**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**HƯỚNG DẪN BẢO ĐẢM AN TOÀN THÔNG TIN CHO
TRUNG TÂM DỮ LIỆU PHỤC VỤ CHÍNH PHỦ ĐIỆN TỬ**

(*Kèm theo Công văn số /BTTTT-CATTT ngày tháng 6 năm 2020
của Bộ Thông tin và Truyền thông)*

**Hà Nội, 2020**

CHƯƠNG 1

HƯỚNG DẪN CHUNG

# 1. Phạm vi áp dụng

Tài liệu này đưa ra các yêu cầu cơ bản và hướng dẫn bảo đảm an toàn thông tin đối với TTDL phục vụ hoạt động thuê ngoài dịch vụ CNTT của cơ quan, tổ chức để triển khai ứng dụng CNTT theo Khung kiến trúc Chính phủ điện tử Việt Nam, phiên bản 2.0 (sau đây gọi là TTDL phục vụ CPĐT).

# 2. Đối tượng áp dụng

a) Cơ quan, tổ chức vận hành TTDL phục vụ CPĐT (trong trường hợp chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin) theo quy định tại khoản 3, Điều 3 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (Nghị định số 85/2016/NĐ-CP).

b) Cơ quan, tổ chức tự đầu tư, quản lý vận hành TTDL hoặc thuê chỗ đặt thiết bị tại TTDL của doanh nghiệp (dịch vụ Colocation) không thuộc đối tượng áp dụng của hướng dẫn này, việc thực thi bảo đảm an toàn thông tin cho TTDL này thực hiện theo quy định tại Nghị định số 85/2016/NĐ-CP và hướng dẫn chi tiết tại Công văn số 713/CATTT-TĐQLGS ngày 25/7/2019.

c) Cơ quan, tổ chức khác được khuyến nghị tham khảo, áp dụng hướng dẫn này để bảo đảm an toàn thông tin cho TTDL thuộc phạm vi quản lý của mình.

3. Thuật ngữ, định nghĩa

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Từ****viết tắt** | **Thuật ngữ tiếng Anh** | **Thuật ngữ tiếng Việt** |
| 1 | ATTT |  | An toàn thông tin |
| 2 | CNTT |  | Công nghệ thông tin |
| 3 | CPĐT |  | Chính phủ điện tử |
| 4 | HSĐXCĐ |  | Hồ sơ đề xuất cấp độ |
| 5 | TSLCD |  | Truyền số liệu chuyên dùng |
| 6 | TTDL |  | Trung tâm dữ liệu |
| 7 | ĐTĐM |  | Điện toán đám mây |
| 8 | IaaS | Infrastructure as a Service | Dịch vụ điện toán đám mây cung cấp dịch vụ cơ sở hạ tầng |
| 9 | PaaS | Platform as a Service | Dịch vụ điện toán đám mây cung cấp dịch vụ nền tảng |
| 10 | SaaS | Software as a Service | Dịch vụ điện toán đám mây cung cấp dịch vụ phần mềm |
| 11 | MSP | Managed Service Provider | Nhà cung cấp dịch vụ quản trị, vận hành khai thác |

# 4. Nguyên tắc bảo đảm an toàn thông tin cho TTDL phục vụ CPĐT

a) Nguyên tắc bảo đảm an toàn thông tin cho TTDL phục vụ CPĐT phải tuân thủ quy định tại Điều 4 và Điều 5 Nghị định số 85/2016/NĐ-CP;

b) Phương án bảo đảm an toàn thông tin cho TTDL phục vụ CPĐT phải đáp ứng các yêu cầu an toàn cho hệ thống thông tin có cấp độ cao nhất được triển khai trên đó;

c) Hệ thống thông tin hoặc thành phần hệ thống thông tin do bên nào (bên cung cấp hoặc bên sử dụng dịch vụ) quản lý vận hành thì bên đó có trách nhiệm bảo đảm an toàn thông tin cho hệ thống/thành phần đó;

d) HSĐXCĐ và phương án bảo đảm an toàn thông tin cho TTDL phục vụ CPĐT phải được thẩm định, phê duyệt và triển khai, trước khi cung cấp dịch vụ;

e) Hệ thống thông tin khác nhau được triển khai trên TTDL phục vụ CPĐT phải đảm bảo sự phân tách về lô-gíc hoặc vật lý, được mô tả rõ ràng theo mô hình, hồ sơ cung cấp dịch vụ với nhà cung cấp dịch vụ để không gây ra nguy cơ mất an toàn giữa các hệ thống với nhau.

