|  |
| --- |
| ỦY BAN NHÂN TỈNH HẢI DƯƠNG **TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**  **HỒ SƠ ĐỀ XUẤT CẤP ĐỘ 3**  **TRUNG TÂM TÍCH HỢP DỮ LIỆU TỈNH HẢI DƯƠNG**    **Hải Dương - 2023** |

**MỤC LỤC**

[**THUẬT NGỮ, TỪ VIẾT TẮT 1**](#_Toc136804115)

[**PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN 2**](#_Toc136804116)

[1. Thông tin Chủ quản hệ thống thông tin 2](#_Toc136804117)

[2. Thông tin Đơn vị vận hành 2](#_Toc136804118)

[3. Mô tả phạm vi, quy mô của hệ thống 2](#_Toc136804119)

[4. 1. Mô hình logic tổng thể 4](#_Toc136804120)

[4. 2. Mô hình kết nối vật lý 5](#_Toc136804121)

[4. 3. Danh mục thiết bị sử dụng trong hệ thống 5](#_Toc136804122)

[4. 4. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống 10](#_Toc136804123)

[4. 5. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống 12](#_Toc136804124)

[**PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT** 13](#_Toc136804125)

[1. Danh mục hệ thống thông tin và cấp độ đề xuất 13](#_Toc136804126)

[2. Thuyết minh đề xuất cấp độ đối với hệ thống thông tin 13](#_Toc136804127)

[2. 1. Hệ thống cổng thông tin điển tử 13](#_Toc136804128)

[2. 2. Hệ thống LGSP 14](#_Toc136804129)

[Hệ thống liên thông các hệ thống thông tin và ứng dụng quản lý, cung cấp dịch vụ công trực tuyến tỉnh Hải Dương. 14](#_Toc136804130)

[2. 3. Hệ thống giao ban trực tuyến 14](#_Toc136804131)

[**PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN** 15](#_Toc136804132)

[**PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN ĐÁP ỨNG YÊU CẦU QUẢN LÝ BẢO ĐẢM AN TOÀN THÔNG TIN** 18](#_Toc136804133)

[1. Thiết lập chính sách an toàn thông tin 18](#_Toc136804134)

[1. 1. Chính sách an toàn thông tin 18](#_Toc136804135)

[1. 2. Xây dựng và công bố 24](#_Toc136804136)

[1. 3. Rà soát, sửa đổi 25](#_Toc136804137)

[2. Tổ chức bảo đảm an toàn thông tin 25](#_Toc136804138)

[2. 1. Đơn vị chuyên trách về an toàn thông tin 25](#_Toc136804139)

[2. 2. Phối hợp với những cơ quan/tổ chức có thẩm quyền 26](#_Toc136804140)

[3. Bảo đảm nguồn nhân lực 29](#_Toc136804141)

[3. 1. Tuyển dụng 29](#_Toc136804142)

[3. 2. Trong quá trình làm việc 29](#_Toc136804143)

[3. 3. Chấm dứt hoặc thay đổi công việc 32](#_Toc136804144)

[4. Quản lý thiết kế, xây dựng hệ thống thông tin 33](#_Toc136804145)

[4. 1. Thiết kế an toàn hệ thống thông tin 33](#_Toc136804146)

[4. 2. Phát triển phần mềm thuê khoán 36](#_Toc136804147)

[4. 3. Thử nghiệm và nghiệm thu hệ thống 37](#_Toc136804148)

[5. Quản lý vận hành hệ thống thông tin 38](#_Toc136804149)

[5. 1. Quản lý an toàn mạng 38](#_Toc136804150)

[5. 2. Quản lý an toàn máy chủ và ứng dụng 44](#_Toc136804151)

[5. 3. Quản lý an toàn dữ liệu 47](#_Toc136804152)

[5. 4. Quản lý an toàn thiết bị đầu cuối 48](#_Toc136804153)

[5. 5. Quản lý phòng chống phần mềm độc hại 50](#_Toc136804154)

[5. 6. Quản lý giám sát an toàn hệ thống thông tin 51](#_Toc136804155)

[5. 7. Quản lý điểm yếu an toàn thông tin 55](#_Toc136804156)

[5. 8. Quản lý sự cố an toàn thông tin 58](#_Toc136804157)

[5. 9. Quản lý an toàn người sử dụng đầu cuối 62](#_Toc136804158)

[**PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT CẤP ĐỘ 3** 65](#_Toc136804159)

[1. Bảo đảm an toàn mạng 65](#_Toc136804160)

[1. 1. Thiết kế hệ thống 65](#_Toc136804161)

[1. 2. Kiểm soát truy cập từ bên ngoài mạng 68](#_Toc136804162)

[1. 3 Kiểm soát truy cập từ bên trong mạng 69](#_Toc136804163)

[1. 4. Nhật ký hệ thống 69](#_Toc136804164)

[1. 5. Phòng chống xâm nhập 70](#_Toc136804165)

[1. 6. Phòng chống phần mềm độc hại trên môi trường mạng 70](#_Toc136804166)

[1. 7. Bảo vệ thiết bị hệ thống 71](#_Toc136804167)

[2. Bảo đảm an toàn máy chủ 72](#_Toc136804168)

[2. 1. Xác thực 72](#_Toc136804169)

[2. 2. Kiểm soát truy cập 75](#_Toc136804170)

[2. 3. Nhật ký hệ thống 77](#_Toc136804171)

[2. 4. Phòng chống xâm nhập 81](#_Toc136804172)

[2. 5. Phòng chống phần mềm độc hại 83](#_Toc136804173)

[2. 6. Xử lý máy chủ khi chuyển giao 86](#_Toc136804174)

[3. Bảo đảm an toàn ứng dụng 86](#_Toc136804175)

[3. 1. Xác thực 86](#_Toc136804176)

[3. 2. Kiểm soát truy cập 87](#_Toc136804177)

[3. 3. Nhật ký hệ thống 88](#_Toc136804178)

[3. 4. Bảo mật thông tin liên lạc 88](#_Toc136804179)

[3. 5. Chống chối bỏ 88](#_Toc136804180)

[3. 6. An toàn ứng dụng và mã nguồn 89](#_Toc136804181)

[4. Bảo đảm an toàn dữ liệu 89](#_Toc136804182)

[4. 1. Nguyên vẹn dữ liệu 89](#_Toc136804183)

[4. 2. Bảo mật dữ liệu 89](#_Toc136804184)

[4. 3. Sao lưu dự phòng 90](#_Toc136804185)

# THUẬT NGỮ, TỪ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| **STT** | **Từ viết tắt** | **Nghĩa đầy đủ** |
|  | CNTT | Công nghệ thông tin |
|  | CSDL | Cơ sở dữ liệu |
|  | HTTT | Hệ thống thông tin |
|  | TTDL | Trung tâm dữ liệu |
|  | ATTT | An toàn thông tin |
|  | SỞ TT&TT | Sở Thông tin và Truyền thông |
|  | CNTT&TT | Công nghệ Thông tin và Truyền thông |
|  | MCĐT | Một cửa điện tử |
|  | WAN | Mạng tin học diện rộng |
|  | LAN | Mạng nội bộ |
|  | TSLCD | Mạng Truyền số liệu chuyên dùng |
|  | VPN | Vitural Private Network |
|  | DNS | Domain Name Server |

**PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN**

## 1. Thông tin chủ quản hệ thống thông tin

## - Tên đơn vị: UBND Tỉnh Hải Dương

## - Người đại diện: Triệu Thế Hùng Chức vụ: Chủ Tịch.

## - Trụ sở chính: Số 45 Quang Trung, TP Hải Dương, tỉnh Hải Dương

## - Thông tin liên hệ:

## + Điện thoại: 0220.3837 444 Fax: 0220.3853 601

## + Website: <http://haiduong.gov.vn>

**2. Thông tin Đơn vị vận hành**

- Tên tổ chức: Trung tâm Công nghệ thông tin và Truyền thông

- Số quyết định quy định chức năng, nhiệm vụ và quyền hạn: Quyết định số 1364/QĐ-UBND ngày 28/5/2010 của UBND tỉnh Hải Dương về việc việc sáp nhập Trung tâm Tin học Văn phòng UBND tỉnh vào Trung tâm Công nghệ Thông tin và Truyền thông thuộc Sở Thông tin và Truyền thông.

- Người đại diện: Ông **Hà Tuấn Giang**, Chức vụ: Giám đốc Trung tâm

- Địa chỉ: Số 1 Đức Minh, Phường Thanh Bình, Thành phố Hải Dương, Tỉnh Hải Dương.

- Điện thoại liên hệ: 02203897373

- Thư điện tử: trungtamcntt@haiduong.gov.vn

**3. Mô tả phạm vi, quy mô của hệ thống**

- Phạm vi, quy mô của Hệ thống: Trung tâm tích hợp dữ liệu tỉnh Hải Dương (TTTHDL tỉnh Hải Dương) là nơi tích hợp hệ thống chuyên dụng, bao gồm cả phần cứng (các hệ thống máy chủ, các hệ thống sao lưu trữ dữ liệu, hệ thống lưu nguồn điện dự phòng) và các chương trình phần mềm dùng chung toàn tỉnh. Trung tâm dữ liệu là hạ tầng kỹ thuật phục vụ cho ứng dụng công nghệ thông tin trong hoạt động của các cơ quan nhà nước thuộc UBND tỉnh Hải Dương ~~và có thể~~ hỗ trợ cung cấp dịch vụ cho các tổ chức, công dân.

- Phạm vi, quy mô của hạ tầng kỹ thuật trung tâm dữ liệu: Thiết lập để phục vụ công tác chỉ đạo điều hành và lưu trữ dữ liệu của tỉnh Hải Dương.

- Đối tượng phục vụ của hệ thống: Cơ quan, tổ chức, công dân, doanh nghiệp trên địa bàn tỉnh Hải Dương.

- Danh mục các hệ thống thông tin thành phần/các dịch vụ được cung cấp bởi trung tâm tích hợp dữ liệu:

+ Hạ tầng Trung tâm THDL tỉnh Hải Dương.

+ Cổng Thông tin điện tử tỉnh Hải Dương.

+ Cổng thông tin điện tử của ….. Sở, ngành gồm: ……

+ Hệ thống thư điện tử công vụ tỉnh Hải Dương.

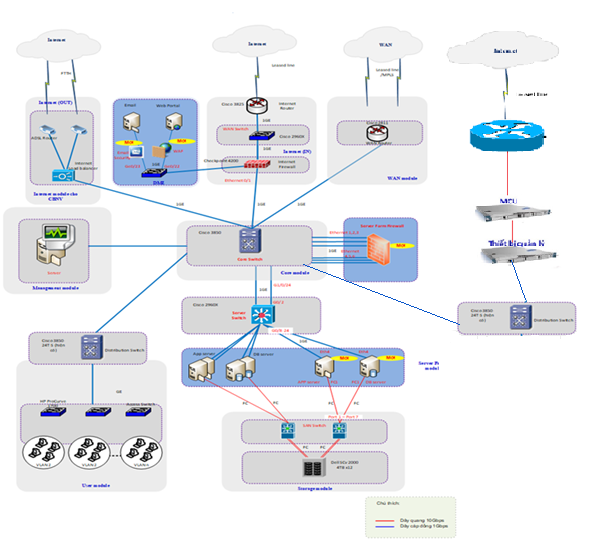
+ Hệ thống thông tin giải quyết thủ tục hành chính tỉnh Hải Dương.

**+** Hệ thống Giao ban trực tuyến tỉnh Hải Dương.

+ Hệ thống nền tảng tích hợp, chia sẻ dữ liệu tỉnh Hải Dương (LGSP tỉnh Hải Dương).

