã hóa, sử dụng và quản lý phương tiện lưu trữ đối với phương tiện lưu trữ những dữ liệu đặc biệt quan trọng.

đ) Chỉ định bộ phận có trách nhiệm quản lý tài sản; có chính sách, quy định về việc quản lý và sử dụng tài sản.

**9.2.5.12 Quản lý thay đổi hệ thống**

Yêu cầu bao gồm:

a) Xây dựng quy trình quản lý thay đổi quy trình nghiệp vụ; thay đổi tổ chức, cán bộ liên quan đến hoạt động bảo đảm an toàn thông tin của tổ chức;

b) Xây dựng quy trình quản lý thay đổi hạ tầng vật lý: bổ sung, gỡ bỏ, di chuyển, thay đổi chức năng của thiết bị phụ trợ trong hệ thống;

c) Xây dựng quy trình quản lý thay đổi hạ tầng mạng: bổ sung hoặc gỡ bỏ kết nối mạng; cấu hình trên thiết bị mạng, bảo mật, bổ sung hoặc gỡ bỏ thiết bị khỏi hệ thống mạng…;

d) Xây dựng quy trình quản lý thay đổi trên ứng dụng và dịch vụ: cài đặt hoặc gỡ bỏ dịch vụ, phần mềm; kết nối mạng; chính sách truy nhập…;

đ) Xây dựng quy trình khôi phục lại hệ thống sau khi thay đổi (trong trường hợp thay đổi xảy ra sự cố hoặc không hợp lý);

e) Xây dựng quy trình thay đổi trong trường hợp hệ thống cần thay đổi khẩn cấp.