TCVN TIÊU CHUẨN QUỐC GIA

TCVN 11930:2017

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

Information technology.Security techniques - Basic requirements for securing information system according to security levels

HÀ NỘI - 2017

Mục lục

Lời giới thiệu 6

1 Phạm vi áp dụng 9

2 Tài liệu viện dẫn 9

3 Thuật ngữ và định nghĩa 9

4 Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ 15

5 Yêu cầu cơ bản cho hệ thống thông tin cấp độ 1 15

5.1 Yêu cầu quản lý 15

5.1.1 Thiết lập chính sách an toàn thông tin 15

5.1.2 Tổ chức bảo đảm an toàn thông tin 15

5.1.3 Bảo đảm nguồn nhân lực 16

5.1.4 Quản lý thiết kế, xây dựng hệ thống 16

5.1.5 Quản lý vận hành hệ thống 16

5.2 Yêu cầu kỹ thuật 17

5.2.1 Bảo đảm an toàn mạng 17

5.2.2 Bảo đảm an toàn máy chủ 17

5.2.3 Bảo đảm an toàn ứng dụng 18

5.2.4 Bảo đảm an toàn dữ liệu 19

6 Yêu cầu cơ bản cho hệ thống thông tin cấp độ 2 19

6.1 Yêu cầu quản lý 19

6.1.1 Thiết lập chính sách an toàn thông tin 19

6.1.2 Tổ chức bảo đảm an toàn thông tin 19

6.1.3 Bảo đảm nguồn nhân lực 20

6.1.4 Quản lý thiết kế, xây dựng hệ thống 20

6.1.5 Quản lý vận hành hệ thống 21

6.2 Yêu cầu kỹ thuật 22

6.2.1 Bảo đảm an toàn mạng 22

6.2.2 Bảo đảm an toàn máy chủ 23

6.2.3 Bảo đảm an toàn ứng dụng 24

6.2.4 Bảo đảm an toàn dữ liệu 25

7 Yêu cầu cơ bản cho hệ thống thông tin cấp độ 3 25
7.1 Yêu cầu quản lý 25
7.1.1 Thiết lập chính sách an toàn thông tin 25
7.1.2 Tổ chức bảo đảm an toàn thông tin 26
7.1.3 Bảo đảm nguồn nhân lực 27
7.1.4 Quản lý thiết kế, xây dựng hệ thống 27
7.1.5 Quản lý vận hành hệ thống 28
7.2 Yêu cầu kỹ thuật 31
7.2.1 Bảo đảm an toàn mạng 31
7.2.2 Bảo đảm an toàn máy chủ 33
7.2.3 Bảo đảm an toàn ứng dụng 35
7.2.4 Bảo đảm an toàn dữ liệu 36
8 Yêu cầu cơ bản cho hệ thống thông tin cấp độ 4 37
8.1 Yêu cầu quản lý 37
8.1.1 Thiết lập chính sách an toàn thông tin 37
8.1.2 Tổ chức bảo đảm an toàn thông tin 38
8.1.3 Bảo đảm nguồn nhân lực 38
8.1.4 Quản lý thiết kế, xây dựng hệ thống 39
8.1.5 Quản lý vận hành hệ thống 40
8.2 Yêu cầu kỹ thuật 43
8.2.1 Bảo đảm an toàn mạng 43
8.2.2 Bảo đảm an toàn máy chủ 46
8.2.3 Bảo đảm an toàn ứng dụng 48
8.2.4 Bảo đảm an toàn dữ liệu 50
9 Yêu cầu cơ bản cho hệ thống thông tin cấp độ 5 51
9.1 Yêu cầu quản lý 51
9.1.1 Thiết lập chính sách an toàn thông tin 51
9.1.2 Tổ chức bảo đảm an toàn thông tin 52
9.1.3 Bảo đảm nguồn nhân lực 52

9.1.4 Quản lý thiết kế, xây dựng hệ thống 53
9.1.5 Quản lý vận hành hệ thống 54
9.2 Yêu cầu kỹ thuật 57
9.2.1 Bảo đảm an toàn mạng 57
9.2.2 Bảo đảm an toàn máy chủ 61
9.2.3 Bảo đảm an toàn ứng dụng 63
9.2.4 Bảo đảm an toàn dữ liệu 65
Phụ lục A (Quy định): Yêu cầu cơ bản về an toàn vật lý cho hệ thống thông tin theo cấp độ 67

Lời nói đầu

TCVN 11930:2017 được xây dựng trên cơ sở tham khảo Tiêu chuẩn quốc tế ISO/IEC 27001:2013 và Tiêu chuẩn SP 800-53 phiên bản 4.0 của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) Mỹ, có điều chỉnh, sửa đổi, bổ sung để phù hợp với điều kiện của Việt Nam.

TCVN 11930:2017 do Cục An toàn thông tin biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Tiêu chuẩn này quy định các yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ, bao gồm hai nhóm: yêu cầu quản lý và yêu cầu kỹ thuật. Nhóm các yêu cầu quản lý là cơ sở để cơ quan, tổ chức xây dựng chính sách, quy trình quản lý an toàn thông tin cho hệ thống của mình trong quá trình thiết kế, xây dựng, vận hành, khai thác, sử dụng. Nhóm yêu cầu kỹ thuật là cơ sở để cơ quan, tổ chức thiết kế, thiết lập cấu hình hệ thống trong quá trình xây dựng hệ thống thông tin.

Cơ quan, tổ chức sau khi xác định cấp độ an toàn hệ thống thông tin và phương án bảo đảm an toàn hệ thống thông tin, có thể triển khai các biện pháp bảo đảm an toàn thông tin, đáp ứng các yêu cầu cơ bản nêu tại Tiêu chuẩn này, nhằm bảo đảm an toàn hệ thống thông tin ở mức độ cơ bản theo cấp độ tương ứng.

Để bảo đảm an toàn hệ thống thông tin ở mức độ cao hơn, phù hợp với yêu cầu thực tế và đặc thù của hệ thống thông tin của cơ quan, tổ chức cần tiến hành đánh giá rủi ro an toàn hệ thống thông tin để xác định và triển khai các biện pháp bảo đảm an toàn thông tin bổ sung.

Khuyến khích cơ quan, tổ chức triển khai các biện pháp bảo đảm an toàn thông tin đáp ứng toàn bộ các yêu cầu an toàn cơ bản cho cấp độ đã xác định và bổ sung thêm các yêu cầu an toàn ở cấp độ cao hơn nhằm tăng cường bảo đảm an toàn thông tin cho hệ thống thông tin của mình.

Để hướng dẫn cơ quan, tổ chức xác định các yêu cầu cơ bản về an toàn vật lý, Phụ lục A, tiêu chuẩn này đưa ra các yêu cầu cơ bản về an toàn vật lý cho hệ thống thông tin theo từng cấp độ. Cơ quan, tổ chức có thể áp dụng để có phương án bảo đảm an toàn vật lý cơ bản cho hệ thống thông tin của mình.

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

Information technology - Security techniques - Basic requirements for securing information system according to security levels

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

Yêu cầu an toàn cơ bản quy định trong tiêu chuẩn này tập trung vào các yêu cầu bảo đảm an toàn hệ thống thông tin. Các yêu cầu khác về an toàn thông tin, không liên quan trực tiếp đến bảo đảm an toàn hệ thống thông tin (ví dụ: bảo vệ thông tin cá nhân, bảo vệ trẻ em trên mạng...) không thuộc phạm vi của Tiêu chuẩn này.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau là cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi (nếu có).

ISO/IEC 27001:2013 Information Technology – Security techniques – Information security management system – Requirements *(Công nghệ thông tin – Các kỹ thuật an toàn – Hệ thống quản lý an toàn thông tin – Các yêu cầu)*

SP 800-53 R4, Security and Privacy Controls for Federal Information Systems and Organizations *(Biện pháp kiểm soát bảo mật và riêng tư cho các Hệ thống thông tin liên bang và Tổ chức).*

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong các tiêu chuẩn ISO/IEC 27001:2013, SP 800-53 R4 và các thuật ngữ, định nghĩa sau:

3.1

An toàn dữ liệu (data security)

Tập hợp các biện pháp quản lý và kỹ thuật nhằm bảo đảm tính bí mật, tính nguyên vẹn và khả dụng của thông tin, dữ liệu khi lưu trữ, xử lý, truy cập và trao đổi dữ liệu qua môi trường mạng.

3.2

An toàn mạng (network security)

Tập hợp các biện pháp quản lý và kỹ thuật nhằm bảo đảm việc thiết lập, quản lý, vận hành hạ tầng mạng (bao gồm kênh kết nối, thiết bị mạng, thiết bị bảo mật, thiết bị phụ trợ và các thành phần khác nếu có) bảo đảm an toàn.

3.3

An toàn mạng không dây (wireless network security)

Tập hợp các biện pháp quản lý và kỹ thuật nhằm bảo đảm việc kết nối, truy cập và trao đổi thông tin sử dụng mạng không dây bảo đảm an toàn.

3.4

An toàn máy chủ (server security)

Tập hợp các biện pháp quản lý và kỹ thuật nhằm bảo đảm an toàn cho máy chủ trong quá trình thiết lập, quản lý, vận hành và gỡ bỏ.

3.5

An toàn thông tin/An toàn thông tin mạng (information security)

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

3.6

An toàn ứng dụng (application security)

Tập hợp các biện pháp quản lý và kỹ thuật nhằm bảo đảm các ứng dụng, dịch vụ cung cấp bởi hệ thống bảo đảm an toàn trong quá trình thiết lập, quản lý, vận hành.

3.7

Chính sách an toàn thông tin (information security policy)

Tập các 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.

3.8

Chống thất thoát dữ liệu (data leak prevention)

Giải pháp giúp cơ quan, tổ chức bảo vệ dữ liệu quan trọng của mình tránh việc bị đánh cắp, rò rỉ hoặc khi dữ liệu bị vô ý mất mát, thất lạc thì bên thứ ba không thể khai thác dữ liệu đó trái phép.

3.9

Điểm yếu an toàn thông tin (information security vulnerability)

Lỗi tồn tại trên sản phẩm phần cứng, phần mềm, dịch vụ hoặc hệ thống trong quá trình phát triển, cài đặt và thiết lập, có thể gây ra nguy cơ mất an toàn cho hệ thống thông tin khi bị tin tặc khai thác.

3.10

Dữ liệu quan trọng (important data)

Dữ liệu trong hệ thống, được cơ quan, tổ chức xác định là quan trọng, cần được ưu tiên bảo vệ. Dữ liệu quan trọng bao gồm, nhưng không giới hạn các loại dữ liệu chứa các thông tin sau: thông tin nghiệp vụ, thông tin bí mật nhà nước, thông tin riêng và các loại thông tin quan trọng khác (nếu có).

3.11

Dự phòng nóng (hot standby)

Khả năng thay thế chức năng của thiết bị khi xảy ra sự cố mà không làm gián đoạn hoạt động của hệ thống.

3.12

Giám sát an toàn hệ thống thông tin (information system security monitoring)

Hoạt động lựa chọn đối tượng, công cụ giám sát, thu thập, phân tích thông tin trạng thái của đối tượng giám sát, báo cáo, cảnh báo hành vi xâm phạm an toàn thông tin hoặc có khả năng gây ra sự cố an toàn thông tin đối với hệ thống thông tin.