**Mô tả cấu trúc của hệ thống**

**4. 1. Mô hình logic tổng thể**

****

Hình 1. Cấu trúc logic của Trung tâm dữ liệu

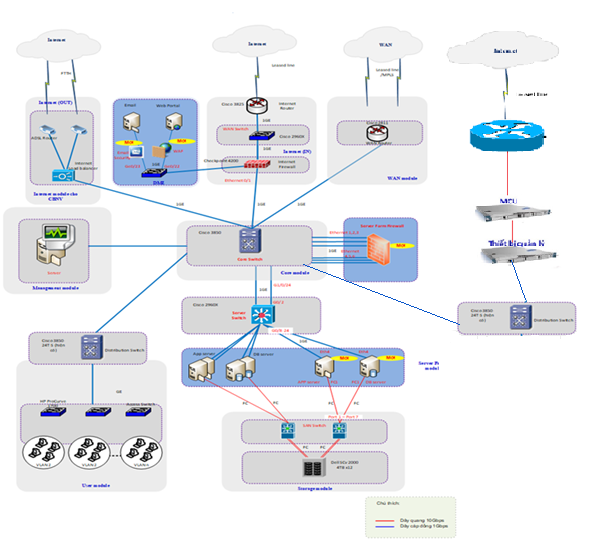
Các vùng mạng được thiết kế như sau:

- Vùng mạng user module là dùng cho người dùng trong cơ quan. Các máy được kết nối qua các Access switch, core switch 3850, wan router 2811 ra ngoài internet.

-Vùng máy chủ cơ sở dữ liệu đặt các máy chủ cài đặt cơ sở dữ liệu phục vụ việc lưu trữ và quản lý cơ sở dữ liệu tập trung trên hệ thống. Vùng này gồm có San scv 2000, san switch, máy chủ Dell, server switch, core switch, Firewall fortinet (bảo vể ứng dụng web), Firewall checkpoint 4200.

- Vùng mạng DMZ gồm các máy ứng dụng Cổng thông tin, website các sở ban ngành và các ứng dụng lưu trữ khác. Mạng này triển khái các thiết bị phòng chống xâm nhập IP, thiết bị Web Application Firewall.

**4. 2. Mô hình kết nối vật lý**

****

Hình 2. Kết nối vật lý của Trung tâm dữ liệu

**4. 3. Danh mục thiết bị sử dụng trong hệ thống**

| **STT** | **Tên thiết bị/Chủng loại** | **Vị trí triển khai** | **Mục đích sử dụng** |
| --- | --- | --- | --- |
|  | Core Switch: Cisco 3825 | Vùng nội bộ | Phân vùng mạng |
|  | Core Switch: Cisco 2811 | Vùng nội bộ | Truy cập internet |
|  | Switch 24 port: Cisco SRW224p | Vùng nội bộ | Phân vùng mạng |
|  | Tủ Rack 42U | Phòng máy chủ | Chứa các thiết bị |
|  | Máy chủ hiệu năng cao xử lý  Dell Power Edge R730  (2 CPU 6 core/ 32 GB Ram):  + Processor: 2 x Intel Xeon E5-2630 v3 (2. 4GHz, 20M Cache, 8Core) + Memory: 4 x 16GB RDIMM, 2133 MT/s + HDD: 2 x 600GB 10K RPM SAS 12Gbps 2. 5in Hot-plug Hard Drive | Vùng DMZ cổng | Xử lý dữ liệu hiển thị cho người dùng |
|  | Máy chủ hiệu năng cao DB  Dell Power Edge R730  + Processor: 2 x Intel Xeon E5-2630 v3 (2. 4GHz, 20M Cache, 8Core)  + Memory: 4 x 16GB RDIMM, 2133 MT/s  + HDD: 2 x 600GB 10K RPM SAS 12Gbps 2. 5in Hot-plug Hard Drive  + HBA Card: QLogic 2560, Single Port 8Gb Optical Fibre Channel HBA. | Vùng core cổng | Lữu trữ dữ liệu |
|  | Core Switch (Sử dụng cho trung tâm dữ liệu): Cisco WS-C3850-24T-S  - Cấu hình kỹ thuật: Stackable 24 x 10/100/1000 Ethernet ports, with 350WAC power supply 1 RU, IP Base feature set | Vùng mạng nội bộ | Phân vùng mạng Lan nội bộ |
|  | Switch cho máy chủ: Cisco WS-C2960X-24TS-L  Interfaces: 24 x 10/100/1000 Ethernet Ports, 4 x 1G SFP  Memory: 512 MB for LAN Base | Vùng mạng nội bộ | Phân vùng mạng Lan nội bộ |
|  | Hệ thống lưu trữ (SAN): Dell SCv2000  Processor: Intel™ Xeon™ 4-core  Memory: 8GB  Maximum Drives: 168  Total storage capacity: 1008TB | Vùng core cổng | Lưu trữ dữ liệu |
|  | SAN Switch: Brocade 300 Ports-On-Demand 8Gb FC Switch  Cổng FC : 8-device port Fibre Channel Switch với 8 active ports | Vùng core cổng | Phân vùng dữ liệu trong vùng |
|  | KVM: 16 Port Keyboard / Video / Mouse Analog Switch: Dell DAV2216-G01; monitor: Dell 18. 5in LED KMM DKMMLED185-00  - Kiểu dáng (Form Factor): 1U Rack  - KVM Swith: Dell DAV2216-G01: 16 Port Analog Switch  - Server interface moduel for VGA, USB keyboard, mouse: 16 chiếc | Quản lý các máy farm cổng | Điều khiển các máy vùng DMZ và vùng core |
|  | Switch for management workstation: Plannet GSW – 2401  Cổng kết nối: 24 port | Phân vùng quản lý cổng | Phân vùng điều khiển các máy của hệ thống cổng |
|  | Thiết bị Firewall: Checkpoint 4200 Next Generation Threat Prevention Appliance  - Interfaces: 4 x 10/100/1000 copper  - Max Firewall Throughput: 3 Gbps, 1518 byte UDP  - Storage: 250 GB | Vùng cổng thông tin | Phân vùng mạng core, dmz |
|  | Hệ thống UPS:  UPS EATON 9155  - Output Power Capacity: Rating (VA/W) 15kVA/12kW, Full load 15 phút;  - Nominal Output Voltage: 230V  - Input voltage range for main operations: 160 - 280V  - Maximum Input Current : 115A | Vùng cổng thông tin | Cung cấp điện lưới ổn định cho cả trung tâm tích hợp dữ liệu |
|  | Bình Ắc quy dùng cho bộ lưu điện Thông số kỹ thuật như sau:  + Chủng loại: OUTDO/OT40-12  + Điện áp: 12V  + Dung lượng: 40 Ah  + Loại: Ắc quy không phải bảo trì, chuyên dùng cho bộ lưu điện (UPS) | Vùng cổng thông tin | Chuyên dùng cho bộ lưu điện (UPS) |
|  | Máy phát điện Cummins C33D5 33kVA Generator  **-** Công suất phát dự phòng: 33 KVA  - Công suất phát liên tục: 30 KVA  **-** Điện áp: 220VA/380VA; xoay chiều; 3 pha; 50Hz  - Loại động cơ: 4 kỳ  - Số lượng xi lanh: 4 xi lanh  **-** Hệ thống khởi động: Khởi động bằng điện một chiều 12V hoặc 24 V  - Hệ thống làm mát: Bằng nước và quạt gió  - Nhiên liệu: Diezel  **-** Tủ Atomation Transfer System (ATS) cho máy phát 30kVA  - Khung sắt để máy phát | Vùng cổng thông tin | Chuyên cung cấp điện cho trung tâm tích hợp dữ liệu khi mất điện |
|  | Tủ Rack 42U: APC AR3100 42U |  |  |
|  | Máy chủ HPE DL360 Gen10  HPE DL360 Gen10 Xeon-G 5115 (2. 4GHz /10 core / 13. 75 MB Cache), 2 x HPE 600GB SAS 10K SFF SC DS HDD 2. 5in Hard Drive, 128GB RAM. | Phần core LGSP | Cung cấp ứng dụng trục LGSP |
|  | Máy chủ HPE DL360 Gen10  HPE DL360 Gen10 Xeon-G 5115 (2. 4GHz/10 core/13. 75 MB Cache), 2 x HPE 600GB SAS 10K SFF SC DS HDD 2. 5in Hard Drive, 64GB RAM. | Phần core LGSP | Cung cấp ứng dụng LGSP |
|  | Firewall FortiGate 301E | Vùng LGSP | Bảo vệ dữ liệu trục LGSP |
|  | Firewall FortiMail 400E | Vùng Email công vụ | Bảo vệ dữ liệu cho ứng dụng Mail |
|  | Firewall FortiWeb 400D | Vùng Cổng thông tin điện tử và các trang thành phần | Bảo vệ cho ứng dụng Web |
|  | Thiết bị chuyển mạch trung tâm Core Switch: C9300-24T-E | Vùng LGSP | Phân vùng mạng LGSP |
|  | Thiết bị access cho máy chủ Server Switch: C9200-24T-E | Vùng LGSP | Phân vùng mạng |
|  | Thiết bị cân bằng tải cho máy chủ Load Balancing: FortiADC-300F |  | Cân bằng tải cho đường truy cập ứng dụng trên LGSP |
|  | Hệ thống lưu điện (UPS) 15KVA: APC Smart-UPS RT 15kVA | Vùng trục LGSP | Cung cấp điện cho trục LSGP |
|  | Máy chủ HPE ProLiant DL360 Gen10  + 2 x HPE DL360 Gen10 Xeon-G 5115 (2. 4GHz/10 core/13. 75 MB Cache);  + 4 x 32GB Dual Rank x4 DDR4-2666, hỗ trợ mở rộng tới 3TB, hỗ trợ 24 khe cắm RAM  + 2 x HPE 600GB SAS 10K SFF SC DS HDD 2. 5in Hard Drive | Vùng LGSP | Triển khai phần mềm ứng dụng |
|  | Máy chủ HPE ProLiant DL360 Gen10  **+** 2 x HPE DL360 Gen10 Xeon-G 5115 (2. 4GHz/10 core/13. 75 MB Cache);  + 2 x 32GB Dual Rank x4 DDR4-2666, hỗ trợ mở rộng tới 3TB, hỗ trợ 24 khe cắm RAM  **+** 2 x HPE 600GB SAS 10K RPM HDD 2. 5in Hard Drive | Vùng LGSP | Triển khai phần mềm ứng dụng |
|  | SAN Switch: Cisco C9148S |  |  |
|  | Bộ thiết bị điều khiển đa điểm MCU chuyên dụng (Cisco Meeting Server 1000 Bundle): CTI-CMS-1000-M5-K9 | Vùng Giao ban | Phục vụ họp trực tuyến |
|  | Thiết bị phần cứng điều khiển cuộc gọi quản lý MCU (Cisco Business Edition 6000H Svr, Export Restricted SW) | Vùng giao ban | Phục vụ họp trực tuyến |

**4. 4. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Máy chủ / Ứng dụng cài đăt / Vùng mạng / HĐH** | **Mục đích sử dụng** |
|  | Hệ thống cổng thông tin điện tử tỉnh và các cổng thông tin điện tử sở ban ngành, tổ chức | Cài hệ thống Farm:  02 server AD, 2 server DB, 1 App-web nối VLAN1 là vùng core.  02 front web, 1 server Dotnet ALL IN ONE nối VLAN2 là vùng DMZ | Cung cấp và lưu trữ thông tin của Cổng TTĐT tỉnh, sở ban ngành, tổ chức |
|  | Hệ thống nền tảng tích hợp, chia sẻ dữ liệu tỉnh Hải Dương (LGSP tỉnh Hải Dương). | 04 máy chủ HPE ProLiant DL360 Gen10 vật ý | Liên thông dữ liệu và quản lý ứng dùng chung, cung cấp dịch vu công trực tuyến. |
|  | Giao ban trực tuyến | 02 Thiết bị MCU chuyên dụng | Kết nối các điểm cầu họp hội nghị trực tuyến. |
|  | Hệ thống thư điện tử công vụ tỉnh Hải Dương | 03 máy chủ Dell Power Edge R730 | Cung cấp và lưu trữ thông tin của Hệ thống thư điện tử công vụ tỉnh Hải Dương |
|  | Hệ thống dịch vụ công trực tuyến tỉnh Hải Dương | Cung cấp và lưu trữ thông tin Hệ thống dịch vụ công trực tuyến tỉnh Hải Dương |