# 5. Hồ sơ đề xuất cấp độ

Cơ quan, tổ chức vận hành TTDL phục vụ CPĐT và bên thuê ngoài dịch vụ CNTT (thuộc phạm vi áp dụng tại Mục 1) phải xây dựng, thẩm định và phê duyệt HSĐXCĐ theo quy định tại Nghị định số 85/2016/NĐ-CP.

Hướng dẫn chi tiết việc xây dựng HSĐXCĐ tại Chương 3 hướng dẫn này.

# 6. Phương án bảo đảm an toàn thông tin

Yêu cầu bảo đảm an toàn thông tin đối với TTDL đưa ra tại hướng dẫn này là các yêu cầu cơ bản, phù hợp với các loại hình hệ thống thông tin phổ biến. Đối với các hệ thống thông tin có tính chất đặc thù riêng (nếu có) thì có thể điều chỉnh và thuyết minh phương án phù hợp. Các yêu cầu cơ bản bao gồm:

- Yêu cầu an toàn trong thiết kế, thiết lập bao gồm: (1) Bảo đảm an toàn mạng, (2) Bảo đảm an toàn máy chủ, (3) Bảo đảm an toàn ứng dụng, (4) Bảo đảm an toàn dữ liệu;

- Yêu cầu an toàn trong quản lý, vận hành bao gồm: (1) Thiết lập chính sách an toàn thông tin; (2) Tổ chức bảo đảm an toàn thông tin; (3) Quản lý thiết kế, xây dựng hệ thống; (4) Quản lý vận hành hệ thống.

Hướng dẫn chi tiết yêu cầu bảo đảm an toàn thông tin tại Chương 2 hướng dẫn này.

CHƯƠNG 2

YÊU CẦU AN TOÀN CƠ BẢN ĐỐI VỚI TRUNG TÂM DỮ LIỆU PHỤC VỤ CHÍNH PHỦ ĐIỆN TỬ

# 1. Yêu cầu chung

a) Việc thực thi bảo đảm an toàn thông tin phải tuân thủ các quy định của pháp luật; phương án bảo đảm an toàn thông tin phải đáp ứng các yêu cầu an toàn cơ bản theo quy định, phù hợp với Khung CPĐT 2.0 và các văn bản liên quan;

 b) Trung tâm dữ liệu phải được xây dựng HSĐXCĐ, thẩm định và phê duyệt theo quy định của pháp luật;

c) Phương án bảo đảm an toàn thông tin phải đáp ứng các yêu cầu tối thiểu theo quy định tại Thông tư 03/2017/TT-BTTTT ngày 24/4/2017 và hướng dẫn tại tiêu chuẩn quốc gia TCVN 11930:2017;

d) Trung tâm dữ liệu có kết nối vào mạng Truyền số liệu chuyên dùng phải đáp ứng các quy định tại Thông tư số 12/2019/TT-BTTTT ngày 05/11/2019;

đ) Giải pháp nền tảng điện toán đám mây của TTDL đáp ứng các yêu cầu an toàn theo văn bản “Hướng dẫn bộ tiêu chí, chỉ tiêu kỹ thuật để đánh giá và lựa chọn giải pháp nền tảng điện toán đám mây phục vụ Chính phủ điện tử/Chính quyền điện tử” tại Công văn số 1145/BTTTT-CATTT của Bộ Thông tin và Truyền thông ngày 03/04/2020.

# 2. Yêu cầu an toàn thông tin tối thiểu đối với TTDL phục vụ CPĐT

a) Đáp ứng các yêu cầu an toàn cơ bản cấp độ 3 tại Tiêu chuẩn quốc gia TCVN 11930:2017 về yêu cầu an toàn cơ bản về hệ thống thông tin theo cấp độ;

b) Việc thiết kế, thiết lập hệ thống thông tin của bên thuê ngoài dịch vụ CNTT phải đáp ứng các yêu cầu:

- Hệ thống phải được thiết kế tách riêng, độc lập với các hệ thống khác về lô-gíc (lớp mạng) và có biện pháp quản lý truy cập giữa các hệ thống;

- Các vùng mạng trong hệ thống phải được thiết kế tách riêng, độc lập với nhau về lô-gíc (lớp mạng) và có biện pháp quản lý truy cập giữa các vùng mạng;

- Có phân vùng lưu trữ được phân tách độc lập về lô-gíc;

- Các thiết bị mạng chính bao gồm: cổng kết nối, thiết bị chuyển mạch trung tâm, thiết bị tường lửa và thiết bị định tuyến biên (nếu có) phải được phân tách độc lập về lô-gíc.