3.13

Giám sát hệ thống thông tin (information system monitoring)

Biện pháp giám sát, theo dõi trạng thái hoạt động của hệ thống để phát hiện, cảnh báo sớm các sự cố có thể gây gián đoạn hoạt động của hệ thống và làm mất tính khả dụng của hệ thống thông tin.

3.14

Hệ thống lọc phần mềm độc hại (malware filter system)

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

3.15

Hệ thống thông tin (information system)

Tập hợp 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 trên mạng.

3.16

Hệ thống thông tin cấp độ 1 (information system level 1)

Hệ thống thông tin mà khi bị phá hoại sẽ làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân nhưng không làm tổn hại tới lợi ích công cộng, trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia.

3.17

Hệ thống thông tin cấp độ 2 (information system level 2)

Hệ thống thông tin mà khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng nhưng không làm tổn hại tới trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia.

3.18

Hệ thống thông tin cấp độ 3 (information system level 3)

Hệ thống thông tin mà khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia.

3.19

Hệ thống thông tin cấp độ 4 (information system level 4)

Hệ thống thông tin mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia.

3.20

Hệ thống thông tin cấp độ 5 (information system level 5)

Hệ thống thông tin mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia.

3.21

Kết nối mạng an toàn (secure network connection)

Việc thiết lập, sử dụng các giao thức mạng có hỗ trợ các tính năng bảo mật (mã hóa, xác thực) nhằm bảo đảm việc trao đổi thông tin qua môi trường mạng an toàn. Ví dụ một số giao thức: SSH, SSL/TLS, VPN hoặc các giao thức tương đương khác.

3.22

Nhật ký hệ thống (system log)

Những sự kiện được hệ thống ghi lại liên quan đến trạng thái hoạt động, sự cố, sự kiện an toàn thông tin và các thông tin khác liên quan đến hoạt động của hệ thống (nếu có).

3.23

Phần mềm độc hại (malware)

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.

3.24

Phần mềm phòng chống mã độc (anti-malware software)

Phần mềm có chức năng phát hiện, cảnh báo và xử lý phần mềm độc hại.

3.25

Phần mềm thuê khoán (outsource software)

Phần mềm được phát triển, nâng cấp, chỉnh sửa theo các yêu cầu riêng của tổ chức hoặc người sử dụng nhằm đáp ứng yêu cầu đặc thù của tổ chức.

3.26

Phương tiện lưu trữ (media storage)

Các thiết bị, phương tiện được sử dụng để lưu trữ, sao chép, trao đổi thông tin giữa các thiết bị, máy tính một cách gián tiếp.

3.27

Quản lý tài khoản đặc quyền (privileged identity management - PIM)

Biện pháp quản lý tập trung các tài khoản có quyền quản trị cao nhất (có đầy đủ các quyền hệ thống cung cấp) trên hệ thống.

3.28

Sự cố an toàn thông tin/Sự cố (information security incident)

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

3.29

Thiết bị mạng chính (core network device)

Thiết bị gây gián đoạn hoạt động của toàn bộ hệ thống khi xảy ra sự cố. Ví dụ: thiết bị chuyển mạch trung tâm, thiết bị định tuyến biên, tường lửa trung tâm và các thiết bị khác có chức năng và vị trí tương đương.

3.30

Tính bảo mật (confidentiality)

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

3.31

Tính khả dụng (availability)

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

3.32

Tính nguyên vẹn (integrity)

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

3.33

Vùng mạng biên (outside zone)

Vùng mạng được thiết lập để cung cấp các kết nối hệ thống ra bên ngoài Internet và các mạng khác.

3.34

Vùng DMZ (demilitarized zone)

Vùng mạng được thiết lập để đặt các máy chủ công cộng, cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng Internet.

3.35

Vùng máy chủ nội bộ (internal server zone)

Vùng mạng được thiết lập để đặt các máy chủ nội bộ, cung cấp các ứng dụng, dịch vụ phục vụ hoạt động nội bộ của tổ chức và các hoạt động khác mà không cho phép truy cập trực tiếp từ các mạng bên ngoài.

3.36

Vùng mạng nội bộ (LAN - local area network)

Vùng mạng này được thiết lập để cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối và các thiết bị khác của người sử dụng vào hệ thống.

3.37

Vùng quản trị (management zone)

Vùng mạng được thiết lập để đặt các máy chủ, máy quản trị và các thiết bị chuyên dụng khác phục vụ việc quản lý, vận hành và giám sát hệ thống.

3.38

Vùng quản trị thiết bị hệ thống (device management zone)

Vùng mạng riêng cho các địa chỉ quản trị của các thiết bị hệ thống cho phép thiết lập chính sách chung và quản lý tập trung các thiết bị hệ thống.

3.39

Vùng máy chủ cơ sở dữ liệu (database server zone)

Vùng mạng được thiết lập để đặt các máy chủ cơ sở dữ liệu. Các máy chủ trong vùng này được triển khai tách biệt với các máy chủ ứng dụng nhằm tăng cường các biện kiểm soát truy cập giữa các vùng máy chủ khác với vùng máy chủ này.

3.40

Xác thực đa nhân tố (multi-factor authentication)

Phương pháp xác thực không chỉ dựa vào một mà là kết hợp một số yếu tố liên quan đến người dùng, bao gồm: những thông tin mà người dùng biết (mật khẩu, mã số truy cập...), những thông tin mà người dùng sở hữu (chứng thư số, thẻ thông minh...) hoặc những thông tin về sinh trắc học của người dùng (vân tay, mống mắt...).

4 Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ

Các yêu cầu của từng cấp độ được chia làm hai nhóm: yêu cầu quản lý và yêu cầu kỹ thuật.

Yêu cầu quản lý đưa ra các yêu cầu về mặt quản lý nhằm quản lý việc xây dựng, quản lý vận hành và gỡ bỏ hệ thống thông tin bảo đảm an toàn. Các yêu cầu quản lý được chia thành các nhóm yêu cầu: thiết lập chính sách an toàn thông tin; tổ chức bảo đảm an toàn thông tin; bảo đảm nguồn nhân lực; quản lý thiết kế, xây dựng hệ thống; quản lý vận hành hệ thống.

Yêu cầu kỹ thuật đưa ra các yêu cầu về mặt kỹ thuật để bảo đảm việc thiết kế, xây dựng và thiết lập hệ thống thông tin bảo đảm an toàn. Các yêu cầu kỹ thuật được chia thành các nhóm yêu cầu: bảo đảm an toàn mạng; bảo đảm an toàn máy chủ; bảo đảm an toàn ứng dụng; bảo đảm an toàn dữ liệu.

5 Yêu cầu cơ bản cho hệ thống thông tin cấp độ 1

5.1 Yêu cầu quản lý

5.1.1 Thiết lập chính sách an toàn thông tin

5.1.1.1 Chính sách an toàn thông tin

Xây dựng chính sách, quy trình quản lý, vận hành hoạt động bình thường của hệ thống nhằm bảo đảm tính sẵn sàng của hệ thống trong quá trình vận hành, khai thác.

5.1.1.2 Xây dựng và công bố

Chính sách được tổ chức/bộ phận được ủy quyền thông qua trước khi công bố áp dụng.

5.1.1.3 Rà soát, sửa đổi

Định kỳ 03 năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.

5.1.2 Tổ chức bảo đảm an toàn thông tin

5.1.2.1 Đơn vị chuyên trách về an toàn thông tin

Có cán bộ có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin.

5.1.2.2 Phối hợp với cơ quan/tổ chức có thẩm quyền

a) Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin;

b) Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin.

5.1.3 Bảo đảm nguồn nhân lực

5.1.3.1 Tuyển dụng

Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành phù hợp với vị trí tuyển dụng.

5.1.3.2 Trong quá trình làm việc

a) Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống;

b) Có hình thức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng.

5.1.3.3 Chấm dứt hoặc thay đổi công việc

Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức.

5.1.4 Quản lý thiết kế, xây dựng hệ thống

5.1.4.1 Thiết kế an toàn hệ thống thông tin

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 thiết kế và các thành phần của hệ thống thông tin.

5.1.4.2 Thử nghiệm và nghiệm thu hệ thống

Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng.

5.1.5 Quản lý vận hành hệ thống

5.1.5.1 Quản lý an toàn mạng

Xây dựng và thực thi chính sách, quy trình quản lý vận hành hoạt động bình thường của hạ tầng mạng.

5.1.5.2 Quản lý an toàn máy chủ và ứng dụng

Xây dựng và thực thi chính sách, quy trình quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ.

5.1.5.3 Quản lý an toàn dữ liệu

Có phương án sao lưu dự phòng thông tin, dữ liệu, cấu hình hệ thống.

5.2 Yêu cầu kỹ thuật

5.2.1 Bảo đảm an toàn mạng

5.2.1.1 Thiết kế hệ thống

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

- Vùng mạng nội bộ;

- Vùng mạng biên;

- Vùng DMZ.

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

- Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn;

- Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập.

5.2.1.2 Kiểm soát truy cập từ bên ngoài mạng

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet;

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

5.2.1.3 Nhật kí hệ thống

Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị mạng chính.

5.2.1.4 Phòng chống xâm nhập

a) Có phương án phòng chống xâm nhập để bảo vệ vùng DMZ;

b) Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng (Signatures).

5.2.1.5 Bảo vệ thiết bị hệ thống

a) Cấu hình chức năng xác thực trên các thiết bị hệ thống (nếu hỗ trợ) để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa;

b) Thiết lập cấu hình chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa.

5.2.2 Bảo đảm an toàn máy chủ

5.2.2.1 Xác thực

a) Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng khi truy cập, 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);

c) Thiết lập cấu hình máy chủ để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:

- Yêu cầu thay đổi mật khẩu mặc định;

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

5.2.2.2 Kiểm soát truy cập

Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa.

5.2.2.3 Nhật ký hệ thống

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;

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

5.2.2.4 Phòng chống xâm nhập

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

b) Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ.

5.2.2.5 Phòng chống phần mềm độc hại

Cài đặt phần mềm phòng chống mã độc (hoặc có phương án khác tương đương) và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm.

5.2.3 Bảo đảm an toàn ứng dụng

5.2.3.1 Xác thực

a) Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng;

b) Lưu trữ có mã hóa thông tin xác thực hệ thống;

c) Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:

- Yêu cầu thay đổi mật khẩu mặc định;

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

5.2.3.2 Kiểm soát truy cập

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa;

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

5.2.3.3 Nhật kí hệ thống

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

- Thông tin truy cập ứng dụng;

- Thông tin đăng nhập khi quản trị ứng dụng.

5.2.4 Bảo đảm an toàn dữ liệu

5.2.4.1 Sao lưu dự phòng

Thực hiện sao lưu dự phòng các thông tin, dữ liệu quan trọng trên hệ thống.

6 Yêu cầu cơ bản cho hệ thống thông tin cấp độ 2

6.1 Yêu cầu quản lý

6.1.1 Thiết lập chính sách an toàn thông tin

6.1.1.1 Chính sách an toàn thông tin

Xây dựng chính sách an toàn thông tin, 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 người sử dụng đầu cuối.

6.1.1.2 Xây dựng và công bố

Chính sách được tổ chức/bộ phận được ủy quyền thông qua trước khi công bố áp dụng;

6.1.1.3 Rà soát, sửa đổi

Định kỳ 03 năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.

6.1.2 Tổ chức bảo đảm an toàn thông tin

6.1.2.1 Đơn vị chuyên trách về an toàn thông tin

Có bộ phận có trách nhiệm bảo đảm an toàn thông tin cho tổ chức.