*Bảng 1. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống*

**4. 5. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Vùng mạng** | **IP Private** | **IP Public** |
|  | Vùng Cổng TTĐT | 10. 30. 1. 0/24 | 113. 160. 212 (17-22) |
|  | Vùng Thư điện tử công vụ | 10. 30. 1. 0/24 | 113. 160. 212 (17-22) |
|  | Vùng Dịch vụ công trực tuyến | 10. 30. 1. 0/24 | 113. 160. 212 (17-22) |
|  | Vùng giao ban | 10. 88. x. 10/24 | 202. 191. z. 0/24 |
|  | Vùng LGSP | 172. 16. 30. x/24 | 123. 25. 60. (1-7) |
|  | Vùng mạng nội bộ | 192. 168. 1. 0/254 | Cấp phát động (DHCP) |

*Bảng 2. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống*

**PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT**

**1. Danh mục hệ thống thông tin và cấp độ đề xuất**

Hệ thống thông tin của Đơn vị vận hành bao gồm các hệ thống thành phần với cấp độ đề xuất tương ứng, bao gồm:

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Hệ thống** | **Cấp độ đề xuất** | **Căn cứ đề xuất** |
|  | Hạ tầng Trung tâm THDL tỉnh Hải Dương | 3 | Khoản 3/Điều 9/NĐ85 |
|  | Cổng Thông tin điện tử tỉnh Hải Dương | 3 | Khoản 2/Điều 9/NĐ85 |
|  | Hệ thống thư điện tử công vụ tỉnh Hải Dương | 3 | Khoản 3/Điều 9/NĐ85 |
|  | Hệ thống dịch vụ công trực tuyến tỉnh Hải Dương | 3 | Khoản 2/Điều 9/NĐ85 |
|  | Hệ thống Giao ban trực tuyến tỉnh Hải Dương | 3 | Khoản 3/Điều 9/NĐ85 |
|  | Hệ thống nền tảng tích hợp, chia sẻ dữ liệu tỉnh Hải Dương (LGSP tỉnh Hải Dương). | 3 | Khoản 2/Điều 9/NĐ85 |

**2. Thuyết minh đề xuất cấp độ đối với các hệ thống thông tin**

**2.1. Hạ tầng Trung tâm THDL tỉnh Hải Dương**

Hạ tầng trung tâm tích hợp dữ liệu tỉnh Hải Dương gồm tập hợp các thiết bị máy chủ, lưu trữ, thiết bị mạng, thiết bị an toàn thông tin bảo mật, đường truyền... sử dụng chung cho hệ thống ứng dụng của các cơ quan nhà nước trong tỉnh. Căn cứ theo Khoản 3/Điều 9/NĐ85, hệ thống được đề xuất cấp độ 3.

**2.2. Hệ thống Cổng thông tin điển tử của tỉnh**

Đây là hệ thống thông tin phục vụ công tác chỉ đạo, điều hành của lãnh đạo UBND tỉnh, có cung cấp thông tin phục cụ người dân và doanh nghiệp. Căn cứ theo Khoản 2/Điều 9/NĐ85, hệ thống được đề xuất cấp độ 3.

**2.3. Hệ thống thư điện tử công vụ tỉnh Hải Dương**

Đây là hệ thống thông tin phục vụ công tác chỉ đạo, điều hành của các Sở, ban ngành, UBND các huyện, thành phố, thị xã, các xã phường trên địa bàn tỉnh. Căn cứ theo Khoản 3/Điều 9/NĐ85, hệ thống được đề xuất cấp độ 3.

**2.4. Hệ thống dịch vụ công trực tuyến tỉnh Hải Dương**

Đây là hệ thống phục vụ người dân, doanh nghiệp trên toàn địa bàn tỉnh, số lượng trên 10.000 người. Căn cứ theo Điểm c Khoảng 2 Điều 9 của Nghị định số 85/2016/NĐ-CP, hệ thống này được đề xuất cấp độ 3.

**2.5. Hệ thống Giao ban trực tuyến tỉnh Hải Dương**

Đây là hệ thống thông tin được thiết lập từ cấp tỉnh đến cấp huyện, thành phố, thị xã, xã, phường, nhằm phục vụ sự lãnh đạo, chỉ đạo của UBND tỉnh đến các UBND các huyện, thành phố, thị xã, xã, phường, trên địa bàn tỉnh; giúp quá trình lãnh đạo, điều hành một cách nhanh chóng, kịp thời, giảm thiểu thời gian và công sức đi lại. Căn cứ theo Khoản 3/Điều 9/NĐ85, hệ thống được đề xuất cấp độ 3.

**2.6 Hệ thống LGSP tỉnh Hải Dương**

Hệ thống LGSP tỉnh Hải Dương: là hệ thống thông tin phục vụ chia sẻ, kết nối các phần mềm, ứng dụng phục vụ người dân, doanh nghiệp trên toàn địa bàn tỉnh. Căn cứ theo Điểm c Khoảng 2 Điều 9 Nghị định số 85/2016/NĐ-CP, hệ thống này được đề xuất cấp độ 3.

**PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM** **AN TOÀN HỆ THỐNG THÔNG TIN**

**Thuyết minh phương án về quản lý bao gồm các nội dung sau:**

1. Thiết lập chính sách an toàn thông tin

2. Tổ chức bảo đảm an toàn thông tin

3. Bảo đảm nguồn nhân lực

4. Quản lý thiết kế, xây dựng hệ thống

5. Quản lý vận hành hệ thống

- 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 giám sát an toàn hệ thống thông tin

- Quản lý điểm yếu an toàn thông tin

- Quản lý sự cố an toàn thông tin

- Quản lý an toàn người sử dụng đầu cuối.

Đối với những yêu cầu quản lý chưa đáp ứng các yêu cầu an toàn trong Thuyết minh này, Đơn vị vận hành – Trung tâm Công nghệ thông tin và Truyền thông sẽ cập nhật, bổ sung trình Chủ quản hệ thống thông tin ban hành trong vòng 12 tháng, kể từ khi HSĐXCĐ được phê duyệt.

**Thuyết minh phương án về kỹ thuật bao gồm các nội dung:**

**1. Bảo đảm an toàn mạng**

1.1. Thiết kế hệ thống

1.2. Kiểm soát truy cập từ bên ngoài mạng

1.3. Kiểm soát truy cập từ bên trong mạng

1.4. Nhật ký hệ thống

1.5. Phòng chống xâm nhập

1.6. Phòng chống phần mềm độc hại trên môi trường mạng

1.7. Bảo vệ thiết bị hệ thống

**2. Bảo đảm an toàn máy chủ**

2.1. Xác thực

2.2. Kiểm soát truy cập

2.3. Nhật ký hệ thống

2.4. Phòng chống xâm nhập

2.5. Phòng chống phần mềm độc hại

2.6. Xử lý máy chủ khi chuyển giao

**3. Bảo đảm an toàn ứng dụng**

3.1. Xác thực

3.2. Kiểm soát truy cập

3.3. Nhật ký hệ thống

3.4. Bảo mật thông tin liên lạc

3.5. Chống chối bỏ

**4. Bảo đảm an toàn dữ liệu**

4.1. Nguyên vẹn dữ liệu

4.2. Bảo mật dữ liệu

4.3. Sao lưu dự phòng

Đối với các yêu cầu kỹ thuật chưa đáp ứng yêu cầu an toàn cơ bản trong Thuyết minh này, Đơn vị vận hành sẽ triển khai nâng cấp, thiết lập cấu hình hệ thống để đáp ứng yêu cầu trong vòng 12 tháng, kể từ khi HSĐXCĐ được phê duyệt.

Thuyết minh phương án bảo đảm an toàn thông tin về quản lý được thuyết minh chung tại Phụ lục I.

Thuyết minh phương án bảo đảm an toàn thông tin về kỹ thuật theo cấp độ 3 tại Phụ lục II.

Trên cơ sở đó, thuyết minh phương án bảo đảm ATTT cho các hệ thống thông tin tại Trung tâm tích hợp dữ liệu của tỉnh Hải Dương sẽ bao gồm các nội dung sau:

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Hệ thống** | **Cấp độ đề xuất** | **Nội dung thuyết minh** |
| 1 | Thuyết minh phương án đáp ứng yêu cầu quản lý | 3 | Phụ lục I |
| 2 | Thuyết minh phương án đáp ứng yêu cầu kỹ thuật | 3 | Phụ lục II |

# PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN ĐÁP ỨNG YÊU CẦU QUẢN LÝ BẢO ĐẢM AN TOÀN THÔNG TIN

## 1. Thiết lập chính sách an toàn thông tin

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

|  |  |
| --- | --- |
| **Yêu cầu 01** | Xác định các mục tiêu, nguyên tắc bảo đảm ATTT. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Áp dụng QĐ 29/2013/QĐ-UBND ngày 11/12/2013, Quy chế bảo đảm ATTT, TT-CNTT&TT có phương án quy định về việc xác định các mục tiêu, nguyên tắc đảm bảo an toàn, an ninh thông tin như sau:  1. Tổ chức hệ thống mạng phù hợp để tăng cường tính bảo mật. Các cơ quan, đơn vị có nhiều phòng, ban, đơn vị trực thuộc không nằm trong cùng một khu vực, cần thiết lập mạng riêng ảo để bảo đảm an ninh cho mạng nội bộ. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin, hạn chế sử dụng các chức năng, cổng giao tiếp, giao thức và dịch vụ mạng không cần thiết.  2. Đối với việc lắp đặt mạng không dây để kết nối với mạng nội bộ, cần thiết lập, cấu hình các thông số, đặt mật khẩu và thường xuyên thay đổi mật khẩu nhằm bảo đảm công tác bảo mật.  3. Trang bị thiết bị chuyển mạch bảo đảm khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng.  4. Trang bị, cài đặt tường lửa bảo đảm khả năng xử lý được số lượng kết nối đồng thời cao và chịu được thông lượng cao, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu, cung cấp đầy đủ các cơ chế bảo mật, quản lý luồng dữ liệu ra vào và có khả năng bảo vệ hệ thống thông tin trước các loại tấn công từ chối dịch vụ; trang bị thiết bị phát hiện hoặc phòng chống xâm nhập trái phép.  5. Bố trí phòng máy chủ độc lập, bảo đảm khô, thoáng, nguồn điện cung cấp ổn định cao, được trang bị máy điều hòa nhiệt độ và cho vận hành liên tục, được lắp đặt thiết bị chống sét và hệ thống phòng cháy chữa cháy. Phòng máy chủ được giao cho cán bộ có chuyên môn về công nghệ thông tin trực tiếp quản lý, các cán bộ không liên quan không được vào phòng máy chủ.  6. Cài đặt các phần mềm hệ điều hành, phần mềm ứng dụng, phần mềm quản trị cơ sở dữ liệu, phần mềm chống vi-rút máy tính có bản quyền trên các máy chủ, máy trạm, các thiết bị, phương tiện kỹ thuật trong hệ thống mạng; cài đặt các phần mềm tiện ích để đánh giá, tìm kiếm các lỗ hổng bảo mật.  7. Tạo tài khoản và phân quyền người dùng để truy nhập hệ thống thông tin; yêu cầu người dùng đặt mật khẩu với độ an toàn cao; thiết lập giới hạn một số hữu hạn lần đăng nhập sai liên tiếp vào hệ thống thông tin, nếu liên tục đăng nhập sai vượt quá số lần quy định thì hệ thống thông tin phải tự động khóa tài khoản hoặc cô lập tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập.  8. Cấu hình hệ thống thông tin bảo đảm ghi nhận đầy đủ các thông tin, sự kiện trong các bản ghi nhật ký hệ thống thông tin; lưu giữ nội dung nhật ký hệ thống thông tin trong khoảng thời gian tối thiểu 1 năm để phục vụ việc quản lý, kiểm soát hệ thống thông tin.  9. Thiết lập phương án dự phòng để bảo đảm hệ thống thông tin hoạt động liên tục 24/24 giờ. |
| **Yêu cầu 02** | Xác định trách nhiệm của đơn vị chuyên trách về ATTT, các cán bộ làm về ATTT và các đối tượng thuộc phạm vi điều chỉnh của chính sách ATTT. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | 1. Áp dụng QĐ 29/2013/QĐ-UBND ngày 11/12/2013, Quy chế bảo đảm ATTT. Tại Khoản 1, 3, 4 điều 7 quy định:  - Tham mưu Ủy ban nhân dân tỉnh về công tác bảo đảm ATTT trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị trên địa bàn tỉnh, cụ thể: về quy trình, chính sách chung; thẩm định đầu tư thiết bị phần cứng, phần mềm, hạ tầng mạng truyền thông; đào tạo về ATTT cho cán bộ, công chức, viên chức; tổ chức các hội thảo chuyên ngành về ứng cứu sự cố máy tính, đảm bảo ATTT; tổ chức bảo đảm ATTT cho các hệ thống thông tin dùng chung cấp tỉnh phục vụ sự lãnh đạo, điều hành của lãnh đạo tỉnh được nhanh chóng, an toàn, hiệu quả.  - Thông báo cho các cơ quan, đơn vị biết và hướng dẫn các biện pháp kỹ thuật nghiệp vụ phòng ngừa, ngăn chặn các nguy cơ gây mất ATTT.  - Chủ trì, phối hợp với các cơ quan, đơn vị liên quan xử lý, ứng cứu các sự cố máy tính trong các cơ quan, đơn vị.  2. Trung tâm CNTT&TT đưa ra phương án xác định trách nhiệm của đơn vị chuyên trách về ATTT:  - Trung tâm CNTT&TT chịu sự chỉ đạo trực tiếp từ Lãnh đạo Sở TT&TT, chịu trách nhiệm tổ chức triển khai bảo đảm ATTT của Trung tâm dữ liệu tỉnh.  - Trung tâm CNTT&TT chịu sự chỉ đạo trực tiếp từ Lãnh đạo Sở TT&TT (với vai trò là đơn vị chuyên trách về ATTT cấp tỉnh) tham mưu, hỗ trợ các đơn vị khác trong tỉnh về nhiệm vụ đảm bảo an toàn cho TTDL từ cấp tỉnh, các hệ thống thông tin dùng chung khác của tỉnh nói chung;  - Trách nhiệm của người vận hành, giám sát hạ tầng kỹ thuật tại trung tâm dữ liệu cần phải nghiêm chỉnh chấp hành các quy định tại quy chế nội bộ đảm bảo an toàn, an ninh thông tin, các quy định khác của pháp luật về ATTT. Chịu trách nhiệm đảm bảo ATTT trong phạm vi trách nhiệm, quyền hạn được giao;  - Trung tâm CNTT&TT là đơn vị vận hành trực tiếp Trung tâm dữ liệu tỉnh, luôn xác định trách nhiệm của mình là đầu mối của đơn vị chuyên trách về ATTT trong việc phối hợp với các đơn vị liên quan đảm bảo kỹ thuật an toàn, chất lượng, hiệu quả; Ứng cứu sự cố máy tính trong trung tâm cũng như các đơi vị có liên quan. |
| **Yêu cầu 03** | Xác định phạm vi chính sách ATTT 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 ATTT. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | 1. Áp dụng Quyết định số 29/2013/QĐ-UBND ngày 11/12/2013, Quy chế bảo đảm ATTT. Chỉ thị Số 11/CT-UBND về việc tăng cường bảo đảm an toàn, an ninh mạng trên địa bàn tỉnh Hải Dương. Sở TT&TT được quy định phạm vi chính sách ATTT như sau:  a) Chủ trì, phối hợp với các đơn vị có liên quan tiếp tục tham mưu UBND tỉnh hoàn thiện cơ chế chính sách, Văn bản quy phạm pháp luật về ATTT mạng, an ninh mạng, chữ ký số... đảm bảo đồng bộ với các các hệ thống Văn bản quy phạm pháp luật, của Trung ương.  b) Là đầu mối thông tin thực hiện giám sát, ứng cứu sự cố ATTT mạng của tỉnh; có trách nhiệm liên kết, phối hợp với các đơn vị trong mạng lưới ứng cứu sự cố mạng, máy tính quốc gia như Trung tâm ứng cứu sự cố mạng máy tính Việt Nam; Trung tâm Internet Việt Nam (VNNIC) nhằm thực hiện tốt công tác đảm an toàn, an ninh thông tin mạng, máy tính của tỉnh.  c) Chủ trì, phối hợp với các cơ quan, đơn vị của tỉnh triển khai giải pháp bảo đảm ATTT mạng tổng thể trong các cơ quan, đơn vị nhà nước phục vụ công tác nâng cao thứ hạng của tỉnh về an toàn, an ninh mạng; xây dựng bộ tiêu chí đánh giá mức độ ATTT mạng của tỉnh, tổ chức đánh giá và công bố định kỳ hàng năm khi có văn bản hướng dẫn của Bộ Thông tin và Truyền thông.  d) Chủ trì, phối hợp các cơ quan, đơn vị tổ chức, triển khai thực hiện công tác xác định cấp độ và xây dựng hồ sơ đề xuất cấp độ an toàn hệ thống thông tin trên địa bàn tỉnh; Đối với các hệ thống thông tin cấp độ 3 và cấp độ 4, định kỳ hàng năm thực hiện kiểm tra, đánh giá và tổng hợp báo cáo Bộ Thông tin và Truyền thông trước ngày 14/12 hàng năm để tổng hợp, báo cáo Thủ tướng Chính phủ.  e) Tổ chức diễn tập, các lớp đào tạo, bồi dưỡng nâng cao kiến thức, kỹ năng bảo đảm an toàn, an ninh thông tin cho cán bộ chuyên trách công nghệ thông tin trên địa bàn tỉnh.  f) Chủ trì, phối hợp với các cơ quan báo chí trong việc xây dựng nội dung tuyên truyền, phổ biến nâng cao nhận thức cho cán bộ công chức, viên chức trên địa bàn tỉnh về các mối nguy hại và phương thức phòng, chống mã độc.  g) Chỉ đạo các doanh nghiệp viễn thông, công nghệ thông tin trên địa bàn tỉnh triển khai các biện pháp kỹ thuật đảm bảo an toàn cho các hệ thống thông tin do đơn vị quản lý; tham gia hỗ trợ các cơ quan, tổ chức nhà nước giám sát, bảo vệ, kiểm tra, đánh giá ATTT mạng.  h) Chủ trì, đôn đốc, theo dõi việc thực hiện Chỉ thị này, tổng hợp, định kỳ báo cáo Thủ tướng Chính phủ, Bộ Thông tin và Truyền thông và UBND tỉnh về kết quả thực hiện. |
| **Yêu cầu 04** | Xây dựng chính sách ATTT 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 ATTT; Quản lý giám sát AT HTTT; Quản lý an toàn sử dụng đầu cuối. |
| **Hiện trạng** | Sở TT&TT chưa có quy chế nội bộ bảo đảm ATTT cho trung tâm tích hợp dữ liệu. |
| **Phương án** | Sẽ xây dựng quy chế nội bộ bảo đảm bảo ATTT với một số nội dung sau:  1. Sở TT&TT sẽ ban hành quy chế nội bộ bảo đảm ATTT cho hệ thống mạng, máy tính tại Trung tâm tích hợp dữ liệu (hoặc sẽ trình UBND tỉnh phê duyệt quy chế). Quy chế nêu rõ các nội dung sau:  - Phạm vi, đối tượng áp dụng;  - Mục đích, nguyên tắc chung đảm bảo an toàn, an ninh thông tin từ cấp tỉnh đến cấp huyện;  - Quy định về quản lý, vận hành hệ thống máy chủ, thiết bị mạng, thiết bị bảo mật đảm bảo an toàn;  - Trách nhiệm của các đơn vị;  - Khen thưởng, kỷ luật;  - Tổ chức thực hiện.  2. Trung tâm CNTT&TT phải căn cứ các nội dung quy định tại Quy chế này, các quy định của pháp luật về bảo vệ bí mật nhà nước và các quy định khác của pháp luật có liên quan để xây dựng Quy chế nội bộ đảm bảo an toàn, an ninh thông tin tại cơ quan, đơn vị cho phù hợp. |

### 1. 2. Xây dựng và công bố

|  |  |
| --- | --- |
| **Yêu cầu 01** | Chính sách tổ chức / bộ phận được ủy quyền thông qua trước khi công bố áp dụng. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | 1. Quy định chung quản lý an toàn của trung tâm tích hợp dữ liệu  Tuân thủ theo Quy chế bảo đảm ATTT trên địa bàn tỉnh Hải Dương ban hành kèm theo Quyết định số 29/2013/QĐ-UBND ngày 11/12/2013.  2. Trung tâm CNTT&TT sẽ là các đối tượng phải tuân thủ theo quy định về xây dựng và công bố Quy chế bảo đảm ATTT cho trung tâm tích hợp dữ liệu. |
| **Yêu cầu 02** | Chính sách được công bố trước khi áp dụng. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Đã áp dụng theo các Chính sách của các Quy chế, Quyết định, văn bản chỉ đạo của UBND tỉnh như trên Yêu cầu 01 trên. Do vậy những chính sách về ATTT đã được công bố rộng rãi trước khi áp dụng cho việc khai thác, vận hành an toàn theo Quy chế, Quyết định liên quan đến ATTT. |

### 1. 3. Rà soát, sửa đổi

|  |  |
| --- | --- |
| **Yêu cầu** | Định kỳ 02 năm hoặc có thay đổi chính sách ATTT kiểm tra tính phù hợp và thực hiện rà soát, cập nhật bổ sung. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | 1. Quy chế bảo đảm ATTT kèm theo Quyết định số 29/2013/QĐ-UBND ngày 11/12/2013 của UBND tỉnh Hải Dương, quy định rằng: Sở Thông tin và Truyền thông có trách nhiệm chủ trì, phối hợp với các cơ quan, tổ chức liên quan hướng dẫn, triển khai và kiểm tra, đôn đốc việc thực hiện quy chế.  Trong quá trình thực hiện nếu có gì vướng mắc, Sở TT&TT sẽ tổng hợp, báo cáo UBND tỉnh xem xét, sửa đổi, bổ sung cho phù hợp.  2. Trung tâm CNTT&TT đóng vai trò chính trong việc vận hành Hạ tầng kỹ thuật trung tâm dữ liệu tỉnh. Qua quá trình vận hành sẽ tổng hợp được nhiều kinh nghiệm thực tế diễn ra, từ đó tham mưu cho Sở TT&TT rà soát, cập nhật bổ sung, kiểm tra tính phù hợp, để thay đổi chính sách bảo đảm ATTT cấp tỉnh đến cấp huyện định kỳ hàng năm. |

## 2. Tổ chức bảo đảm an toàn thông tin

### 2. 1. Đơn vị chuyên trách về an toàn thông tin

|  |  |
| --- | --- |
| **Yêu cầu 01** | Thành lập hoặc chỉ định đơn vị/bộ phận chuyên trách về ATTT trong tổ chức. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Áp dụng QĐ số 2979/QĐ-UBND ngày 29/9/2017 của UBND tỉnh Hải Dương về việc thành lập Đội ứng cứu sự cố bảo đảm ATTT mạng tỉnh Hải Dương. Tại khoản 2 điều 3 quy định:  - Bộ phận giúp việc của đội ứng cứu ATTT mạng là phòng Quản trị và An ninh mạng Trung tâm CNTT&TT, Sở TT&TT;  - Từ quyết định trên, Trung tâm CNTT phải bố trí cán bộ chuyên trách về ATTT của đơn vị; tạo điều kiện để cán bộ chuyên trách này được học tập, nâng cao kiến thức về ATTT. |
| **Yêu cầu 02** | Phân định vai trò, trách nhiệm, cơ chế phối hợp của các bộ phận, cán bộ trong đơn vị chuyên trách về ATTT. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Áp dụng Quy chế bảo đảm ATTT ban hành kèm theo Quyết định số Quyết định 29/2013/QĐ-UBND ngày 11/12/2013. Trong đó quy định vai trò của Sở TT&TT đóng vai trò chuyên trách về ATTT, đảm bảo an toàn, an ninh thông tin cho các HTTT dùng chung của tỉnh;  - Trung tâm CNTT&TT và các đơn vị sẽ phối hợp với Sở TT&TT và các đơn vị liên quan như VNCERT, BKAV, Viễn thông VNPT Hải Dương, Vietel… thực hiện công tác kiểm tra, khắc phục sự cố nhanh chóng, kịp thời và hiệu quả (nếu xảy ra sự cố); đồng thời cung cấp đầy đủ thông tin khi được yêu cầu trong công tác bảo đảm an toàn, an ninh thông tin. |