# 3. Yêu cầu an toàn thông tin tối thiểu đối với TTDL phục vụ CPĐT đối với hệ thống thông tin từ cấp độ 4 đến cấp độ 5

a) Đáp ứng các yêu cầu an toàn cơ bản cấp độ 4 hoặc 5 tương ứng với hệ thống thông tin được triển khai trên đó theo Tiêu chuẩn quốc gia TCVN 11930:2017;

b) Việc thiết kế, thiết lập hệ thống thông tin của bên thuê ngoài dịch vụ CNTT phải đáp ứng các yêu cầu:

- Hệ thống phải được thiết kế tách riêng, độc lập với các hệ thống khác về vật lý và có biện pháp quản lý truy cập giữa các hệ thống;

- Các vùng mạng trong hệ thống phải được thiết kế tách riêng, độc lập với nhau về lô-gic (lớp mạng) và có biện pháp quản lý truy cập giữa các vùng mạng;

- Có phân vùng lưu trữ được phân tách độc lập về vật lý;

- Các thiết bị mạng chính bao gồm: cổng kết nối, thiết bị chuyển mạch trung tâm, thiết bị tường lửa và thiết bị định tuyến biên (nếu có) phải được phân tách độc lập về vật lý.

# 4. Yêu cầu an toàn cơ bản về kỹ thuật đối với TTDL phục vụ CPĐT theo tiêu chuẩn TCVN 11930:2017

## 4.1. Yêu cầu an toàn hạ tầng mạng

a) Yêu cầu về thiết lập, cấu hình hệ thống

Yêu cầu an toàn đối với hạ tầng mạng bao gồm 07 nhóm yêu cầu, được tham chiếu trong tiêu chuẩn quốc gia TCVN 11930:2017 như sau:

***Bảng 1. Bảng tham chiếu yêu cầu an toàn hạ tầng mạng***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Cấp độ | Thiết kế hệ thống | Kiểm soát truy cập từ bên ngoài mạng | Kiểm soát truy cập từ bên trong mạng | Nhật ký hệ thống | Phòng chống xâm nhập | Phòng chống phần mềm độc hại trên môi trường mạng | Bảo vệ thiết bị hệ thống |
| Cấp độ 3 | 7.2.1.1 | 7.2.1.2 | 7.2.1.3 | 7.2.1.4 | 7.2.1.5 | 7.2.1.6 | 7.2.1.7 |
| Cấp độ 4 | 8.2.1.1 | 8.2.1.2 | 8.2.1.3 | 8.2.1.4 | 8.2.1.5 | 8.2.1.6 | 8.2.1.7 |
| Cấp độ 5 | 9.2.1.1 | 9.2.1.2 | 9.2.1.3 | 9.2.1.4 | 9.2.1.5 | 9.2.1.6 | 9.2.1.7 |

b) Yêu cầu về phương án bảo vệ

***Bảng 2. Bảng tham chiếu yêu cầu về các phương án bảo vệ***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STT | Tên phương án | Cấp độ 3 | Cấp độ 4 | Cấp độ 5 |
| 1 | Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn | X | X | X |
| 2 | Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập | X | X | X |
| 3 | Phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng | X | X | X |
| 4 | Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu | X | X | X |
| 5 | Phương án chặn lọc phần mềm độc hại trên môi trường mạng | X | X | X |
| 6 | Phương án phòng chống tấn công từ chối dịch vụ | X | X | X |
| 7 | Phương án giám sát hệ thống thông tin tập trung | X | X | X |
| 8 | Phương án giám sát an toàn hệ thống thông tin tập trung | X | X | X |
| 9 | Phương án quản lý sao lưu dự phòng tập trung | X | X | X |
| 10 | Phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung | X | X | X |
| 11 | Phương án phòng, chống thất thoát dữ liệu | X | X | X |
| 12 | Phương án quản lý tài khoản đặc quyền |  | X | X |
| 13 | Phương án dự phòng hệ thống ở vị trí địa lý khác nhau |  |  | X |
| 14 | Phương án dự phòng cho kết nối mạng giữa hệ thống chính và hệ thống dự phòng |  |  | X |

## 4.2. Yêu cầu bảo đảm an toàn máy chủ

Yêu cầu an toàn đối với máy chủ bao gồm 06 nhóm yêu cầu, được tham chiếu trong tiêu chuẩn quốc gia TCVN 11930:2017 như sau:

***Bảng 3. Bảng tham chiếu yêu cầu an toàn cơ bản cho máy chủ***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| STT | Xác thực | Kiểm soát truy cập | Nhật ký hệ thống | Phòng chống xâm nhập | Phòng chống phần mềm độc hại | Xử lý máy chủ khi chuyển giao |
| Cấp độ 3 | 7.2.2.1 | 7.2.2.2 | 7.2.2.3 | 7.2.2.4 | 7.2.2.5 | 7.2.2.6 |
| Cấp độ 4 | 8.2.2.1 | 8.2.2.2 | 8.2.2.3 | 8.2.2.4 | 8.2.2.5 | 8.2.2.6 |
| Cấp độ 5 | 9.2.2.1 | 9.2.2.2 | 9.2.2.3 | 9.2.2.4 | 9.2.2.5 | 9.2.2.6 |

## 4.3. Yêu cầu về an toàn ứng dụng

Yêu cầu an toàn đối với ứng dụng bao gồm 06 nhóm yêu cầu, được tham chiếu trong tiêu chuẩn quốc gia TCVN 11930:2017 như sau:

***Bảng 4. Bảng tham chiếu yêu cầu an toàn cơ bản cho ứng dụng***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| STT | Xác thực | Kiểm soát truy cập | Nhật ký hệ thống | Bảo mật thông tin liên lạc | Chống chối bỏ | An toàn ứng dụng và mã nguồn |
| Cấp độ 3 | 7.2.3.1 | 7.2.3.2 | 7.2.3.3 | 7.2.3.4 | 7.2.3.5 | 7.2.3.6 |
| Cấp độ 4 | 8.2.3.1 | 8.2.3.2 | 8.2.3.3 | 8.2.3.4 | 8.2.3.5 | 8.2.3.6 |
| Cấp độ 5 | 9.2.3.1 | 9.2.3.2 | 9.2.3.3 | 9.2.3.4 | 9.2.3.5 | 9.2.3.6 |

## 4.4. Yêu cầu về an toàn dữ liệu

Yêu cầu an toàn đối với dữ liệu bao gồm 03 nhóm yêu cầu, được tham chiếu trong tiêu chuẩn quốc gia TCVN 11930:2017 như sau:

***Bảng 5. Bảng tham chiếu yêu cầu an toàn cơ bản cho dữ liệu***

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nguyên vẹn dữ liệu | Bảo mật dữ liệu | Sao lưu dự phòng |
| Cấp độ 3 | 7.2.4.1 | 7.2.4.2 | 7.2.4.3 |
| Cấp độ 4 | 8.2.4.1 | 8.2.4.2 | 8.2.4.3 |
| Cấp độ 5 | 9.2.4.1 | 9.2.4.2 | 9.2.4.3 |

# 5. Yêu cầu an toàn cơ bản về quản lý đối với TTDL phục vụ CPĐT theo tiêu chuẩn TCVN 11930:2017

Yêu cầu an toàn đối với quản lý bao gồm 05 nhóm yêu cầu, được tham chiếu trong tiêu chuẩn quốc gia TCVN 11930:2017 như sau:

***Bảng 6. Bảng tham chiếu yêu cầu an toàn cơ bản về quản lý***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| STT | 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 |
| Cấp độ 3 | 7.1.1 | 7.1.2 | 7.1.3 | 7.1.4 | 7.1.5 |
| Cấp độ 4 | 8.1.1 | 8.1.2 | 8.1.3 | 8.1.4 | 8.1.5 |
| Cấp độ 5 | 9.1.1 | 9.1.2 | 9.1.3 | 9.1.4 | 9.1.5 |

CHƯƠNG 3

HƯỚNG DẪN THỰC THI BẢO ĐẢM AN TOÀN THÔNG TIN

# 1. Hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ cho TTDL phục vụ CPĐT

## 1.1. Xác định các chủ thể liên quan

a) Chủ quản hệ thống thông tin

Chủ quản hệ thống thông tin được xác định căn cứ quy định tại Điều 5 Thông tư số 03/2017/TT-BTTTT ngày 24/04/2017.

Đối với TTDL thì chủ quản hệ thống thông tin là cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống TTDL.

Đối với cơ quan, tổ chức thuê ngoài dịch vụ CNTT thì chủ quản hệ thống thông tin là cấp có thẩm quyền phê duyệt dự án thuê dịch vụ CNTT.

b) Đơn vị vận hành

Đơn vị vận hành hệ thống thông tin được xác định căn cứ quy định tại Điều 6 Thông tư số 03/2017/TT-BTTTT ngày 24/04/2017.