6.1.2.2 Phối hợp với cơ quan/tổ chức có thẩm quyền

a) Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin;

b) Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin;

c) Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

6.1.3 Bảo đảm nguồn nhân lực

6.1.3.1 Tuyển dụng

Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành phù hợp với vị trí tuyển dụng.

6.1.3.2 Trong quá trình làm việc

a) Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống;

b) Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng.

6.1.3.3 Chấm dứt hoặc thay đổi công việc

a) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức;

b) Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

6.1.4 Quản lý thiết kế, xây dựng hệ thống

6.1.4.1 Thiết kế an toàn hệ thống thông tin

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 thiết kế và các thành phần của hệ thống thông tin;

c) Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ;

d) Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin;

đ) Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

6.1.4.2 Phát triển phần mềm thuê khoán

a) Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán;

b) Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm.

6.1.4.3 Thử nghiệm và nghiệm thu hệ thống

a) Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng;

b) Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống;

c) Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống.

6.1.5 Quản lý vận hành hệ thống

6.1.5.1 Quản lý an toàn mạng

Chính sách, quy trình quản lý an toàn mạng bao gồm:

a) Quản lý, vận hành hoạt động bình thường của hệ thống;

b) Cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố;

c) Truy cập và quản lý cấu hình hệ thống.

6.1.5.2 Quản lý an toàn máy chủ và ứng dụng

Chính sách, quy trình quản lý an toàn máy chủ và ứng dụng bao gồm:

a) Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ;

b) Truy cập mạng của máy chủ;

c) Truy cập và quản trị máy chủ và ứng dụng;

d) Cập nhật; sao lưu dự phòng và khôi phục sau khi xảy ra sự cố.

6.1.5.3 Quản lý an toàn dữ liệu

Chính sách, quy trình quản lý an toàn dữ liệu bao gồm:

a) Chính sách, quy trình dự phòng và khôi phục dữ liệu;

b) Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

6.1.6.4 Quản lý sự cố an toàn thông tin

Chính sách, quy trình quản lý sự cố an toàn thông tin bao gồm:

a) Phân nhóm sự cố an toàn thông tin mạng;

b) Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng;

c) Kế hoạch ứng phó sự cố an toàn thông tin mạng;

d) Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin;

đ) Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường;

e) Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng;

g) Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin.

6.1.5.5 Quản lý an toàn người sử dụng đầu cuối

Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:

a) Quản lý truy cập, sử dụng tài nguyên nội bộ;

b) Quản lý truy cập mạng và tài nguyên trên Internet.

6.2 Yêu cầu kỹ thuật

6.2.1 Bảo đảm an toàn mạng

6.2.1.1 Thiết kế hệ thống

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

- Vùng mạng nội bộ;

- Vùng mạng biên;

- Vùng DMZ;

- Vùng máy chủ nội bộ;

- Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác.

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

- Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn;

- Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập;

- Có phương án dự phòng cho các thiết bị mạng chính.

6.2.1.2 Kiểm soát truy cập từ bên ngoài mạng

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet;

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

6.2.1.3 Kiểm soát truy cập từ bên trong mạng

Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài theo yêu cầu nghiệp vụ, chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức.

6.2.1.4 Nhật ký hệ thống

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

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

6.2.1.5 Phòng chống xâm nhập

a) Có phương án phòng chống xâm nhập để bảo vệ vùng DMZ và vùng máy chủ nội bộ;

b) Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng (Signatures).

6.2.1.6 Bảo vệ thiết bị hệ thống

a) Cấu hình chức năng xác thực trên các thiết bị hệ thống (nếu hỗ trợ) để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa;

b) Thiết lập cấu hình chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa;

c) Cấu hình thiết bị (nếu hỗ trợ) chỉ cho phép hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa.

6.2.2 Bảo đảm an toàn máy chủ

6.2.2.1 Xác thực

a) Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng khi truy cập, 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);

c) Thiết lập cấu hình máy chủ để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:

- Yêu cầu thay đổi mật khẩu mặc định;

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

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

- Thiết lập thời gian mật khẩu hợp lệ.

6.2.2.2 Kiểm soát truy cập

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa;

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.

6.2.2.3 Nhật ký hệ thống

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;

- Thông tin thay đổi cấu hình máy chủ;

- Thông tin truy cập dữ liệu và dịch vụ quan trọng trên máy chủ (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.

6.2.2.4 Phòng chống xâm nhập

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

b) Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ;

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

d) Có phương án cập nhật bản vá, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ.

6.2.2.5 Phòng chống phần mềm độc hại

a) Cài đặt phần mềm phòng chống mã độc (hoặc có phương án khác tương đương) 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.

6.2.2.6 Xử lý máy chủ khi chuyển giao

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

6.2.3 Bảo đảm an toàn ứng dụng

6.2.3.1 Xác thực

a) Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng;

b) Lưu trữ có mã hóa thông tin xác thực hệ thống;

c) Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:

- Yêu cầu thay đổi mật khẩu mặc định;

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

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

- Thiết lập thời gian mật khẩu hợp lệ.

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

6.2.3.2 Kiểm soát truy cập

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa;

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

c) Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa.

6.2.3.3 Nhật ký hệ thống

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

- Thông tin truy cập ứng dụng;

- Thông tin đăng nhập khi quản trị ứng dụng;

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

- Thông tin thay đổi cấu hình ứng dụng;

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

6.2.3.4 An toàn ứng dụng và mã nguồn

Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý.

6.2.4 Bảo đảm an toàn dữ liệu

6.2.4.1 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.

6.2.4.2 Sao lưu dự phòng

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

7 Yêu cầu cơ bản cho hệ thống thông tin cấp độ 3

7.1 Yêu cầu quản lý

7.1.1 Thiết lập chính sách an toàn thông tin

7.1.1.1 Chính sách an toàn thông tin

Xây dựng chính sách an toàn thông tin, bao gồm:

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

b) Xác định trách nhiệm của đơn vị chuyên trách về an toàn thông tin, các cán bộ làm về 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 chính sách an toàn thông tin bao gồm:

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

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

- Nguồn nhân lực bảo đảm an toàn thông tin.

d) Xây dựng chính sách an toàn thông tin 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;

- Quản lý giám sát an toàn hệ thống thông tin;

- Quản lý an toàn người sử dụng đầu cuối.

7.1.1.2 Xây dựng và công bố

a) Chính sách được tổ chức/bộ phận được ủy quyền thông qua trước khi công bố áp dụng;

b) Chính sách được công bố trước khi áp dụng.

7.1.1.3 Rà soát, sửa đổi

Định kỳ 02 năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.

7.1.2 Tổ chức bảo đảm an toàn thông tin

7.1.2.1 Đơn vị chuyên trách về an toàn thông tin

a) Thành lập hoặc chỉ định đơn vị/bộ phận chuyên trách về an toàn thông tin trong tổ chức;

b) Phân định vai trò, trách nhiệm, cơ chế phối hợp của các bộ phận, cán bộ trong đơn vị chuyên trách về an toàn thông tin.

7.1.2.2 Phối hợp với những cơ quan/tổ chức có thẩm quyền

a) Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin;

b) Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin;

c) Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

7.1.3 Bảo đảm nguồn nhân lực

7.1.3.1 Tuyển dụng

a) Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng;

b) Có quy định, quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ.

7.1.3.2 Trong quá trình làm việc

a) Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống;

b) Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng;

c) Định kỳ hàng năm, tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin cho người sử dụng.

7.1.3.3 Chấm dứt hoặc thay đổi công việc

a) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức;

b) Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc;

c) Có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

7.1.4 Quản lý thiết kế, xây dựng hệ thống

7.1.4.1 Thiết kế an toàn hệ thống thông tin

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 thiết kế và các thành phần của hệ thống thông tin;

c) Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ;

d) Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin;

đ) Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

7.1.4.2 Phát triển phần mềm thuê khoán

a) Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán;

b) Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm;

c) Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng;

d) Kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.

7.1.4.3 Thử nghiệm và nghiệm thu hệ thống

a) Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng;

b) Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống;

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

d) Có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống;

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

7.1.5 Quản lý vận hành hệ thống

7.1.5.1 Quản lý an toàn mạng

Chính sách, quy trình quản lý an toàn mạng bao gồm:

a) Quản lý, vận hành hoạt động bình thường của hệ thống;

b) Cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố;

c) Truy cập và quản lý cấu hình hệ thống;

d) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

7.1.5.2 Quản lý an toàn máy chủ và ứng dụng

Chính sách, quy trình quản lý an toàn máy chủ và ứng dụng bao gồm:

a) Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ;

b) Truy cập mạng của máy chủ;

c) Truy cập và quản trị máy chủ và ứng dụng;

d) Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố;

đ) Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng;

e) Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống;

g) Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

7.1.5.3 Quản lý an toàn dữ liệu

Chính sách, quy trình quản lý an toàn dữ liệu bao gồm:

a) Xây dựng và thực thi chính sách, quy trình dự phòng và khôi phục dữ liệu;

c) Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

7.1.5.4 Quản lý an toàn thiết bị đầu cuối

Chính sách, quy trình quản lý thiết bị đầu cuối bao gồm:

a) Quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối;

b) Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa;

c) Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống.

7.1.5.5 Quản lý phòng chống phần mềm độc hại

Chính sách, quy trình quản lý phần mềm độc hại bao gồm:

a) Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động;

b) Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng;

c) Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động;

d) Định kỳ thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

7.1.5.6 Quản lý giám sát an toàn hệ thống thông tin

Chính sách, quy trình quản lý giám sát an toàn hệ thống thông tin bao gồm:

a) Quản lý, vận hành hoạt động bình thường của hệ thống giám sát;

b) Đối tượng giám sát bao gồm: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống (nếu có);

c) Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát;

d) Truy cập và quản trị hệ thống giám sát;

đ) Loại thông tin cần được giám sát;

e) Lưu trữ và bảo vệ thông tin giám sát (nhật ký hệ thống);

g) Đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát;

h) Theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin.

7.1.5.7 Quản lý điểm yếu an toàn thông tin

Chính sách, quy trình quản lý điểm yếu an toàn thông tin bao gồm:

a) Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin: thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác (nếu có);

b) Quản lý, cập nhật 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) Cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin;

d) Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng;

đ) Định kỳ kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.

7.1.5.8 Quản lý sự cố an toàn thông tin

Chính sách, quy trình quản lý sự cố an toàn thông tin bao gồm:

a) Phân nhóm sự cố an toàn thông tin mạng;

b) Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng;

c) Kế hoạch ứng phó sự cố an toàn thông tin mạng;

d) Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin;

đ) Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường;

e) Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng;

g) Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin;

h) Định kỳ tổ chức diễn tập phương án xử lý sự cố an toàn thông tin.

7.1.5.9 Quản lý an toàn người sử dụng đầu cuối

Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:

a) Quản lý truy cập, sử dụng tài nguyên nội bộ;

b) Quản lý truy cập mạng và tài nguyên trên Internet;

c) Cài đặt và sử dụng máy tính an toàn.

7.2 Yêu cầu kỹ thuật

7.2.1 Bảo đảm an toàn mạng

7.2.1.1 Thiết kế hệ thống

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

- Vùng mạng nội bộ;

- Vùng mạng biên;

- Vùng DMZ;

- Vùng máy chủ nội bộ;

- Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác;

- Vùng mạng máy chủ cơ sở dữ liệu;

- Vùng quản trị;

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

- Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn;

- Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập;

- Có phương án cân bằng tải và dự phòng nóng cho các thiết bị mạng chính;

- Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu;

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

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

- Có phương án giám sát hệ thống thông tin tập trung;

- Có phương án giám sát an toàn hệ thống thông tin tập trung;

- Có phương án quản lý sao lưu dự phòng tập trung;

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

- Có phương án phòng, chống thất thoát dữ liệu;

- Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ;

- Có phương án bảo đảm an toàn cho mạng không dây (nếu có).