### 2. 2. Phối hợp với những cơ quan/tổ chức có thẩm quyền

|  |  |
| --- | --- |
| **Yêu cầu 01** | Có đầu mối liên hệ, phối hợp với những cơ quan, tổ chức có thẩm quyền quản lý về ATTT. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | 1. Trung tâm CNTT&TT có phương án đáp ứng đầu mối liên hệ, phối hợp với những cơ quan, tổ chức có thẩm quyền quản lý về ATTT, một số nội dung sau:  - Trung tâm CNTT&TT thực hiện công tác kiểm tra, khắc phục sự cố nhanh chóng, kịp thời và hiệu quả (nếu xảy ra sự cố); đồng thời cung cấp đầy đủ thông tin khi được yêu cầu trong công tác bảo đảm an toàn, an ninh thông tin.  2. Trung tâm CNTT&TT chịu sự chỉ đạo trực tiếp của lãnh đạo Sở TT&TT, sẽ phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin. Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.  3. Trung tâm CNTT&TT chịu sự chỉ đạo trực tiếp của lãnh đạo Sở TT&TT chủ trì, phối hợp với Ban Cơ yếu Chính phủ triển khai giải pháp an toàn, bảo mật đối với HTTT, CSDL liên quan đến lưu trữ, truyền tải thông tin bí mật nhà nước trên Mạng truyền số liệu chuyên dùng của của các cơ quan nhà nước tỉnh.  4. Trung tâm CNTT&TT chịu sự chỉ đạo trực tiếp của lãnh đạo Sở TT&TT là cơ quan đầu mối về ứng cứu sự cố máy tính của tỉnh, tham gia vòa mạng lưới điều phối ứng cứu sự cố, tiếp nhận và xử lý các thông báo sự cố về ATTT. Tùy thuộc vòa mức độ sự cố, phối hợp với Trung tâm ứng cứu khẩn cấp sự cố không gian mạng Việt Nam (VNCERT), các đơn vị liên quan hướng dẫn xử lý, ứng cứu sự cố mất ATTT. |
| **Yêu cầu 02** | Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố ATTT. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Quy chế bảo đảm ATTT kèm theo Quyết định số 29/2013/QĐ-UBND ngày 11/12/2013 của UBND tỉnh Hải Dương. Trung tâm CNTT&TT có phương án quy định về việc quy định phải có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố ATTT, một số nội dung như sau:  - Trung tâm CNTT&TT phát hiện, kiểm tra, khắc phục sự cố nhanh chóng, kịp thời và hiệu quả; đồng thời cung cấp đầy đủ thông tin khi được yêu cầu trong công tác bảo đảm an toàn, an ninh thông tin.  - Sở TT&TT sẽ tạo điều kiện tốt nhất cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện theo hướng dẫn công tác ATTT (nếu xảy ra sự cố).  - Sở TT&TT tạo điều kiện tốt nhất để thành viên là cán bộ của Sở tham gia tích cực vào mạng lưới đội ứng cứu sự cố ATTT mạng của tỉnh. |
| **Yêu cầu 03** | Tham gia các hoạt động, công tác bảo đảm ATTT khi có yêu cầu của tổ chức có thẩm quyền. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Căn cứ quyết định 2979/QĐ-UBND tỉnh Hải Dương, ngày 29/09/2017 về việc thành lập Đội ứng cứu sự cố ATTT mạng tỉnh Hải Dương. Theo chức năng nhiệm vụ thì Đội ứng cứu sự cố ATTT mạng tỉnh là một địa chỉ liên hệ quan trọng trong công tác điều phối xử lý sự cố ATTT nói chung và việc vận hành an toàn. |

## 3. Bảo đảm nguồn nhân lực

### 3. 1. Tuyển dụng

|  |  |
| --- | --- |
| **Yêu cầu 01** | Cán bộ được tuyển dụng vào vị trí làm về ATTT có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, ATTT, phù hợp với vị trí tuyển dụng. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Người cán bộ kỹ thuật tham gia vận hành là những cán bộ được tuyển dụng có chuyên môn phù hợp, chuyên trách về CNTT, ATTT;  - Bố trí công việc vận hành Trung tâm THDL tỉnh sẽ dựa vào trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, ATTT, theo quy định của của Sở Nội vụ và Sở TT&TT. |
| **Yêu cầu 02** | Có quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | 1. Trung tâm CNTT&TT tuyển dụng cán bộ nhằm thực hiện các nhiệm vụ về Công nghệ thông tin, ATTT dựa vào trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, ATTT bố trí vị trí việc làm về ATTT theo quy định của của Sở Nội vụ và các cấp có thẩm quyền.  2. Cán bộ kỹ thuật tham gia vận hành được bố trí là những cán bộ được tuyển dụng có chuyên môn phù hợp, chuyên trách về CNTT, ATTT. |

### 3. 2. Trong quá trình làm việc

|  |  |
| --- | --- |
| **Yêu cầu 01** | Có quy định về việc thực hiện nội quy, quy chế bảo đảm ATTT cho người sử dụng, cán bộ quản lý và vận hành hệ thống. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Quy định về việc thực hiện bảo đảm ATTT trong quá trình làm việc:  1. Trách nhiệm bảo đảm ATTT của cán bộ quản lý và vận hành tại phòng máy chủ Trung tâm tích hợp dữ liệu:  + Nghiêm chỉnh chấp hành các quy định tại Quy chế nội bộ bảo đảm an toàn, an ninh thông tin của cơ quan, đơn vị, các quy định tại Quy chế này và quy định khác của pháp luật về ATTT. Chịu trách nhiệm đảm bảo ATTT trong phạm vi trách nhiệm, quyền hạn được giao;  + Khi phát hiện nguy cơ hoặc sự cố mất ATTT phải báo cáo ngay với cấp trên và cán bộ chuyên trách của đơn vị để kịp thời ngăn chặn, xử lý;  2. Trách nhiệm bảo đảm ATTT khi vận hành của cán bộ quản lý và vận hành tại các Phòng họp điểm cầu, một số nội dung như sau:  - Luôn có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị;  - Không cho phép truy cập mạng với mục đích khác vào hệ;  - Tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập tới hệ thống thông tin;  - Mật khẩu thay đổi định kỳ và ở mức độ khó để đảm bảo tính ATT.  - Giám sát theo dõi hệ thống thông qua Firewall. |
| **Yêu cầu 02** | Có kế hoạch và định kỳ hàng năm tổ chức, tuyên truyền nâng cao nhận thức về ATTT cho người sử dụng |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Quy chế bảo đảm ATTT kèm theo Quyết định số 29/2013/QĐ-UBND ngày 11/12/2013 của UBND tỉnh Hải Dương. Tại khoản 5 điều 6 quy định:  - Báo cáo định kỳ hàng năm về tình hình an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan, đơn vị gửi về Sở Thông tin và Truyền thông trước ngày 25 tháng 12 để tổng hợp chung báo cáo Ủy ban nhân dân tỉnh.  Tuân thủ Căn cứ quyết định 2979/QĐ-UBND tỉnh Hải Dương, ngày 29/09/2017 về việc thành lập Đội ứng cứu sự cố ATTT mạng tỉnh Hải Dương  - Tham mưu cho Ban Chỉ đạo ứng dụng công nghệ thông tin tỉnh tổ chức diễn tập chuyên đề hàng năm về ATTT, ứng cứu sự cố mạng trên địa bàn tỉnh; phối hợp, tham gia các cuộc diễn tập quốc gia, quốc tế do cơ quan điều phối quốc gia, Bộ Thông tin và Truyền thông tổ chức. |
| **Yêu cầu 03** | Định kỳ hàng năm, tổ chức đào tạo các kỹ năng cơ bản về ATTT cho người sử dụng. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Tham gia đầy đủ các chương trình đào tạo, tập huấn, hội nghị về an toàn, an ninh thông tin do Sở Thông tin và Truyền thông hoặc các cơ quan, đơn vị chuyên môn tổ chức;  - Tuân thủ Căn cứ quyết định 2979/QĐ-UBND tỉnh Hải Dương, ngày 29/09/2017 về việc thành lập Đội ứng cứu sự cố ATTT mạng tỉnh Hải Dương.  + Tham gia các chương trình bồi dưỡng, tập huấn, đào tạo, hội thảo nhằm nâng cao trình độ, nghiệp vụ, tăng cường nhận thức, phổ biến kiến thức liên quan bao gồm đào tạo về quy trình, quản lý rủi do, chuẩn quốc tế về ATTT mạng; đào tạo nâng cao kiến thức pháp luật, đạo đức nghề nghiệp. |

### 3. 3. Chấm dứt hoặc thay đổi công việc

|  |  |
| --- | --- |
| **Yêu cầu 01** | 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. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT quy định cán bộ, công chức, viên chức đã nghỉ việc, chuyển công tác phải có biện pháp khóa tài khoản, hủy quyền truy cập, thu hồi các thiết bị liên quan tới hệ thống thông tin. |
| **Yêu cầu 02** | 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. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án quy định về việc xây dựng Quy chế nội bộ bảo đảm an toàn, an ninh thông tin, quy định cụ thể về trách nhiệm của từng cá nhân khi tham gia sử dụng hệ thống thông tin:  - Thực hiện cấu hình trong việc quản lý tài khoản, định danh người dùng trong các hệ thống thông tin bao gồm: tạo mới, kích hoạt, sửa đổi và loại bỏ tài khoản người dùng. |
| **Yêu cầu 03** | Có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Trung tâm CNTT&TT nêu rõ trong Quy chế nội bộ bảo đảm an toàn, an ninh thông tin, quy định cụ thể về trách nhiệm của từng cá nhân khi tham gia sử dụng hệ thống thông tin, nội dung sau:  - Các cán bộ, công chức, viên chức nghiêm chỉnh chấp hành các quy định tại quy chế nội bộ bảo đảm an toàn, an ninh thông tin của cơ quan, đơn vị, các quy định tại Quy chế này và quy định của pháp luật về ATTT. Chịu trách nhiệm đảm bảo ATTT trong phạm vi trách nhiệm, quyền được giao. Trong đó cá nhân phải cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc. Trung tâm CNTT&TT sẽ có biện pháp áp dụng cho người nghỉ việc để thực hiện quy định này. |