## 1.2. Hồ sơ đề xuất cấp độ

Việc lập, thẩm định và phê duyệt HSĐXCĐ được hướng dẫn chi tiết tại Công văn số 713/CATTT-TĐQLGS ngày 25/7/2019. Đối tượng yêu cầu xây dựng HSĐXCĐ cho TTDL phục vụ CPĐT bao gồm:

a) Cơ quan chủ quản của TTDL phục vụ CPĐT phải xây dựng HSĐXCĐ cho TTDL thuộc phạm vi quản lý. Cấp độ của TTDL được xác định dựa vào cấp độ cao nhất của các hệ thống thông tin được triển khai trên đó. Trường hợp, TTDL được thiết lập mới thì cấp độ của TTDL được xác định dựa vào mục đích kinh doanh là TTDL này sẽ được xây dựng để cung cấp dịch vụ cho hệ thống thông tin cấp độ cao nhất là cấp độ nào.

b) Cơ quan, tổ chức thuê ngoài dịch vụ CNTT phải xây dựng HSĐXCĐ cho hệ thống thông tin được triển khai trên hệ thống TTDL phục vụ CPĐT. Thuyết minh phương án bảo đảm an toàn thông tin trong HSĐXCĐ của bên thuê ngoài dịch vụ CNTT được kế thừa từ HSĐXCĐ của TTDL phục vụ CPĐT mà không cần thuyết minh lại, chỉ thuyết minh các phương án bổ sung nếu chưa được đưa ra trong HSĐXCĐ của TTDL.

## 1.3. Phương án bảo đảm an toàn thông tin

Phương án bảo đảm an toàn thông tin được xác định dựa vào cấp độ đề xuất của hệ thống. Căn cứ vào cấp độ của hệ thống thì phương án bảo đảm an toàn thông tin được xác định theo quy định tại Thông tư số 03/2017/TT-BTTTT và hướng dẫn chi tiết tại Tiêu chuẩn quốc gia TCVN 11930:2017.

Phương án bảo đảm an toàn thông tin cho TTDL phục vụ CPĐT cần được triển khai và đáp ứng đầy đủ các yêu cầu trước khi cung cấp cho bên thuê ngoài dịch vụ CNTT.

Như đã hướng dẫn ở trên, phương án bảo đảm an toàn thông tin cho hệ thống thông tin của bên thuê ngoài dịch vụ CNTT có thể tham chiếu, kế thừa phương án bảo đảm an toàn thông tin được thuyết minh trong HSĐXCĐ của TTDL phục vụ CPĐT đã được phê duyệt.

Hướng dẫn chi tiết liên quan đến thuyết minh phương án bảo đảm an toàn thông tin tại Công văn số 713/CATTT-TĐQLGS ngày 25/7/2019 về ban hành hướng dẫn xác định và thực thi bảo đảm an toàn hệ thống thông tin theo cấp độ.

# 2. Hướng dẫn thực hiện kiểm tra, đánh giá an toàn thông tin cho TTDL phục vụ CPĐT

Cơ quan, tổ chức vận hành TTDL phục vụ CPĐT phải thực hiện kiểm tra, đánh giá an toàn thông tin theo quy định tại Thông tư 03/2017/TT-BTTTT. Trong đó, nội dung kiểm tra, đánh giá bao gồm: (1) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ; (2) Đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin; (3) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

# 3. Hướng dẫn giám sát an toàn thông tin cho TTDL phục vụ CPĐT

Hoạt động, phương án giám sát an toàn thông tin cho TTDL phục vụ CPĐT phải tuân thủ các quy định tại Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin và hướng dẫn chi tiết tại Công văn số 2973/BTTTT-CATTT ngày 04/9/2019.

# 4. Hướng dẫn xây dựng phương án ứng cứu sự cố an toàn thông tin mạng cho TTDL phục vụ CPĐT

Phương án ứng cứu sự cố an toàn thông tin mạng cho TTDL phục vụ CPĐT phải đáp ứng các yêu cầu được quy định tại Điều 16, Quyết định số 05/2017/NĐ-CP ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia và Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017.

# 5. Hướng dẫn bảo đảm an toàn thông tin cho TTDL phục vụ CPĐT khi kết nối vào mạng TSLCD

Trung tâm dữ liệu phục vụ CPĐT khi kết nối vào mạng TSLCD phải đáp ứng các yêu cầu an toàn theo quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ và các yêu cầu cụ thể tại Điều 1, khoản 5 và Phụ lục 1 Thông tư số 12/2019/TT-BTTTT và hướng dẫn của Bộ Thông tin và Truyền thông tại Công văn số 1694/BTTTT-CATTT ngày 31/5/2019.