7.2.1.2 Kiểm soát truy cập từ bên ngoài mạng

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet;

b) Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập 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 cập từ bên ngoài vào hệ thống 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 được hệ thống cung cấp theo năng lực thực tế của hệ thống.

7.2.1.3 Kiểm soát truy cập từ bên trong mạng

a) Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài theo yêu cầu nghiệp vụ, chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức;

b) Giới hạn truy cập các ứng dụng, dịch vụ bên ngoài theo thời gian (theo chính sách truy cập của tổ chức nếu có);

c) Có phương án kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ theo chức năng và chính sách của tổ chức.

7.2.1.4 Nhật ký hệ thống

a) Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống (nếu hỗ trợ), bao gồm các thông tin sau:

- 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;

- Thông tin hiệu năng hoạt động của thiết bị và tài nguyên mạng.

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 tham gia hoạt động giám sát;

c) Lưu trữ và quản lý tập trung nhật ký hệ thống thu thập được từ các thiết bị hệ thống;

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

7.2.1.5 Phòng chống xâm nhập

a) Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống;

b) Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng (Signatures);

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

7.2.1.6 Phòng chống phần mềm độc hại trên môi trường mạng

a) Có phương án phòng chống phần mềm độc hại trên môi trường mạng;

b) Định kỳ cập nhật dữ liệu cho hệ thống phòng chống phần mềm độc hại;

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

7.2.1.7 Bảo vệ thiết bị hệ thống

a) Cấu hình chức năng xác thực trên các thiết bị hệ thống (nếu hỗ trợ) để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa;

b) Thiết lập cấu hình chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa;

c) Cấu hình thiết bị (nếu hỗ trợ) chỉ cho phép hạn chế các địa chỉ mạng có thể 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 mạng;

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

e) Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng;

g) Xóa bỏ thông tin cấu hình, dữ liệu trên thiết bị hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ khỏi hệ thống.

7.2.2 Bảo đảm an toàn máy chủ

7.2.2.1 Xác thực

a) Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng khi truy cập, 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);

c) Thiết lập cấu hình máy chủ để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:

- Yêu cầu thay đổi mật khẩu mặc định;

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

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

- Thiết lập thời gian mật khẩu hợp lệ.

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.

7.2.2.2 Kiểm soát truy cập

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa;

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;

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

d) Giới hạn địa chỉ mạng được phép truy cập, quản trị máy chủ từ xa.

7.2.2.3 Nhật ký hệ thống

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;

- Thông tin thay đổi cấu hình máy chủ;

- Thông tin truy cập dữ liệu và dịch vụ quan trọng trên máy chủ (nếu có).

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

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 tập trung nhật ký hệ thống thu thập được từ máy chủ;

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

7.2.2.4 Phòng chống xâm nhập

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

b) Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ;

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

d) Có phương án cập nhật bản vá, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ;

đ) Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng.

7.2.2.5 Phòng chống phần mềm độc hại

a) Cài đặt phần mềm phòng chống mã độc (hoặc có phương án khác tương đương) 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;

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

7.2.2.6 Xử lý máy chủ khi chuyển giao

a) Có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng;

b) Sao lưu dự phòng thông tin, dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành;

c) Có biện pháp kiểm tra, bảo đảm dữ liệu không thể khôi phục sau khi xóa.

7.2.3 Bảo đảm an toàn ứng dụng

7.2.3.1 Xác thực

a) Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng;

b) Lưu trữ có mã hóa thông tin xác thực hệ thống;

c) Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:

- Yêu cầu thay đổi mật khẩu mặc định;

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

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

- Thiết lập thời gian mật khẩu hợp lệ.

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

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 đối với các ứng dụng, dịch vụ cung cấp và xử lý dữ liệu quan trọng trong hệ thống.

7.2.3.2 Kiểm soát truy cập

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa;

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

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

d) Phân quyền truy cập, 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;

đ) 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.

7.2.3.3 Nhật ký hệ thống

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

- Thông tin truy cập ứng dụng;

- Thông tin đăng nhập khi quản trị ứng dụng;

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

- Thông tin thay đổi cấu hình ứng dụng.

b) Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung;

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

7.2.3.4 Bảo mật thông tin liên lạc

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; sử dụng phương án mã hóa theo quy định về bảo vệ bí mật nhà nước đối với thông tin mật;

b) Sử dụng kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền.

7.2.3.5 Chống chối bỏ

Sử dụng chữ ký số khi trao đổi thông tin, dữ liệu quan trọng.

7.2.3.6 An toàn ứng dụng và mã nguồn

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

b) Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu;

c) Có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF;

d) Có chức năng kiểm soát lỗi, thông báo lỗi từ ứng dụng.

7.2.4 Bảo đảm an toàn dữ liệu

7.2.4.1 Nguyên vẹn dữ liệu

Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.

7.2.4.2 Bảo mật dữ liệu

a) 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;

b) Sử dụng các phương pháp mã hóa mạnh (chưa được các tổ chức quốc tế công bố điểm yếu an toàn thông tin) để mã hóa dữ liệu.

7.2.4.3 Sao lưu dự phòng

a) Thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ 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 để sao lưu dự phòng.

8 Yêu cầu cơ bản cho hệ thống thông tin cấp độ 4

8.1 Yêu cầu quản lý

8.1.1 Thiết lập chính sách an toàn thông tin

8.1.1.1 Chính sách an toàn thông tin

Xây dựng chính sách an toàn thông tin, bao gồm:

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

b) Xác định trách nhiệm của đơn vị chuyên trách về an toàn thông tin, các cán bộ làm về 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 chính sách an toàn thông tin bao gồm:

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

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

- Nguồn nhân lực bảo đảm an toàn thông tin.

d) Xây dựng chính sách an toàn thông tin 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;

- Quản lý giám sát an toàn hệ thống thông tin;

- Quản lý sự cố an toàn thông tin;

- Quản lý an toàn người sử dụng đầu cuối.

8.1.1.2 Xây dựng và công bố

a) Chính sách được tổ chức/bộ phận được ủy quyền thông qua trước khi công bố áp dụng;

b) Chính sách được công bố trước khi áp dụng;

c) Tổ chức tuyên truyền, phổ biến cho toàn bộ cán bộ trong tổ chức.

8.1.1.3 Rà soát, sửa đổi

a) Định kỳ hàng năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung;

b) Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng chính sách trong quá trình triển khai, áp dụng chính sách an toàn thông tin.

8.1.2 Tổ chức bảo đảm an toàn thông tin

8.1.2.1 Đơn vị chuyên trách về an toàn thông tin

a) Thành lập hoặc chỉ định đơn vị chuyên trách về an toàn thông tin trong tổ chức;

b) Phân định vai trò, trách nhiệm, cơ chế phối hợp của các bộ phận, cán bộ trong đơn vị chuyên trách về an toàn thông tin;

c) Chỉ định bộ phận chuyên trách trong đơn vị chuyên trách về an toàn thông tin có trách nhiệm xây dựng và thực thi chính sách an toàn thông tin.

8.1.2.2 Phối hợp với những cơ quan/tổ chức có thẩm quyền

a) Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin;

b) Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin;

c) Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

8.1.3 Bảo đảm nguồn nhân lực

8.1.3.1 Tuyển dụng

a) Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng;

b) Có quy định, quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ;

c) Có chuyên gia trong lĩnh vực đánh giá, kiểm tra trình độ chuyên môn phù hợp với vị trí tuyển dụng.

8.1.3.2 Trong quá trình làm việc

a) Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống;

b) Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng;

c) Có kế hoạch và định kỳ hàng 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.

8.1.3.2 Chấm dứt hoặc thay đổi công việc

a) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức;

b) Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc;

c) Có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

8.1.4 Quản lý thiết kế, xây dựng hệ thống

8.1.4.1 Thiết kế an toàn hệ thống thông tin

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 thiết kế và các thành phần của hệ thống thông tin;

c) Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ;

d) Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin;

đ) Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống;

e) Có phương án quản lý và bảo vệ hồ sơ thiết kế;

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

8.1.4.2 Phát triển phần mềm thuê khoán

a) Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán;

b) Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm;

c) Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng;

d) Kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng;

đ) Khi thay đổi mã nguồn, kiến trúc phần mềm thực hiện kiểm tra, đánh giá an toàn thông tin cho phần mềm;

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

8.1.4.3 Thử nghiệm và nghiệm thu hệ thống

a) Thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng;

b) Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống;

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

d) Có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống;

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

8.1.5 Quản lý vận hành hệ thống

8.1.5.1 Quản lý an toàn mạng

Chính sách, quy trình quản lý an toàn mạng bao gồm:

a) Quản lý, vận hành hoạt động bình thường của hệ thống;

b) Cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố;

c) Truy cập và quản lý cấu hình hệ thống;

d) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

8.1.5.2 Quản lý an toàn máy chủ và ứng dụng

Chính sách, quy trình quản lý an toàn máy chủ và ứng dụng bao gồm:

a) Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ;

b) Truy cập mạng của máy chủ;

c) Truy cập và quản trị máy chủ và ứng dụng;

d) Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố;

đ) Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng;

e) Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống;

g) Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

8.1.5.3 Quản lý an toàn dữ liệu

Chính sách, quy trình quản lý an toàn dữ liệu bao gồm:

a) Yêu cầu an toàn đối với phương pháp mã hóa;

b) Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa;

c) Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu;

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

đ) Sao lưu dự phòng và khôi 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;

e) Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ;

g) Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống (nếu có).

8.1.5.4 Quản lý an toàn thiết bị đầu cuối

Chính sách, quy trình quản lý thiết bị đầu cuối bao gồm:

a) Quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối;

b) Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa;

c) Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống;

d) Cấu hình tối ưu 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) Kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin cho thiết bị đầu cuối trước khi đưa vào sử dụng.

8.1.5.5 Quản lý phòng chống phần mềm độc hại

Chính sách, quy trình quản lý phần mềm độc hại bao gồm:

a) Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động;

b) Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng;

c) Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động;

d) Định kỳ thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

8.1.5.6 Quản lý giám sát an toàn hệ thống thông tin

Chính sách, quy trình quản lý giám sát an toàn hệ thống thông tin bao gồm:

a) Quản lý, vận hành hoạt động bình thường của hệ thống giám sát;

b) Đối tượng giám sát bao gồm: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống (nếu có);

c) Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát;

d) Truy cập và quản trị hệ thống giám sát;

đ) Loại thông tin cần được giám sát;

e) Lưu trữ và bảo vệ thông tin giám sát (nhật ký hệ thống);

g) Đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát;

h) Theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin;

i) Bố trí nguồn lực và tổ chức giám sát an toàn hệ thống thông tin 24/7.

8.1.5.7 Quản lý điểm yếu an toàn thông tin

Chính sách, quy trình quản lý điểm yếu an toàn thông tin bao gồm:

a) Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin: thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác (nếu có);

b) Quản lý, cập nhật 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) Cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin;

d) Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng;

đ) Định kỳ kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.