## 4. Quản lý thiết kế, xây dựng hệ thống thông tin

### 4. 1. Thiết kế an toàn hệ thống thông tin

|  |  |
| --- | --- |
| **Yêu cầu 01** | Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành HTTT. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Đầu tư các trang thiết bị để vận hành trung tâm dữ liệu của Tỉnh. |
| **Yêu cầu 02** | Có tài liệu mô tả thiết kế và các thành phần của HTTT. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Thiết kế đảm bảo tuân thủ theo các quy định tại Công văn số 1655/BTTTT-UDCNTT ngày 27/5/2008 của Bộ Thông tin và Truyền thông về việc Hướng dẫn các yêu cầu cơ bản về chức năng, tính năng kỹ thuật đối với Hệ thống giao ban điện tử đa phương tiện.  - Thiết kế đảm bảo áp dụng các quy chuẩn, tiêu chuẩn kỹ thuật theo quy định của Bộ Thông tin và Truyền thông; lựa chọn các thiết bị, công nghệ hiện đại nhất hiện nay, phương án kỹ thuật và công nghệ kết nối ra bên ngoài đảm bảo thông suốt trong quá trình tổ chức hội nghị truyền hình trực tuyến tại các điểm cầu. |
| **Yêu cầu 03** | Có tài liệu mô tả phương án bảo đảm ATTT theo cấp độ. |
| **Hiện trạng** | Chưa có tài liệu mô tả chính thức trước khi xây dựng hồ sơ đề xuất cấp độ. |
| **Phương án** | Sẽ xây dựng tài liệu mô tả phương án bảo đảm ATTT theo cấp độ, sau 06 tháng khi hồ sơ đề xuất cấp độ ATTT được phê duyệt. |
| **Yêu cầu 04** | Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm ATTT. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Nghị quyết số: 20/2019/NQ-HĐND của HDND tỉnh Hải Dương về việc **Xây dựng Chính quyền điện tử và Đô thị thông minh tỉnh Hải Dương, giai đoạn 2020 - 2025, định hướng đến năm 2030. Tại điều 6. 2 đề ra:**  - Nâng cấp, hoàn thiện Cổng Dịch vụ công trực tuyến tỉnh Hải Dương; Hệ thống Một cửa điện tử 3 cấp nhằm liên thông giải quyết các thủ tục hành chính và dịch vụ công trực tuyến trên địa bàn tỉnh.  - Hoàn thiện nền tảng tích hợp, chia sẻ dữ liệu dùng chung của tỉnh (LGSP) đảm bảo 100% các HTTT/CSDL cốt lõi của tỉnh được chia sẻ, tích hợp kết nối các quy trình nghiệp vụ của cơ quan nhà nước trên địa bàn tỉnh, trung ương và mở rộng thành nền tảng phục vụ đô thị thông minh.  - Xây dựng Trung tâm hành chính công đến 100% cấp huyện, thị xã, thành phố và hệ thống dịch vụ công trực tuyến phục vụ người dân.  - Xây dựng cơ sở hạ tầng công nghệ thông tin đảm bảo phục vụ nhu cầu phát triển chính quyền điện tử và đô thị thông minh triển khai các dự án ứng dụng thông minh hiệu quả, nâng cao năng lực quản lý điều hành, phục vụ người dân và doanh nghiệp.  - Xây dựng Trung tâm giám sát, điều hành đô thị thông minh phục vụ công tác chỉ đạo, điều hành của lãnh đạo.  - Xây dựng Trung tâm giám sát điều hành ATTT mạng tỉnh Hải Dương; Hệ thống nền tảng điều hành an ninh bảo mật đủ mạnh để giám sát phát hiện và ngăn chặn được hầu hết các cuộc tấn công trên không gian mạng.  - Xây dựng Trung tâm điều hành, giám sát thông minh Tỉnh ủy.  - Xây dựng Hệ thống họp không giấy tờ; hệ thống điều hành thông minh Hội đồng nhân dân phục vụ công tác chỉ đạo, điều hành của lãnh đạo.  - Thí điểm xây dựng đô thị thông minh trên địa bàn thành phố Hải Dương và thành phố Chí Linh.  - Xây dựng hệ thống y tế thông minh, giáo dục thông minh, giao thông thông minh, du lịch thông minh, hệ thống quan trắc môi trường, xây dựng hệ thống camera chung cho (giao thông, công an, trường học, bệnh viện, trung tâm hành chính cống, phòng tiếp dân... ), đảm bảo người dân có thể tiếp cận một cách tốt nhất thông tin và các dịch vụ công ích của các lĩnh vực thông qua các ứng dụng thông minh. |
| **Yêu cầu 05** | 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. |
| **Hiện trạng** | ~~Chưa có tài liệu mô tả chính thức trước khi xây dựng hồ sơ đề xuất cấp độ.~~ |
| **Phương án** | Sở TT&TT sẽ có văn bản mới về phương án thiết kế đối với các yêu cầu ATTT cho trung tâm tích hợp dữ liệu, nếu có thay đổi về thiết kế hoặc các yêu cầu ATTT không còn phù hợp. |

### 4. 2. Phát triển phần mềm thuê khoán

|  |  |
| --- | --- |
| **Yêu cầu 01** | Có điều khoản hợp đồng và các cam kết đối với bên thuê khoán khi thực hiện các nội dung liên quan đến việc phát triển phần mềm thuê khoán. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | ~~- Có hợp đồng dịch vụ tư vấn.~~  ~~- Thiết lập các giải pháp ATTT của hãng Cisco, fortinet…phải bao gồm: Đường truyền, hệ thống thiết bị, các hệ thống thiết bị phụ trợ khác. Trong đó mỗi thiết bị phần cứng đã được đóng gói phần mềm chuyên dụng xử lý. Do đó việc phát triển phần mềm thuê khoán là không cần thiết trong dự án này.~~ |
| **Yêu cầu 02** | Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | ATTT từ cấp tỉnh đến cấp huyện sử dụng giải pháp của hãng Cisco, Fortinet… Hệ thống bao gồm phần các phần cứng và phần mềm; Các phần mềm chuyên dụng được đóng gói trong các thiết bị phần cứng. Nhà phát triển cung cấp phần mềm điều khiển quản trị, vận hành với nhiều phiên bản phù hợp . |
| **Yêu cầu 03** | Phần mềm thuê khoán phải được kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trước khi đưa phần mềm ATTT từ cấp tỉnh đến cấp huyện vào sử dụng chính thức, đã được kiểm tra thử nghiệm thành công nhiều lần. |
| **Yêu cầu 04** | Phần mềm thuê khoán phải được kiểm tra, đánh giá ATTT trước khi đưa vào sử dụng. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Hệ thống ATTT từ cấp tỉnh đến cấp huyện sử dụng giải pháp của hãng: Cisco, fortinet... Trong đó, Cisco, Fortinet đã có cam kết đảm bảo ATTT nói riêng và chất lượng, thương hiệu nổi tiếng của mình nói chung. |

### 4. 3. Thử nghiệm và nghiệm thu hệ thống

|  |  |
| --- | --- |
| **Yêu cầu 01** | Thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Các mốc thời gian thực hiện đầu tư dự án, chỉ ra thời điểm tiến hành Nghiệm thu, Báo cáo, tổng kết, vận hành hệ thống chính thức. |
| **Yêu cầu 02** | Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Các mốc thời gian thực hiện đầu tư dự án, chỉ ra thời điểm tiến hành Nghiệm thu, Báo cáo, tổng kết, vận hành hệ thống chính thức. |
| **Yêu cầu 03** | Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Nội dung này được quy định trong gói thầu được triển khai trong trung tâm tích hợp dữ liệu tỉnh Hải Dương. |
| **Yêu cầu 04** | Có đơn vị độc lập hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Nội dung này được quy định trong gói thầu được triển khai trong trung tâm tích hợp dữ liệu tỉnh Hải Dương. |
| **Yêu cầu 05** | Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản HTTT trước khi sử dụng. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Đã có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản HTTT trước khi sử dụng. |

## 5. Quản lý vận hành hệ thống thông tin

### 5. 1. Quản lý an toàn mạng

|  |  |
| --- | --- |
| **Yêu cầu 01** | Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống mạng. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Trung tâm CNTT&TT có phương án quy định về việc quản lý, vận hành hoạt động bình thường của hạ tầng mạng như sau:  - Thường xuyên theo dõi bản ghi nhật ký trên các thiết bị mạng của ATTT của Trung tâm dữ liệu tỉnh Hải Dương.  - Tuân thủ đầy đủ kiến thức về ATTT, bảo mật thông tin cho cán bộ làm công tác vận hành, quản trị, khai thác và quản trị hệ thống.  - Tham mưu về chuyên môn và vận hành Trung tâm dữ liệu, triển khai các biện pháp đảm bảo ATTT cho cán bộ, công chức, viên chức trong khi sử dụng hệ thống.  - Nắm vững và thực hiện nghiêm túc các quy định về bảo mật nhà nước, thường xuyên nghiên cứu, cập nhật kiến thức về an toàn, an ninh thông tin; các nguy cơ tiềm ẩn có thể gây mất ATTT và biện pháp kỹ thuật phòng ngừa.  2. Một số quy định về quản lý, vận hành hoạt động tại Trung tâm dữ liệu  - Bố trí cán bộ có năng lực chuyên môn cao để quản lý, vận hành phòng máy chủ và duy trì chế độ trực để bảo đảm ATTT mạng.  - Các thiết bị mạng chính đáp ứng tốt tại Trung tâm dữ liệu phải được cài đặt và cấu hình đảm bảo:  + Các thiết bị mạngcủa hệ thống phải được bảo vệ an toàn trước những thảm họa từ con người và thiên nhiên như chống cháy, nổ, chống sét, …  + Các thiết bị chuyển mạch (Switch), tường lửa (Firewall) phải đảm bảo cấu hình, khai thác sử dụng tối ưu về tính năng và hiệu xuất và phải được cập nhật thường xuyên phiên bản phần mềm mới nhất.  - Không được tự ý sử dụng, di chuyển và cài đặt hoặc sử dụng không đúng với mục đích đối với các thiết bị của Trung tâm dữ liệu khi không được cho phép. |
| **Yêu cầu 02** | Có quy định về cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Quyết định 29/2013/QĐ-UBND ngày 11/12/2013 Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT của các cơ quan nhà nước trên địa bàn tỉnh Hải Dương. Tại điều 4 sử dụng hệ thống thông tin:  1. Có kế hoạch kiểm tra, bảo dưỡng định kỳ các thiết bị thuộc hệ thống thông tin; duy trì phù hợp, đúng cách và an toàn các thiết bị với yêu cầu về thời gian và thông số kỹ thuật của nhà cung cấp.  2. Thực hiện quản lý chặt chẽ các tài khoản truy nhập hệ thống thông tin; yêu cầu người dùng thường xuyên thay đổi mật khẩu; định kỳ tổ chức kiểm tra các tài khoản truy nhập hệ thống thông tin; hủy tài khoản truy nhập hệ thống thông tin và thu hồi các tài liệu, hồ sơ, thông tin liên quan tới tài khoản bị hủy bỏ đối với cán bộ, nhân viên đã nghỉ việc hoặc chuyển công tác; tổ chức theo dõi, kiểm soát tất cả các phương pháp truy nhập từ xa tới hệ thống thông tin, bao gồm cả sự truy nhập có chức năng quản trị.  3. Thường xuyên kiểm tra, sao lưu các bản ghi nhật ký hệ thống thông tin để lưu vết những sự kiện đã xảy ra.  4. Thường xuyên cập nhật phiên bản mới, bản vá lỗi của các phần mềm hệ điều hành, phần mềm ứng dụng, phần mềm quản trị cơ sở dữ liệu, phần mềm chống vi-rút máy tính nhằm bảo đảm khả năng phát hiện, ngăn chặn, loại trừ vi-rút máy tính cũng như sự xâm nhập của tin tặc vào hệ thống thông tin; thực hiện chế độ quét vi-rút máy tính thường xuyên.  5. Tổ chức cấp phát tài nguyên trên máy chủ theo danh mục thư mục cho từng phòng, ban; kiểm tra, giám sát việc chia sẻ tài nguyên, khuyến cáo người sử dụng cân nhắc việc chia sẻ tài nguyên trên các máy trạm, khi sử dụng chức năng chia sẻ tài nguyên cần phải sử dụng mật khẩu để bảo vệ và thực hiện việc thu hồi chức năng này khi đã sử dụng xong.  6. Không phát triển, kiểm thử, cài đặt các ứng dụng thử nghiệm trên hệ thống vận hành chính thức để giảm thiểu rủi ro về ATTT.  7. Bố trí máy vi tính riêng, không kết nối mạng nội bộ và Internet dùng để soạn thảo văn bản, lưu giữ thông tin có nội dung mật theo quy định; cần có các cơ chế đặc biệt nhằm bảo vệ dữ liệu, thông tin nhạy cảm của cơ quan, đơn vị truyền tải qua mạng công cộng để bảo đảm tính toàn vẹn và bí mật của thông tin.  8. Thực hiện định kỳ việc sao lưu dữ liệu hệ điều hành, các phần mềm ứng dụng, phần mềm chuyên ngành, các cơ sở dữ liệu quan trọng phục vụ công tác của cơ quan, đơn vị bằng các phần mềm chuyên dụng, sao chép ra các thiết bị lưu trữ ngoài, thực hiện việc đánh số, dán nhãn để tránh nhầm lẫn và cất giữ ở nơi an toàn; đồng thời thường xuyên kiểm tra để bảo đảm tính sẵn sàng phục hồi và toàn vẹn thông tin.  9. Tắt máy tính trạm hoặc ngưng kết nối mạng trong trường hợp máy tính không sử dụng trong thời gian dài (quá 4 giờ làm việc) để phòng tránh tin tặc lợi dụng chức năng điều khiển từ xa, sử dụng máy tính này tấn công vào các hệ thống thông tin khác; quét vi-rút máy tính trước khi mở các tệp tin kèm theo thư điện tử biết rõ người gửi, các tệp tin tải về từ Internet, các tệp tin trong các thiết bị lưu trữ ngoài và không được mở các tệp tin kèm theo thư điện tử có nguồn gốc không rõ ràng để phòng ngừa vi-rút máy tính xâm nhập vào máy tính; đặt mật khẩu truy nhập vào máy tính, đồng thời thiết lập chế độ bảo vệ màn hình có sử dụng mật khẩu bảo vệ sau một khoảng thời gian nhất định không sử dụng máy tính.  10. Thường xuyên theo dõi hoạt động của hệ thống thông tin. Khi phát hiện sự cố như máy chủ bị tấn công, cần thông báo ngay cho Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ khắc phục sự cố. |
| **Yêu cầu 03** | Có quy định về truy cập và quản lý cấu hình hệ thống |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Để truy cập an toàn phải tổ chức quản lý tài khoản, định danh người dùng trong hệ thống; phải có cơ chế tạo mới, kích hoạt, sửa đổi và loại bỏ tài khoản này.  - Đối với tài khoản người dùng sử dụng để truy cập thiết lập mật khẩu có mức độ bảo mật cao, không sử dụng mật khẩu ngắn, mặc định nhằm bảo đảm an toàn, bảo mật thông tin của người dùng.  2. Một số quy định về truy cập và quản lý cấu hình hệ thống mạng, bảo đảm ATTT của cán bộ quản lý và vận hành tại phòng máy chủ Trung tâm THDL:  - Phải cấu hình hệ thống mạng an toàn với các chính sách an toàn cho truy cập hệ thống, như quản lý chặt chẽ tài khoản truy cập, xác thực tài khoản truy cập đã được cấp phép (địa chỉ IP, địa chỉ MAC, …);  - Giới hạn các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa; hạn chế được số lần đăng nhập sai; phân quyền truy cập, quản trị; nâng cấp, xử lý điểm yếu ATTT của thiết bị hệ thống trước khi đưa vào sử dụng. |
| **Yêu cầu 04** | Có quy định về cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống mạng trước khi đưa vào vận hành khai thác |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | 1. Trung tâm CNTT&TT có phương án quy định về cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống mạng trước khi đưa vào vận hành khai thác  - Tất cả máy tính tại đơn vị thực hiện khai thác, vận hành, quản trị phải được cài đặt và bảo vệ bởi phần mềm phòng chống vi rút, phần mềm độc hại trên môi trường mạng.  - Giới hạn số lần đăng nhập sai liên tiếp vào hệ thống, hệ thống sẽ phải tự động khóa tài khoản trong một thời gian nhất định trước khi tiếp tục cho đăng nhập.  - Luôn có cơ chế ngăn chặn hoặc hạn chế sự cố tấn công mạng (ví dụ tấn công từ chối dịch vụ DDOS). Sử dụng thiết bị tường lửa mạng để quản lý luồng dữ liệu vào ra hệ thống;  - Cấu hình tối ưu, tăng cường bảo mật hệ thống mạng để bảo vệ dữ liệu, ứng dụng và hệ điều hành.  2. Một số quy định về cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống mạng trước khi đưa vào vận hành khai thác của cán bộ quản lý và vận hành tại phòng máy chủ Trung tâm THDL:  - Xây dựng hệ thống mạng phải được thiết kế thống nhất, xác thực đối với tất cả người sử dụng, đảm bảo an toàn và bảo mật.  - Hệ thống mạng tại đơn vị phải được kiểm soát truy cập từ bên ngoài mạng; kiểm soát truy cập tại bên trong mạng; phòng chống phần mềm độc hại trên môi trường mạng.  - Việc thanh lý, tiêu hủy thiết bị, vật mang thông tin trong mạng của Trung tâm tích hợp dữ liệu (nếu không sử dụng nữa hoặc thay thế) luôn bảo đảm yêu cầu không để lộ, lọt thông tin Nhà nước. Có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản việc thanh lý, tiêu hủy. |

### 5. 2. Quản lý an toàn máy chủ và ứng dụng

|  |  |
| --- | --- |
| **Yêu cầu 01** | Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | 1. Trung tâm CNTT&TT có phương án quy định về quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ, một số nội dung như sau:  - Phần mềm hệ điều hành cài trên máy chủ hoặc máy trạm ưu tiên là phần mềm có bản quyền hoặc là phần mềm mã nguồn mở được sử dụng rộng rãi trong nước và quốc tế.  - Kiểm tra chặt chẽ cài đặt phần mềm trên máy chủ, máy trạm quản trị hệ thống.  - Thường xuyên theo dõi các bản ghi nhật ký trên các thiết bị máy tính, mạng máy tính, hệ điều hành, phần cứng ứng dụng, CSDL nhằm bảo đảm các sự kiện quan trọng xảy ra trên các thiết bị này; lưu trữ các sự kiện đó; các sự kiện có thể là sự truy cập trái phép, hoặc gây mất mát, làm thay đổi thông tin. |
| **Yêu cầu 02** | Có quy định về việc quản lý truy cập mạng của máy chủ |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Các thiết bị đặt tại Trung tâm dữ liệu tỉnh phải được kiểm duyệt và đáp ứng quy định về việc an toàn, an ninh thông tin do Trung tâm CNTT&TT quy định. |
| **Yêu cầu 03** | Có quy định về quản lý truy cập và quản trị máy chủ và ứng dụng |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Một số quy định về quản lý truy cập, quản trị máy chủ và ứng dụng tại phòng máy chủ Trung tâm THDL và các Phòng họp điểm cầu:  - Máy chủ và ứng dụng cài đặt lên nó phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Kết nối về hệ thống giám sát tập trung; Có phương án bảo mật thông tin liên lạc, chống chối bỏ và biện pháp bảo đảm an toàn ứng dụng và mã nguồn. |
| **Yêu cầu 04** | Có quy định về quản lý cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Khi vận hành, khai thác Trung tâm THDL phải xác lập cơ chế sao lưu và phục hồi máy chủ, máy trạm: Tiến hành sao lưu định kỳ dữ liệu quan trọng bằng các thiết bị sao lưu và phần mềm chuyên dùng nhằm phục vụ công tác phục hồi dữ liệu một cách nhanh, chính xác nhất.  - Trung tâm CNTT&TT và các Phòng họp điểm cầu phải thường trực phối hợp với Sở TT&TT (sở TT&TT là đơn vị chuyên trách về ATTT, chủ trì, xây dựng phương án ATTT cho các hệ thống thông tin của tỉnh) xây dựng phương án sao lưu dự phòng các dữ liệu quan trọng, và phục hồi dữ liệu nếu xảy ra sự cố. |
| **Yêu cầu 05** | Có quy định về quản lý cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Kiểm tra chặt chẽ cài đặt phần mềm trên máy chủ, máy trạm; bảo đảm thông tin chính xác, không bị thay đổi; phối hợp với các quản trị viên ở các điểm cầu để kiểm soát, phát hiện và khắc phục sự cố an toàn, an ninh thông tin.  - Không cài đặt phần mềm không rõ nguồn gốc, hoặc ảnh hưởng, can thiệp tới hoạt động bình thường của phần mềm ứng dụng.  - Phần mềm hệ điều hành cài lên máy chủ ưu tiên là phần mềm hệ điều hành có bản quyền hoặc là phần mềm mã nguồn mở được sử dụng rộng rãi trong nước và quốc tế.  - Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ. |
| **Yêu cầu 06** | Có quy định về quản lý kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Các cơ quan, đơn vị cài đặt hệ thống tin chuyên ngành, CSDL hoặc kết nối vào trung tâm THDL phải tuân thủ các chính sách đảm bảo ATTT liên quan đến việc kết nối vào trung tâm THDL.  - Các cơ quan, đơn vị khi kết nối vào trung tâm THDL phải tự bảo vệ thiết bị, hệ thống đầu cuối của mình và chịu trách nhiệm nếu bị xâm nhập trái phép, kiểm soát máy tính và gây sự cố cho trung tâm THDL.  - Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và thực hiện theo quy trình đã được phê duyệt.  - Việc quản lý kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống phải luôn đảm bảo nguyên tắc không ảnh hưởng đến sự đang phục vụ liên tục của hệ thống. |
| **Yêu cầu 07** | Có quy định về quản lý cấu hình tối ưu và tăng cường bảo mật cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án đáp ứng cho Trung tâm THDL luôn chuẩn bị sẵn sàng để đảm bảo các điều kiện về hạ tầng kỹ thuật, ATTT đối với hệ thống máy chủ, thiết bị kết nối mạng và các thiết bị khác. Đủ điều kiện về hệ thống máy chủ với cấu hình tối ưu và tăng cường bảo mật, trước khi đưa vào vận hành, khai thác. |

### 5. 3. Quản lý an toàn dữ liệu

|  |  |
| --- | --- |
| **Yêu cầu 01** | Quy định về quản lý sao lưu dự phòng và khôi phục dữ liệu |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Một số quy định về quản lý sao lưu dự phòng và khôi phục dữ liệu của cán bộ quản lý và vận hành tại phòng máy chủ Trung tâm THDL:  - Thực hiện thường xuyên việc quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.  - Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để bảo đảm sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố ATTT mạng xảy ra.  - Tiến hành cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ được thực hiện theo yêu cầu của đơn vị vận hành hệ thống.  - Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ.  - Quản lý chặt chẽ các thiết bị lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép của người có thẩm quyền.  - Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên. |
| **Yêu cầu 02** | Quy định về việc 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 |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Trung tâm CNTT&TT có phương án tiến hành sao lưu định kỳ dữ liệu hệ điều hành, phần mềm chuyên ngành, cơ sở dữ liệu quan trọng của hệ thống.  - Một số quy định về định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng của cán bộ quản lý và vận hành tại phòng máy chủ Trung tâm THDL:  - 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.  - 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. |

### 5. 4. Quản lý an toàn thiết bị đầu cuối

|  |  |
| --- | --- |
| **Yêu cầu 01** | Có quy định về quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Tất cả các máy tính tham gia vào vận hành được cài đặt và bảo vệ bởi phần mềm phòng chống vi rút, phần mềm độc hại.  - Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật.  - Giám sát các thiết bị kết nối đầu cuối hiệu quả bằng cách:  + Đặt tên cho các điểm cầu để giám sát  + Hiển thị, giám sát các thông tin về số lượng, chất lượng của cuộc họp, kết nối và điểm cầu như: số lượng phiên họp trên hệ thống, số lượng điểm cầu trong các phiên họp, chất lượng kết nối các điểm cầu (tốc độ băng thông, độ trễ, tỷ lệ mất gói... ) |
| **Yêu cầu 02** | Có quy định về quản lý kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Đối với tài khoản người dùng sử dụng để đăng nhập phải thiết lập mật khẩu có mức độ bảo mật cao, không sử dụng mật khẩu ngắn, mặc định nhằm đảm bảo an toàn, bảo mật thông tin của người dùng.  - Tổ chức quản lý tài khoản, định danh người dùng trong Trung tâm THDL bao gồm: tạo mới, kích hoạt, sửa đổi và loại bỏ tài khoản; đối với người dùng tham gia vào vận hành hệ thống nghỉ việc hoặc chuyển công tác phải có biện pháp khóa tài khoản, hủy quyền truy cập, thu hồi các thiết bị liên quan tới hệ thống. |
| **Yêu cầu 03** | Có quy định về cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt. = |

### 5. 5. Quản lý phòng chống phần mềm độc hại

|  |  |
| --- | --- |
| **Yêu cầu 01** | Có quy định về 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 |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Các máy tính trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin. |
| **Yêu cầu 02** | Có quy định về cài đặt, sử dụng phần mềm ứng dụng trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Không cho phép cài đặt phần mềm không rõ nguồn gốc hoặc can thiệp lên máy tính, làm ảnh hưởng đến Trung tâm THDL; hoặc cài đặt phần mềm khác lên máy tính mà chưa được sự cho phép của người có thẩm quyền.  - Một số quy định về cài đặt, sử dụng phần mềm ứng dụng trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng trong phòng máy chủ Trung tâm THDL, một số nội dung sau:  - Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng. |
| **Yêu cầu 03** | Có quy định về gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Việc sử dụng, chia sẻ và lưu trữ dữ liệu, thông tin số trên mạng nội bộ, mạng Internet phải tuân thủ các quy định của cơ quan đơn vị và quy định của pháp luật về viễn thông, công nghệ thông tin  - Sử dụng biện pháp kỹ thuật để mã hóa dữ liệu khi cần thiết bảo đảm không bị thay đổi trước khi truyền trên môi trường mạng. |
| **Yêu cầu 04** | Có quy định về việc định kỳ hàng năm 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 |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | -Trung tâm CNTT&TT có phương án quy định về việc định kỳ hàng năm 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. |