8.1.5.8 Quản lý sự cố an toàn thông tin

Chính sách, quy trình quản lý sự cố an toàn thông tin bao gồm:

a) Phân nhóm sự cố an toàn thông tin mạng;

b) Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng;

c) Kế hoạch ứng phó sự cố an toàn thông tin mạng;

d) Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin;

đ) Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường;

e) Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng;

g) Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin;

h) Định kỳ tổ chức diễn tập phương án xử lý sự cố an toàn thông tin.

8.1.5.9 Quản lý an toàn người sử dụng đầu cuối

Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:

a) Quản lý truy cập, sử dụng tài nguyên nội bộ;

b) Quản lý truy cập mạng và tài nguyên trên Internet;

c) Cài đặt và sử dụng máy tính an toàn.

8.2 Yêu cầu kỹ thuật

8.2.1 Bảo đảm an toàn mạng

8.2.1.1 Thiết kế hệ thống

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

- Vùng mạng nội bộ;

- Vùng mạng biên;

- Vùng DMZ;

- Vùng máy chủ nội bộ;

- Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác;

- Vùng mạng máy chủ cơ sở dữ liệu;

- Vùng quản trị;

- Vùng quản trị thiết bị hệ thống.

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

- Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn;

- Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập;

- Có phương án dự phòng cho các thiết bị mạng và phương án cân bằng tải, dự phòng nóng cho thiết bị mạng chính;

- Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu;

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

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

- Có phương án giám sát hệ thống thông tin tập trung;

- Có phương án giám sát an toàn hệ thống thông tin tập trung;

- Có phương án quản lý sao lưu dự phòng tập trung;

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

- Có phương án phòng, chống thất thoát dữ liệu;

- Có phương án duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau (nếu hệ thống buộc phải có kết nối mạng Internet) ;

- Có phương án bảo đảm an toàn cho mạng không dây (nếu có);

- Có phương án quản lý tài khoản đặc quyền.

8.2.1.2 Kiểm soát truy cập từ bên ngoài mạng

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet;

b) Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập 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 cập từ bên ngoài vào hệ thống 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 được hệ thống cung cấp theo năng lực thực tế của hệ thống.

8.2.1.3 Kiểm soát truy cập từ bên trong mạng

a) Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài 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 kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ theo chức năng và chính sách của tổ chức;

c) Không cho phép hoặc giới hạn truy cập (theo chức năng của máy chủ) từ các máy chủ ra các mạng bên ngoài hệ thống;

d) 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.

8.2.1.4 Nhật ký hệ thống

a) Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống (nếu hỗ trợ), bao gồm các thông tin sau:

- 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;

- Thông tin hiệu năng hoạt động của thiết bị và tài nguyên mạng.

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 tham gia hoạt động giám sát;

c) Lưu trữ và quản lý tập trung nhật ký hệ thống thu thập được từ các thiết bị hệ thống;

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 dự phòng dữ liệu nhật ký hệ thống trên hệ thống lưu trữ riêng biệt, có mã hóa với những dữ liệu nhật ký quan trọng (nếu có);

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

8.2.1.5 Phòng chống xâm nhập

a) Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống;

b) Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng (signatures);

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

d) Hệ thống có phương án cân bằng tải và dự phòng nóng.

8.2.1.6 Phòng chống phần mềm độc hại trên môi trường mạng

a) Có phương án phòng chống phần mềm độc hại trên môi trường mạng;

b) Định kỳ cập nhật dữ liệu cho hệ thống phòng chống phần mềm độc hại;

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

d) Hệ thống có phương án cân bằng tải và dự phòng nóng.

8.2.1.7 Bảo vệ thiết bị hệ thống

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

b) Thiết lập cấu hình chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa;

c) Không cho phép quản trị, cấu hình thiết bị trực tiếp từ các mạng bên ngoài, trường hợp bắt buộc phải quản trị thiết bị từ xa phải thực hiện gián tiếp thông qua các máy quản trị trong hệ thống và sử dụng kết nối mạng an toàn;

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

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

e) Nâng cấp, xử lý điểm yếu an toàn thông tin 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) Xóa bỏ thông tin cấu hình, dữ liệu trên thiết bị hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ khỏi hệ thống.

8.2.2 Bảo đảm an toàn máy chủ

8.2.2.1 Xác thực

a) Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng khi truy cập, 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);

c) Thiết lập cấu hình máy chủ để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:

- Yêu cầu thay đổi mật khẩu mặc định;
- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự;
- Thiết lập thời gian yêu cầu thay đổi mật khẩu;
- Thiết lập thời gian mật khẩu hợp lệ.

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) 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);

g) Sử dụng cơ chế xác thực đa nhân tố để xác thực người sử dụng khi truy cập, quản trị vào các máy chủ quan trọng trong hệ thống.

8.2.2.2 Kiểm soát truy cập

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa;

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;

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

d) Không cho phép quản trị, cấu hình máy chủ trực tiếp từ các mạng bên ngoài, trường hợp bắt buộc phải quản trị thiết bị từ xa phải thực hiện gián tiếp thông qua các máy quản trị trong hệ thống và sử dụng kết nối mạng an toàn;

đ) Phân quyền truy cập, 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;

e) Cấp quyền tối thiểu (quyền truy cập, quản trị) cho tài khoản quản trị máy chủ theo quyền hạn.

8.2.2.3 Nhật ký hệ thống

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;

- Thông tin thay đổi cấu hình máy chủ;

- Thông tin truy cập dữ liệu và dịch vụ quan trọng trên máy chủ (nếu có).

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 tập trung nhật ký hệ thống thu thập được từ máy chủ;

đ) Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 06 tháng;

e) Lưu trữ dự phòng dữ liệu nhật ký hệ thống trên hệ thống lưu trữ riêng biệt, có mã hóa với những dữ liệu nhật ký quan trọng (nếu có).

8.2.2.4 Phòng chống xâm nhập

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

b) Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ;

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

d) Có phương án cập nhật bản vá, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ;

đ) Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng;

e) Có biện pháp quản lý tập trung việc 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;

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

8.2.2.5 Phòng chống phần mềm độc hại

a) Cài đặt phần mềm phòng chống mã độc (hoặc có phương án khác tương đương) 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;

c) Quản lý tập trung (cập nhật, cảnh báo và quản lý) các phần mềm phòng chống mã độc cài đặt 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 trước khi kết nối với máy chủ.

8.2.2.6 Xử lý máy chủ khi chuyển giao

a) Có biện pháp chuyên dụng để xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng;

b) Sao lưu dự phòng thông tin, dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành;

c) Có biện pháp kiểm tra, bảo đảm dữ liệu không thể khôi phục sau khi xóa.

8.2.3 Bảo đảm an toàn ứng dụng

8.2.3.1 Xác thực

a) Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng;

b) Lưu trữ có mã hóa thông tin xác thực hệ thống;

c) Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:

- Yêu cầu thay đổi mật khẩu mặc định;

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

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

- Thiết lập thời gian mật khẩu hợp lệ;

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

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 đối với các ứng dụng, dịch vụ cung cấp và xử lý dữ liệu quan trọng trong hệ thống;

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

8.2.3.2 Kiểm soát truy cập

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa;

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

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

d) Phân quyền truy cập, 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;

đ) 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;

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

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

8.2.3.3 Nhật ký hệ thống

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

- Thông tin truy cập ứng dụng;

- Thông tin đăng nhập khi quản trị ứng dụng;

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

- Thông tin thay đổi cấu hình ứng dụng.

b) Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung;

c) Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 06 tháng;

d) Lưu trữ dự phòng dữ liệu nhật ký hệ thống trên hệ thống lưu trữ riêng biệt, có mã hóa với những dữ liệu nhật ký quan trọng (nếu có).

8.2.3.4 Bảo mật thông tin liên lạc

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; sử dụng phương án mã hóa theo quy định về bảo vệ bí mật nhà nước đối với thông tin mật;

b) Sử dụng kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền;

c) Sử dụng kết hợp các kết nối mạng an toàn hoặc biện pháp mã hóa để bảo đảm dữ liệu quan trọng được mã hóa 02 lần khi truyền qua môi trường mạng;

d) Sử dụng kênh vật lý riêng khi truyền đưa, trao đổi qua môi trường mạng đối với dữ liệu quan trọng.

8.2.3.5 Chống chối bỏ

a) Sử dụng chữ ký số khi trao đổi thông tin, dữ liệu quan trọng;

b) Chữ ký số được cung cấp bởi cơ quan có thẩm quyền hoặc đơn vị cung cấp dịch vụ chữ ký số được cấp phép;

c) Có phương án bảo đảm an toàn trong việc quản lý và sử dụng chữ ký số.

8.2.3.6 An toàn ứng dụng và mã nguồn

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

b) Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu;

c) Có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF;

d) Có chức năng kiểm soát lỗi, thông báo lỗi từ ứng dụng;

đ) Không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng;

e) Có chức năng tạo lập, duy trì và quản lý phiên làm việc an toàn.

8.2.4 Bảo đảm an toàn dữ liệu

8.2.4.1 Nguyên vẹn dữ liệu

a) Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra 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;

c) Có phương án khôi phục tính nguyên vẹn của thông tin dữ liệu.

8.2.4.2 Bảo mật dữ liệu

a) 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;

b) Sử dụng các phương pháp mã hóa mạnh (chưa được các tổ chức quốc tế công bố điểm yếu an toàn thông tin) để mã hóa dữ liệu;

c) Có phương án quản lý và bảo vệ dữ liệu mã hóa và khóa giải mã;

đ) Thiết lập phân vùng lưu trữ mã hóa, phân quyền truy cập chỉ cho phép người có quyền được truy cập, quản lý dữ liệu mã hóa.

8.2.4.3 Sao lưu dự phòng

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

d) Phương án sao lưu dự phòng có tính sẵn sàng cao, cho phép khôi phục dữ liệu nóng khi một thành phần trong hệ thống xảy ra sự cố.

9 Yêu cầu cơ bản cho hệ thống thông tin cấp độ 5

9.1 Yêu cầu quản lý

9.1.1 Thiết lập chính sách an toàn thông tin

9.1.1.1 Chính sách an toàn thông tin

Xây dựng chính sách an toàn thông tin, bao gồm:

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

b) Xác định trách nhiệm của đơn vị chuyên trách về an toàn thông tin, các cán bộ làm về 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 chính sách an toàn thông tin bao gồm:

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

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

- Nguồn nhân lực bảo đảm an toàn thông tin.

d) Xây dựng chính sách an toàn thông tin 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;

- Quản lý giám sát an toàn hệ thống thông tin;

- Quản lý sự cố an toàn thông tin;

- Quản lý an toàn người sử dụng đầu cuối.

9.1.1.2 Xây dựng và công bố

a) Chính sách được tổ chức/bộ phận được ủy quyền thông qua trước khi công bố áp dụng;

b) Chính sách được quản lý theo từng phiên bản khi có sự thay đổi, cập nhật;

c) Chính sách được công bố trước khi áp dụng;

d) Tổ chức tuyên truyền, phổ biến nội dung chính sách quản lý an toàn thông tin cho toàn bộ cán bộ trong tổ chức.

9.1.1.3 Rà soát, sửa đổi

a) Định kỳ 06 tháng hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung;

b) Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng chính sách trong quá trình triển khai, áp dụng chính sách an toàn thông tin.

9.1.2 Tổ chức bảo đảm an toàn thông tin

9.1.2.1 Đơn vị chuyên trách về an toàn thông tin

a) Thành lập hoặc chỉ định đơn vị chuyên trách về an toàn thông tin trong tổ chức;

b) Phân định vai trò, trách nhiệm, cơ chế phối hợp của các bộ phận, cán bộ trong đơn vị chuyên trách về an toàn thông tin;

c) Chỉ định bộ phận chuyên trách trong đơn vị chuyên trách về an toàn thông tin có trách nhiệm xây dựng và thực thi chính sách an toàn thông tin;

d) Bố trí cán bộ ở vị trí quan trọng phải là cán bộ chuyên trách;

đ) Bố trí tối thiểu 02 cán bộ theo mỗi mảng công việc cần quản lý, thực thi.

9.1.2.2 Phối hợp với những cơ quan/tổ chức có thẩm quyền

a) Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin;

b) Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin;

c) Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

9.1.3 Bảo đảm nguồn nhân lực

9.1.3.1 Tuyển dụng

a) Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng;

b) Có quy định, quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ;

c) Có chuyên gia trong lĩnh vực đánh giá, kiểm tra trình độ chuyên môn phù hợp với vị trí tuyển dụng.

9.1.3.2 Trong quá trình làm việc

a) Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống;

b) Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng;

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

d) Xây dựng tiêu chí đánh giá kỹ năng, kiến thức chuyên môn và nhận thức về an toàn thông tin đối với cán bộ ở các vị trí;

đ) Định kỳ hàng 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.

9.1.3.2 Chấm dứt hoặc thay đổi công việc

a) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức;

b) Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc;

c) Có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

9.1.4 Quản lý thiết kế, xây dựng hệ thống

9.1.4.1 Thiết kế an toàn hệ thống thông tin

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 thiết kế và các thành phần của hệ thống thông tin;

c) Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ;

d) Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin;

đ) Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống;

e) Có phương án quản lý và bảo vệ hồ sơ thiết kế;

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

9.1.4.2 Phát triển phần mềm thuê khoán

a) Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán;

b) Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm;

c) Kiểm thử phần mềm trên môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng;

d) Kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng;

đ) Khi thay đổi mã nguồn, kiến trúc phần mềm thực hiện kiểm tra, đánh giá an toàn thông tin cho phần mềm;

e) Có cam kết của bên phát triển về bảo đảm tính bí mật của mã nguồn và bản quyền của phần mềm phát triển.

9.1.4.3 Thử nghiệm và nghiệm thu hệ thống

a) Thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng;

b) Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống;

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

d) Có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống;

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

9.1.5 Quản lý vận hành hệ thống

9.1.5.1 Quản lý an toàn mạng

Chính sách, quy trình quản lý an toàn mạng bao gồm:

a) Quản lý, vận hành hoạt động bình thường của hệ thống;

b) Cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố;

c) Truy cập và quản lý cấu hình hệ thống;

d) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

9.1.5.2 Quản lý an toàn máy chủ và ứng dụng

Chính sách, quy trình quản lý an toàn máy chủ và ứng dụng bao gồm:

a) Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ;

b) Truy cập mạng của máy chủ;

c) Truy cập và quản trị máy chủ và ứng dụng;

d) Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố;

đ) Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng;

e) Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống;

g) Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

9.1.5.3 Quản lý an toàn dữ liệu

Chính sách, quy trình quản lý an toàn dữ liệu bao gồm:

a) Yêu cầu an toàn đối với phương pháp mã hóa;

b) Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa;

c) Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu;

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

đ) Sao lưu dự phòng và khôi 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;

e) Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ;

g) Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống (nếu có).

9.1.5.4 Quản lý an toàn thiết bị đầu cuối

Chính sách, quy trình quản lý thiết bị đầu cuối bao gồm:

a) Quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối;

b) Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa;

c) Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống;

d) Cấu hình tối ưu 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) Kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin cho thiết bị đầu cuối trước khi đưa vào sử dụng.

9.1.5.5 Quản lý phòng chống phần mềm độc hại

Chính sách, quy trình quản lý phần mềm độc hại bao gồm:

a) Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động;

b) Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng;

c) Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động;

d) Định kỳ thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

9.1.5.6 Quản lý giám sát an toàn hệ thống thông tin

Chính sách, quy trình quản lý giám sát an toàn hệ thống thông tin bao gồm:

a) Quản lý, vận hành hoạt động bình thường của hệ thống giám sát;

b) Đối tượng giám sát bao gồm: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống (nếu có);

c) Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát;

d) Truy cập và quản trị hệ thống giám sát;

đ) Loại thông tin cần được giám sát;

e) Lưu trữ và bảo vệ thông tin giám sát (nhật ký hệ thống);

g) Đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát;

h) Theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin;

i) Bố trí nguồn lực và tổ chức giám sát an toàn hệ thống thông tin 24/7.

9.1.5.7 Quản lý điểm yếu an toàn thông tin

Chính sách, quy trình quản lý điểm yếu an toàn thông tin bao gồm:

a) Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin: thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác (nếu có);

b) Quản lý, cập nhật 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) Cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin;

d) Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng;

đ) Phương án xử lý tạm thời khi điểm yếu an toàn thông tin không/chưa có khả năng xử lý;

e) Quy trình khôi phục lại hệ thống sau khi xử lý điểm yếu an toàn thông tin thất bại;

g) Định kỳ kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.

9.1.5.8 Quản lý sự cố an toàn thông tin

Chính sách, quy trình quản lý sự cố an toàn thông tin bao gồm:

a) Phân nhóm sự cố an toàn thông tin;

b) Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin;

c) Kế hoạch ứng phó sự cố an toàn thông tin;

d) Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin;

đ) Quy trình ứng cứu sự cố an toàn thông tin thông thường;

e) Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng;

g) Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin;

h) Định kỳ tổ chức diễn tập phương án xử lý sự cố an toàn thông tin.

9.1.5.9 Quản lý an toàn người sử dụng đầu cuối

Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:

a) Quản lý truy cập, sử dụng tài nguyên nội bộ;

b) Quản lý truy cập mạng và tài nguyên trên Internet;

c) Cài đặt và sử dụng máy tính an toàn.

9.2 Yêu cầu kỹ thuật

9.2.1 Bảo đảm an toàn mạng

9.2.1.1 Thiết kế hệ thống

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

- Vùng mạng nội bộ;
- Vùng mạng biên;
- Vùng DMZ;
- Vùng máy chủ nội bộ;
- Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác;
- Vùng mạng máy chủ cơ sở dữ liệu;
- Vùng quản trị;

- Vùng quản trị thiết bị hệ thống.

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

- Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn;

- Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập;

- Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng;

- Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu;

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

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

- Có phương án giám sát hệ thống thông tin tập trung;

- Có phương án giám sát an toàn hệ thống thông tin tập trung;

- Có phương án quản lý sao lưu dự phòng tập trung;

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

- Có phương án phòng, chống thất thoát dữ liệu;

- Có phương án duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau (nếu hệ thống buộc phải có kết nối mạng Internet);

- Có phương án bảo đảm an toàn cho mạng không dây (nếu có);

- Có phương án quản lý tài khoản đặc quyền;

- Có phương án dự phòng hệ thống ở vị trí địa lý khác nhau;

- Có phương án dự phòng cho kết nối mạng giữa hệ thống chính và hệ thống dự phòng.

9.2.1.2 Kiểm soát truy cập từ bên ngoài mạng

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet;

b) Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập 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 cập từ bên ngoài vào hệ thống 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 được hệ thống cung cấp theo năng lực thực tế của hệ thống;

e) Có phương án ưu tiên, bảo đảm chất lượng dịch vụ (QoS) cho các ứng dụng, dịch vụ quan trọng.

9.2.1.3 Kiểm soát truy cập từ bên trong mạng

a) Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài 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 kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ theo chức năng và chính sách của tổ chức;

c) Không cho phép hoặc giới hạn truy cập (theo chức năng của máy chủ) từ các máy chủ ra các mạng bên ngoài hệ thống;

d) 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;

đ) 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 (nếu có);

e) Có phương án ưu tiên, bảo đảm chất lượng dịch vụ (QoS) cho các kết nối mạng quan trọng.

9.2.1.4 Nhật ký hệ thống

a) Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống (nếu hỗ trợ), bao gồm các thông tin sau:

- 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;

- Thông tin hiệu năng hoạt động của thiết bị và tài nguyên mạng.

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 tham gia hoạt động giám sát;

c) Lưu trữ và quản lý tập trung nhật ký hệ thống thu thập được từ các thiết bị hệ thống;

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 dự phòng dữ liệu nhật ký hệ thống trên hệ thống lưu trữ riêng biệt, có mã hóa với những dữ liệu nhật ký quan trọng (nếu có);

e) Lưu trữ nhật ký hệ thống của thiết bị tối thiểu 12 tháng;

g) Phân quyền truy cập, quản lý dữ liệu nhật ký hệ thống đối với các tài khoản có chức năng quản trị hệ thống khác nhau.

9.2.1.5 Phòng chống xâm nhập

a) Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống;

b) Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng (Signatures);

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

d) Hệ thống có phương án cân bằng tải và dự phòng nóng.

9.2.1.6 Phòng chống phần mềm độc hại trên môi trường mạng

a) Có phương án phòng chống phần mềm độc hại trên môi trường mạng;

b) Định kỳ cập nhật dữ liệu cho hệ thống phòng chống phần mềm độc hại;

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

d) Hệ thống có phương án cân bằng tải và dự phòng nóng.

9.2.1.7 Bảo vệ thiết bị hệ thống

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

b) Thiết lập cấu hình chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa;

c) Không cho phép quản trị, cấu hình thiết bị trực tiếp từ các mạng bên ngoài, trường hợp bắt buộc phải quản trị thiết bị từ xa phải thực hiện gián tiếp thông qua các máy quản trị trong hệ thống và sử dụng kết nối mạng an toàn;

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

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

e) Nâng cấp, xử lý điểm yếu an toàn thông tin 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) Xóa bỏ thông tin cấu hình, dữ liệu trên thiết bị hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ khỏi hệ thống.

9.2.2 Bảo đảm an toàn máy chủ

9.2.2.1 Xác thực

a) Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng khi truy cập, 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);

c) Thiết lập cấu hình máy chủ để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:

- Yêu cầu thay đổi mật khẩu mặc định;

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

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

- Thiết lập thời gian mật khẩu hợp lệ.

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) 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);

g) Sử dụng cơ chế xác thực đa nhân tố để xác thực người sử dụng khi truy cập, quản trị vào các máy chủ trong hệ thống.

9.2.2.2 Kiểm soát truy cập

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa;

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;

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

d) Không cho phép quản trị, cấu hình máy chủ trực tiếp từ các mạng bên ngoài, trường hợp bắt buộc phải quản trị thiết bị từ xa phải thực hiện gián tiếp thông qua các máy quản trị trong hệ thống và sử dụng kết nối mạng an toàn;

đ) Phân quyền truy cập, 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;

e) Cấp quyền tối thiểu (quyền truy cập, quản trị) cho tài khoản quản trị máy chủ theo quyền hạn;

g) Kiểm soát truy cập máy chủ theo khoảng thời gian hợp lệ (theo chính sách của tổ chức nếu có).

9.2.2.3 Nhật ký hệ thống

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;

- Thông tin thay đổi cấu hình máy chủ;

- Thông tin truy cập dữ liệu và dịch vụ quan trọng trên máy chủ (nếu có).

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 tập trung nhật ký hệ thống thu thập được từ máy chủ;

đ) Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 12 tháng;

e) Lưu trữ dự phòng dữ liệu nhật ký hệ thống trên hệ thống lưu trữ riêng biệt, có mã hóa với những dữ liệu nhật ký quan trọng (nếu có);

g) Phân quyền truy cập, quản lý dữ liệu nhật ký hệ thống đối với các tài khoản có chức năng quản trị hệ thống khác nhau.

9.2.2.4 Phòng chống xâm nhập

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

b) Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ;

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

d) Có phương án cập nhật bản vá, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ;

đ) Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng;

e) Có biện pháp quản lý tập trung việc 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;

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

h) Có biện pháp phòng chống xâm nhập trên máy chủ và kiểm tra tính nguyên vẹn của các tập tin hệ thống.

9.2.2.5 Phòng chống phần mềm độc hại

a) Cài đặt phần mềm phòng chống mã độc (hoặc có phương án khác tương đương) 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;

c) Quản lý tập trung (cập nhật, cảnh báo và quản lý) các phần mềm phòng chống mã độc cài đặt 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 trước khi kết nối với máy chủ;

đ) Có cơ chế theo dõi, giám sát và cảnh báo khi có sự xuất hiện các tiến trình mới, các tập tin hệ thống trên máy chủ bị thay đổi.

9.2.2.6 Xử lý máy chủ khi chuyển giao

a) Có biện pháp chuyên dụng để xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng;

b) Sao lưu dự phòng thông tin, dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành;

c) Có biện pháp kiểm tra, bảo đảm dữ liệu không thể khôi phục sau khi xóa.

9.2.3 Bảo đảm an toàn ứng dụng

9.2.3.1 Xác thực

a) Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng;

b) Lưu trữ có mã hóa thông tin xác thực hệ thống;

c) Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:

- Yêu cầu thay đổi mật khẩu mặc định;

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

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

- Thiết lập thời gian mật khẩu hợp lệ.

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

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 đối với các ứng dụng, dịch vụ cung cấp và xử lý dữ liệu quan trọng trong hệ thống;

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

h) Sử dụng cơ chế xác thực đa nhân tố để xác thực người sử dụng khi truy cập, quản trị các dịch vụ quan trọng trong hệ thống.

9.2.3.2 Kiểm soát truy cập

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa;

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

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

d) Phân quyền truy cập, 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;

đ) 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;

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

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

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

i) Khóa tạm thời hoặc không cho phép quản trị ứng dụng trong khoảng thời gian ngoài giờ làm việc theo chính sách của tổ chức (nếu có).

9.2.3.3 Nhật ký hệ thống

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

- Thông tin truy cập ứng dụng;

- Thông tin đăng nhập khi quản trị ứng dụng;

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

- Thông tin thay đổi cấu hình ứng dụng.

b) Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung;

c) Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 12 tháng;

d) Lưu trữ dự phòng dữ liệu nhật ký hệ thống trên hệ thống lưu trữ riêng biệt, có mã hóa với những dữ liệu nhật ký quan trọng (nếu có);

đ) Phân quyền truy cập, quản lý dữ liệu nhật ký hệ thống đối với các tài khoản có chức năng quản trị hệ thống khác nhau.

9.2.3.4 Bảo mật thông tin liên lạc

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; sử dụng phương án mã hóa theo quy định về bảo vệ bí mật nhà nước đối với thông tin mật;

b) Sử dụng kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền;

c) Sử dụng kết hợp các kết nối mạng an toàn hoặc biện pháp mã hóa để bảo đảm dữ liệu quan trọng được mã hóa 02 lần khi truyền qua môi trường mạng;

d) Sử dụng kênh vật lý riêng khi truyền đưa, trao đổi qua môi trường mạng đối với dữ liệu quan trọng;

đ) Sử dụng thiết bị phần cứng chuyên dụng để phục vụ mã hóa và giải mã.

9.2.3.5 Chống chối bỏ

a) Sử dụng chữ ký số khi trao đổi thông tin, dữ liệu quan trọng;

b) Chữ ký số được cung cấp bởi cơ quan có thẩm quyền hoặc đơn vị cung cấp dịch vụ chữ ký số được cấp phép;

c) Có phương án bảo đảm an toàn trong việc quản lý và sử dụng chữ ký số;

d) Sử dụng thiết bị, phương tiện chuyên dụng để thực hiện ký và giải mã thông tin, dữ liệu khi gửi và nhận.

9.2.3.6 An toàn ứng dụng và mã nguồn

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

b) Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu;

c) Có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF;

d) Có chức năng kiểm soát lỗi, thông báo lỗi từ ứng dụng;

đ) Không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng;

e) Có chức năng tạo lập, duy trì và quản lý phiên làm việc an toàn.

9.2.4 Bảo đảm an toàn dữ liệu

9.2.4.1 Nguyên vẹn dữ liệu

a) Có phương án chuyên dụng để quản lý, lưu trữ dữ liệu 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;

c) Có phương án khôi phục tính nguyên vẹn của thông tin dữ liệu.

9.2.4.2 Bảo mật dữ liệu

a) 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;

b) Sử dụng các phương pháp mã hóa mạnh (chưa được các tổ chức quốc tế công bố điểm yếu an toàn thông tin) để mã hóa dữ liệu;

c) Có phương án chuyên dụng để quản lý và bảo vệ dữ liệu mã hóa và khóa giải mã;

đ) Thiết lập phân vùng lưu trữ mã hóa, phân quyền truy cập chỉ cho phép người có quyền được truy cập, quản lý dữ liệu mã hóa.

9.2.4.3 Sao lưu dự phòng

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

d) Phương án sao lưu dự phòng có tính sẵn sàng cao, cho phép khôi phục dữ liệu nóng khi một thành phần trong hệ thống xảy ra sự cố;

đ) Lưu trữ dự phòng các dữ liệu quan trọng trên hệ thống/phương tiện lưu trữ dự phòng ở vị trí địa lý khác nhau; bảo đảm môi trường bảo quản và phương pháp quản lý giống như với hệ thống chính;

e) Duy trì ít nhất 02 kết nối mạng từ hệ thống sao lưu dự phòng chính với hệ thống sao lưu dự phòng phụ.

Phụ lục A

(Quy định)

Yêu cầu cơ bản về an toàn vật lý cho hệ thống thông tin theo cấp độ

A.1 Yêu cầu vật lý cho hệ thống thông tin cấp độ 1

A.1.1 Kiểm soát truy cập vật lý

Thiết lập cổng bảo vệ để kiểm soát vào, ra phòng máy chủ.

A.1.2 Chống trộm, chống phá hoại

Thiết bị hệ thống phải được đặt trong phòng máy chủ và có tủ bảo vệ (tủ rack), được đặt cố định và gắn nhãn mô tả.

A.1.3 Chống cháy

Phòng máy chủ được trang bị hệ thống phòng cháy, chữa cháy.

A.1.4 Nguồn cung cấp

Nguồn điện trong phòng máy chủ phải được đảm bảo ổn định có ổn áp, chống quá tải.

A.2 Yêu cầu vật lý cho hệ thống thông tin cấp độ 2

A.2.1 Kiểm soát truy cập vật lý

a) Thiết lập hệ thống cổng bảo vệ để kiểm soát vào, ra phòng máy chủ;

b) Thiết lập hệ thống camera giám sát, ghi lại thông tin vào ra phòng máy chủ.

A.2.2 Chống trộm, chống phá hoại

Thiết bị hệ thống phải được đặt trong phòng máy chủ và có tủ bảo vệ (tủ rack), được đặt cố định và gắn nhãn mô tả.

A.2.3 Chống sét

Tòa nhà đặt phòng máy chủ phải được thiết lập hệ thống chống sét.

A.2.4 Chống cháy

Phòng máy chủ phải lắp đặt hệ thống cảnh báo và chữa cháy tự động.

A.2.5 Kiểm soát nhiệt độ và độ ẩm

Có hệ thống điều hòa, bảo đảm về nhiệt độ, độ ẩm ổn định trong phòng máy chủ.

A.2.6 Nguồn cung cấp

a) Nguồn điện trong phòng máy chủ phải được đảm bảo ổn định có ổn áp, chống quá tải;

b) Có hệ thống UPS đảm bảo hoạt động liên tục của các thiết bị mạng chính và các máy chủ quan trọng.

A.3 Yêu cầu vật lý cho hệ thống thông tin cấp độ 3

A.3.1 Lựa chọn vị trí vật lý

Vị trí phòng máy chủ không được nằm ở các tầng cao của tòa nhà; không được đặt dưới tầng hầm hoặc dưới các nơi chứa, đựng nước.

A.3.2 Kiểm soát truy cập vật lý

a) Thiết lập hệ thống cổng điện tử để kiểm soát vào, ra phòng máy chủ;

b) Thiết lập hệ thống camera giám sát, ghi lại thông tin vào ra phòng máy chủ. Dữ liệu nhật ký camera phải được lưu trữ tối thiểu 03 tháng;

c) Có phương án kiểm soát các thiết bị, vật dụng được mang ra, vào phòng máy chủ.

A.3.3 Chống trộm, chống phá hoại

a) Thiết bị hệ thống phải được đặt trong phòng máy chủ và có tủ bảo vệ (tủ rack), được đặt cố định và gắn nhãn mô tả;

b) Kết nối vật lý (cáp mạng, điện thoại...) trong phòng phải được đi ngầm và có đường ống bảo vệ;

c) Thiết lập hệ thống báo động chống trộm tự động.

A.3.4 Chống sét

a) Tòa nhà đặt phòng máy chủ phải được thiết lập hệ thống chống sét và được nghiệm thu, kiểm tra kỹ thuật của ban quản lý tòa nhà;

b) Các thiết bị, tủ kỹ thuật trong phòng máy chủ phải được nối đất.

A.3.5 Chống cháy

a) Phòng máy chủ phải lắp đặt hệ thống cảnh báo và chữa cháy tự động;

b) Phòng máy chủ phải được xây dựng sử dụng các vật liệu chịu lửa.

A.3.6 Chống ẩm và chống thấm

a) Tường và sàn nhà của phòng máy chủ có các đường ống thoát nước; đường ống thoát nước không được đi qua trần, sàn phòng máy chủ;

b) Trần và các cửa, cửa sổ phòng máy chủ phải được thiết kế đảm bảo không bị nước mưa hắt vào;

c) Có biện pháp ngăn không cho nước mưa thấm qua trần và tường vào phòng máy, tích tụ nước và di chuyển nước tích tụ trong phòng máy.

A.3.7 Chống tĩnh điện

a) Có biện pháp chống tĩnh điện đối với các thiết bị mạng chính;

b) Sàn phòng máy chủ cần phải được lắp đặt sàn chống tĩnh điện.

A.3.8 Kiểm soát nhiệt độ và độ ẩm

Có hệ thống điều hòa trung tâm, bảo đảm về nhiệt độ, độ ẩm ổn định trong phòng máy chủ.

A.3.9 Nguồn cung cấp

a) Nguồn điện trong phòng máy chủ phải được đảm bảo ổn định có ổn áp, chống quá tải;

b) Có nguồn cung cấp điện dự phòng, có thể thay thế nguồn cung cấp điện chính;

c) Có hệ thống UPS đảm bảo hoạt động liên tục của các thiết bị hệ thống và máy chủ.

A.3.10 Bảo vệ điện từ

a) Đường điện và cáp tín hiệu (cáp mạng, thoại...) phải được đặt cách ly để tránh nhiễu điện từ đường điện sang cáp tín hiệu;

b) Có phương án che chắn, cách ly các nguồn nhiễu điện từ như: các máy biến áp, các động cơ và máy phát điện, thiết bị X quang, các máy phát ra-đa hoặc vô tuyến, thiết bị hàn nhiệt.

A.4 Yêu cầu vật lý cho hệ thống thông tin cấp độ 4

A.4.1 Lựa chọn vị trí vật lý

a) Vị trí phòng máy chủ không được nằm ở các tầng cao của tòa nhà; không được đặt dưới tầng hầm hoặc dưới các nơi chứa, đựng nước;

b) Vị trí đặt phòng máy chủ cần tránh khu vực dễ phát sinh lửa như khu vực gần kho dầu, vật dễ cháy, khu vực có điện trường và từ trường mạnh.

A.4.2 Kiểm soát truy cập vật lý

a) Thiết lập hệ thống cổng điện tử để kiểm soát vào, ra phòng máy chủ;

b) Thiết lập hệ thống camera giám sát, ghi lại thông tin vào ra phòng máy chủ; hệ thống phải được quản lý tập trung và được theo dõi, giám sát 24/7. Dữ liệu nhật ký camera phải được lưu trữ tối thiểu 06 tháng;

c) Thiết lập khu vành đai giữa phòng máy chủ với các khu vực khác trong tòa nhà;

d) Các khu vực trong phòng máy chủ đặt thiết bị mạng chính và máy chủ quan trọng phải có hệ thống camera giám sát và có tủ bảo vệ.

A.4.3 Chống trộm, chống phá hoại

a) Thiết bị hệ thống phải được đặt trong phòng máy chủ và có tủ bảo vệ (tủ rack), được đặt cố định và gắn nhãn mô tả;

b) Kết nối vật lý (cáp mạng, điện thoại...) trong phòng phải được đi ngầm và có đường ống bảo vệ;

c) Thiết lập hệ thống báo động chống trộm tự động sử dụng kỹ thuật quang điện hoặc những kỹ thuật khác tương đương.

A.4.4 Chống sét

a) Tòa nhà đặt phòng máy chủ phải được thiết lập hệ thống chống sét và được nghiệm thu, kiểm tra kỹ thuật của ban quản lý tòa nhà;

b) Có phương án phòng chống sét lan truyền cho các thiết bị hệ thống, các thiết bị phụ trợ và nguồn cung cấp điện;

c) Kết nối mạng giữa các thiết bị hệ thống có cơ chế phòng chống sét lan truyền.

A.4.5 Chống cháy

a) Phòng máy chủ phải lắp đặt hệ thống cảnh báo và chữa cháy tự động; có các hình thức phát tín hiệu cảnh báo cháy khác nhau (bằng âm thanh, ánh sáng...);

b) Phòng máy chủ phải được xây dựng sử dụng các vật liệu chịu lửa;

c) Khu vực máy chủ quan trọng và thiết bị mạng chính phải đặt cách ly và có biện pháp cách lửa với các khu vực khác.

A.4.6 Chống ẩm và chống thấm

a) Tường và sàn nhà của phòng máy chủ có các đường ống thoát nước; đường ống thoát nước không được đi qua trần, sàn phòng máy chủ;

b) Trần và các cửa, cửa sổ phòng máy chủ phải được thiết kế đảm bảo không bị nước mưa hắt vào;

c) Có biện pháp ngăn không cho nước mưa thấm qua trần và tường vào phòng máy, tích tụ nước và di chuyển nước tích tụ trong phòng máy.

A.4.7 Chống tĩnh điện

a) Có biện pháp chống tĩnh điện đối với các thiết bị trong phòng máy chủ;

b) Sàn phòng máy chủ cần phải được lắp đặt sàn chống tĩnh điện.

A.4.8 Kiểm soát nhiệt độ và độ ẩm

a) Có hệ thống điều hòa trung tâm, bảo đảm về nhiệt độ, độ ẩm ổn định trong phòng máy chủ;

b) Hệ thống điều hòa không khí tại phòng máy phải riêng biệt hoàn toàn với các hệ thống điều hòa khác trong tòa nhà;

c) Có thiết bị đo độ ẩm và cảnh báo khi độ ẩm trong phòng máy chủ vượt mức cho phép;

d) Có thiết bị hút ẩm để ngăn chặn sự ngưng tụ hơi nước ở phòng máy chủ và thẩm thấu nước đã tích tụ ở sàn phòng máy chủ.

A.4.9 Nguồn cung cấp

a) Nguồn điện trong phòng máy chủ phải được đảm bảo ổn định có ổn áp, chống quá tải;

b) Sử dụng hai nguồn cung cấp kéo từ hai trạm điện khác nhau;

c) Có hệ thống UPS đảm bảo hoạt động liên tục của các thiết bị hệ thống và máy chủ.

A.4.10 Bảo vệ điện từ

a) Đường điện và cáp tín hiệu (cáp mạng, thoại...) phải được đặt cách ly để tránh nhiễu điện từ đường điện sang cáp tín hiệu;

b) Có phương án che chắn, cách ly các nguồn nhiễu điện từ như: các máy biến áp, các động cơ và máy phát điện, thiết bị X quang, các máy phát ra-đa hoặc vô tuyến, thiết bị hàn nhiệt;

c) Có tấm chắn điện từ cho khu vực máy chủ quan trọng và thiết bị mạng chính.

A.5 Yêu cầu vật lý cho hệ thống thông tin cấp độ 5

A.5.1 Lựa chọn vị trí vật lý

a) Vị trí phòng máy chủ không được nằm ở các tầng cao của tòa nhà; không được đặt dưới tầng hầm hoặc dưới các nơi chứa, đựng nước.

b) Vị trí đặt phòng máy chủ cần tránh khu vực dễ phát sinh lửa như khu vực gần kho dầu, vật dễ cháy, khu vực có điện trường và từ trường mạnh;

c) Vị trí xây dựng phòng máy chủ phải tránh được các điều kiện khắc nghiệt của thời tiết như: bão, thiên tai và các điều kiện khác.

A.5.2 Kiểm soát truy cập vật lý

a) Thiết lập hệ thống cổng điện tử để kiểm soát vào, ra phòng máy chủ, có ít nhất 02 yếu tố xác thực khi vào phòng máy chủ hoặc truy cập vật lý các thiết bị mạng chính;

b) Thiết lập hệ thống camera giám sát, ghi lại thông tin vào ra phòng máy chủ; hệ thống phải được quản lý tập trung và được theo dõi, giám sát 24/7. Dữ liệu nhật ký camera phải được lưu trữ tối thiểu 12 tháng;

c) Thiết lập khu vành đai giữa phòng máy chủ với các khu vực khác trong tòa nhà;

d) Các khu vực trong phòng máy chủ đặt thiết bị mạng chính và máy chủ quan trọng phải có hệ thống camera giám sát và có tủ bảo vệ.

A.5.3 Chống trộm, chống phá hoại

a) Thiết bị hệ thống phải được đặt trong phòng máy chủ và có tủ bảo vệ (tủ rack), được đặt cố định và gắn nhãn mô tả;

b) Kết nối vật lý (cáp mạng, điện thoại...) trong phòng phải được đi ngầm và có đường ống bảo vệ;

c) Thiết lập hệ thống báo động chống trộm tự động sử dụng kỹ thuật quang điện hoặc những kỹ thuật khác tương đương;

d) Thiết lập lớp bảo vệ vật lý thứ 2 cho khu vực máy chủ quan trọng, thiết bị mạng chính; có hệ thống kiểm soát vào, ra khu vực này, sử dụng tối thiểu 02 yếu tố xác thực.

A.5.4 Chống sét

a) Tòa nhà đặt phòng máy chủ phải được thiết lập hệ thống chống sét và được nghiệm thu, kiểm tra kỹ thuật của ban quản lý tòa nhà;

b) Có phương án phòng chống sét lan truyền cho các thiết bị hệ thống, các thiết bị phụ trợ và nguồn cung cấp điện;

c) Kết nối mạng giữa các thiết bị hệ thống có cơ chế phòng chống sét lan truyền;

d) Có phương án quản lý, giám sát tập trung hệ thống chống sét.

A.5.5 Chống cháy

a) Phòng máy chủ phải lắp đặt hệ thống cảnh báo và chữa cháy tự động; có các hình thức phát tín hiệu cảnh báo cháy khác nhau (bằng âm thanh, ánh sáng...);

b) Phòng máy chủ phải được xây dựng sử dụng các vật liệu chịu lửa;

c) Khu vực máy chủ quan trọng và thiết bị mạng chính phải đặt cách ly và có biện pháp cách lửa với các khu vực khác;

d) Có phương án quản lý, giám sát tập trung hệ thống chống cháy; bố trí nguồn lực và tổ chức giám sát 24/7.

A.5.6 Chống ẩm và chống thấm

a) Tường và sàn nhà của phòng máy chủ có các đường ống thoát nước; đường ống thoát nước không được đi qua trần, sàn phòng máy chủ;

b) Trần và các cửa, cửa sổ phòng máy chủ phải được thiết kế đảm bảo không bị nước mưa hắt vào;

c) Có biện pháp ngăn không cho nước mưa thấm qua trần và tường vào phòng máy, tích tụ nước và di chuyển nước tích tụ trong phòng máy.

A.5.7 Chống tĩnh điện

a) Có biện pháp chống tĩnh điện đối với các thiết bị trong phòng máy chủ;

b) Sàn phòng máy chủ cần phải được lắp đặt sàn chống tĩnh điện.

c) Có phương án giảm thiểu sự phát sinh tĩnh điện cho các máy chủ quan trọng và thiết bị mạng chính;

d) Các vật liệu sử dụng xây dựng phòng máy chủ phải sử dụng loại vật liệu cách điện hoặc sinh ra tĩnh điện nhỏ.

A.5.8 Kiểm soát nhiệt độ và độ ẩm

a) Có hệ thống điều hòa trung tâm, bảo đảm về nhiệt độ, độ ẩm ổn định trong phòng máy chủ;

b) Hệ thống điều hòa không khí tại phòng máy phải riêng biệt hoàn toàn với các hệ thống điều hòa khác trong tòa nhà.

c) Có thiết bị đo độ ẩm và cảnh báo khi độ ẩm trong phòng máy chủ vượt mức cho phép.

d) Có thiết bị hút ẩm để ngăn chặn sự ngưng tụ hơi nước ở phòng máy chủ và thẩm thấu nước đã tích tụ ở sàn phòng máy chủ;

đ) Có phương án quản lý, giám sát tập trung hệ thống kiểm soát nhiệt độ và độ ẩm; bố trí nguồn lực và tổ chức giám sát 24/7.

A.5.9 Nguồn cung cấp

a) Nguồn điện trong phòng máy chủ phải được đảm bảo ổn định có ổn áp, chống quá tải;

b) Sử dụng hai nguồn cung cấp kéo từ hai trạm điện khác nhau;

c) Có hệ thống UPS đảm bảo hoạt động liên tục của các thiết bị hệ thống và máy chủ;

d) Có phương án quản lý, giám sát tập trung hệ thống nguồn cung cấp; bố trí nguồn lực và tổ chức giám sát 24/7.

A.5.10 Bảo vệ điện từ

a) Đường điện và cáp tín hiệu (cáp mạng, thoại...) phải được đặt cách ly để tránh nhiễu điện từ đường điện sang cáp tín hiệu;

b) Có phương án che chắn, cách ly các nguồn nhiễu điện từ như: các máy biến áp, các động cơ và máy phát điện, thiết bị X quang, các máy phát ra-đa hoặc vô tuyến, thiết bị hàn nhiệt;

c) Có tấm chắn điện từ cho khu vực máy chủ quan trọng và thiết bị mạng chính.