### 5. 6. Quản lý giám sát an toàn hệ thống thông tin

|  |  |
| --- | --- |
| **Yêu cầu 01** | Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống giám sát an toàn hệ thống thông tin |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Trung tâm CNTT&TT chịu sự chỉ đạo trực tiếp của lãnh đạo Sở TT&TT thực hiện việc chủ động giám sát, ứng cứu sự cố ATTT mạng, lựa chọn tổ chức, doanh nghiệp có đủ năng lực để thực hiện; thường xuyên phối hợp, thông báo thông tin đối với đơn vị đầu mối Đội ứng cứu sự cố ATTT của tỉnh trong công tác ứng cứu sự cố ATTT mạng.  - Trung tâm CNTT&TT chịu sự chỉ đạo trực tiếp của lãnh đạo Sở TT&TT là đầu mối thực hiện giám sát, chủ động chỉ đạo ứng cứu sự cố ATTT (nếu có sự cố mất ATTT xảy ra)  - Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại Khoản 1, Điều 5, Thông tư 31/2017/TT-BTTTT.  - Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại Khoản 2, Điều 5, Thông tư 31/2017/TT-BTTTT. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.  - Thực thi nhiệm vụ giám sát theo quy định tại Khoản 3, Điều 5, Thông tư số 31/2017/TT-BTTTT.  - Định kỳ hàng năm tổ chức nâng cao năng lực hoạt động giám sát theo quy định tại Điều 9, Thông tư số 31/2017/TT-BTTTT.  - Chủ quản hệ thống thông tin có trách nhiệm giám sát ATTT theo quy định tại Điều 14, Thông tư số 31/2017/TT-BTTTT. |
| **Yêu cầu 02** | Có quy định danh mục các đối tượng giám sát bao gồm: thiết bị hệ thống, máy chủ ứng dụng, dịch vụ và các thành phần khác trong hệ thống |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Một số quy định chung quản lý an toàn, Trung tâm CNTT&TT có phương án đảm bảo quy định về danh mục các đối tượng giám sát bao gồm: thiết bị hệ thống, máy chủ ứng dụng, dịch vụ và các thành phần khác trong hệ thống, tuân thủ một số nội dung sau:  - Danh mục đối tượng cần giám sát phải được thu thập từ nhật ký và cảnh báo của các phần mềm, thiết bị liên quan.  - Danh mục đối tượng cần giám sát phải được thu thập từ các thiết bị quan trắc cơ sở giúp phát hiện tấn công, rủi ro và cần được giám sát bao phủ được tất cả các đường kết nối mạng Internet.  - Danh mục đối tượng phục vụ Chính phủ điện tử phải được sử dụng giao thức mã hóa an toàn. |
| **Yêu cầu 03** | Có quy định về kết nối và gửi nhật ký hệ thống từ đối tượng giám sát và hệ thống giám sát |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án quy định về kết nối và gửi nhật ký hệ thống từ đối tượng giám sát và hệ thống giám sát, nội dung sau:  - Đối tượng cần giám sát phải được thu thập, ghi lại nhật ký, thống kê và hiển thị cảnh báo trực quan. |
| **Yêu cầu 04** | Có quy định về truy cập và quản trị hệ thống giám sát |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án quy định về truy cập và quản trị hệ thống giám sát, tuân thủ một số nội dung sau:  - Theo dõi, vận hành các thiết bị quan trắc cơ sở để đảm bảo ổn định, liên tục, điều chỉnh kịp thời khi có thay đổi.  - Lập báo cáo kết quả giám sát hàng tuần để báo cáo chủ quản hệ thống thông tin (thời gian, danh mục đối tượng bị tấn công đã phát hiện và chứng cứ liên quan, thay đổi hệ thống). Cung cấp thông tin giám sát, báo cáo hoạt động giám sát cho cấp trên định kỳ 06 tháng hàng năm.  - Xây dựng và ban hành các quy chế giám sát ATTT mạng, trong đó quy định cụ thể về thời hạn định kỳ thống kê kết quả xử lý, lập báo cáo. |
| **Yêu cầu 05** | Có quy định về loại thông tin cần được giám sát |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án quy định về loại thông tin cần được giám sát, tuân thủ một số nội dung sau:  **-** Phải phân loại thông tin được giám sát: thông tin công cộng, thông tin riêng, thông tin cá nhân; thông tin cấu hình hệ thống; thông tin bí mật nhà nước, … |
| **Yêu cầu 06** | Có quy định về lưu trữ và bảo vệ thông tin giám sát |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án quy định về lưu trữ và bảo vệ thông tin giám sát, tuân thủ một số nội dung sau:  - Thông tin giám sát phải được lưu trữ tự động an toàn trên thiết bị lưu trữ được quy định.  - Năng lực lưu trữ thông tin giám sát tối thiểu đạt mức trung bình 30 ngày hoạt động trong điều kiện bình thường (sau đó tự xóa khỏi thiết bị lưu trữ khi không cần thiết). |
| **Yêu cầu 07** | Có quy định về đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Một số quy định chung quản lý an toàn quy định về đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát, tuân thủ một số nội dung sau:  - Các thiết bị mạng, máy chủ tham gia hệ thống giám sát luôn được đồng bộ cùng về thời gian chuẩn đối với quốc gia Việt Nam. |
| **Yêu cầu 08** | Có quy định về theo dõi, giám sát và cảnh báo sự cố phát hiện được trên HTTT |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án quy định về theo dõi, giám sát và cảnh báo sự cố phát hiện được trên HTTT, tuân thủ một số nội dung sau:  - Hệ thống luôn được giám sát và theo dõi, cảnh báo sự cố qua các phần mềm trên máy tính quản trị trực tuyến.  - Các thiết bị mạng luôn được giám sát kết nối, lưu lượng hoặc truy cập bất thường bởi người quản trị mạng. |

### 5. 7. Quản lý điểm yếu an toàn thông tin

|  |  |
| --- | --- |
| **Yêu cầu 01** | Có quy định về quản lý thông tin các thành phần trong hệ thống có khả năng tồn tại điểm yếu ATTT: thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác nếu có |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có quy định về quản lý thông tin thành phần có khả năng tồn tại điểm yếu ATTT. Phương án như sau:  - Quản lý thông tin điểm yếu ATTT đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ, …);  - Báo cáo lãnh đạo ngay khi phát hiện điểm yếu ATTT ở mức độ nghiêm trọng;  - Thực hiện cảnh báo và xử lý điểm yếu ATTT theo chỉ đạo. Việc xử lý điểm yếu ATTT phải bảo đảm không giảm ảnh hưởng/gián đoạn hoạt động của hệ thống.  - Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu ATTT chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại. |
| **Yêu cầu 02** | Có quy định về quản lý, cập nhật nguồn cung cấp điểm yếu ATTT; phân nhóm và mức độ của điểm yếu các thành phần trong hệ thống đã được xác định |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án như sau:  - Phân loại mức độ nguy hiểm của các điểm yếu điểm yếu ATTT;  - Hoạt động đánh giá hiệu quả các biện pháp bảo đảm ATTT, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thực hiện theo quy định tại điểm c, khoản 2, điều 20, Nghị định số 85/2016/NĐ-CP và Điều 11 Thông tư số 12/2022/TT-BTTTT. |
| **Yêu cầu 03** | Có quy định về cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu ATTT. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trong quá trình quản lý, vận hành, Trung tâm CNTT&TT có phương án sau:  - Xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu.  - Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu ATTT đối với các điểm yếu khi cần thiết. |
| **Yêu cầu 04** | Có quy định về kiểm tra, đánh giá và xử lý điểm yếu ATTT cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án như sau:  - Kiểm tra, đánh giá và xử lý điểm yếu ATTT cho máy chủ, thiết bị mạng khi cài đặt bổ sung, hoặc thay thế thiết bị;  - Thường xuyên cập nhật phiên bản mới nhất cho Hệ điều hành máy chủ, phần mềm phiên bản máy chủ, thiết bị mạng, v. v… |
| **Yêu cầu 05** | Có quy định về việc định kỳ hàng năm kiểm tra, đánh giá điểm yếu ATTT 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. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án như sau:  - Định kỳ hàng năm kiểm tra, đánh giá điểm yếu ATTT cho các máy chủ, thiết bị mạng, thiết bị lưu trữ, phần mềm dịch vụ mail của hệ thống v. v…;  - 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; |

### 5. 8. Quản lý sự cố an toàn thông tin

|  |  |
| --- | --- |
| **Yêu cầu 01** | Có quy định về việc phân nhóm sự cố an toàn thông tin mạng. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | 1. Trung tâm CNTT&TT có quy định về việc phân nhóm sự cố ATTT mạng theo các tiêu chí sau:  - Việc phân nhóm sự cố cho Hệ thống ATTT mạng, AT HTTT sẽ căn cứ theo Quyết định  05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia);  - Việc phân nhóm sự cố ATTT mạng dựa trên các sự kiện có thể gặp phải như sau: Hệ thống bị gián đoạn dịch vụ; Dữ liệu tuyệt mật hoặc bí mật nhà nước có khả năng bị tiết lộ; Dữ liệu quan trọng của hệ thống không đảm bảo tính toàn vẹn và không có khả năng khôi phục được; Hệ thống bị mất quyền điều khiển; Sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền, làm tổn hại cho các HTTT cấp độ 3, 4, 5 khác;  - Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất ATTT theo chỉ đạo của Lãnh đạo.  - 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; Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.  - Tổ chức diễn tập phương án xử lý sự cố ATTT theo chỉ đạo của Lãnh đạo.  2. Trách nhiệm của người dùng: Thông tin, báo báo kịp thời cho cán bộ chuyên trách về ATTT của cơ quan khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin của đơn vị; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố. |
| **Yêu cầu 02** | Có quy định về phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTT. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án quy định về phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTT, một số nội dung sau:  - Đầu tiên là thu thập thông tin cảnh báo về sự cố, sau đó phân loại sự cố  - Báo cáo sự cố đối với người quản trị tại Trung tâm THDL. |
| **Yêu cầu 03** | Có quy định về xây dựng kế hoạch ứng phó với sự cố ATTT. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án quy định về xây dựng kế hoạch ứng phó với sự cố ATTT, một số nội dung:  - Trung tâm CNTT&TT sẽ chủ trì việc vận kiểm thử khi nào quá trình kiểm tra không có bất cứ lỗi nào xảy ra thì mới kết thúc vận hành thử.  - Tham mưu, cải tiến việc vận hành hiệu quả hệ thống, xây dựng kế hoạch ứng phó với sự cố ATTT mạng tỉnh Hải Dương trình UBND tỉnh phê duyệt (qua Sở TT&TT). |
| **Yêu cầu 04** | Có quy định về giám sát, phát hiện và cảnh báo cự cố ATTT. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án quy định về giám sát, phát hiện và cảnh báo cự cố ATTT, một số nội dung:  - Trong quá trình vận hành thử, tiến hành thu thập và cung cấp kịp thời thông tin thông báo, cảnh báo bằng văn bản về sự cố mạng máy tính, các điểm yếu, lỗ hổng bảo mật, các nguồn tấn công mạng để chủ động khắc phục ngay. |
| **Yêu cầu 05** | Có quy định về quy trình ứng cứu sự cố ATTT thông thường. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án quy định về quy trình ứng cứu sự cố ATTT thông thường, một số nội dung:  **- Phát hiện, tiếp nhận, ứng cứu ban đầu và thông báo sự cố**  **- Triển khai ứng cứu, ngăn chặn sự cố**  - Xử lý sự cố, gỡ bỏ và khôi phục  **- Tổng kết, đánh giá.** |
| **Yêu cầu 06** | Có quy định về quy trình ứng cứu sự cố ATTT nghiêm trọng. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án quy định về quy trình ứng cứu sự cố ATTT nghiêm trọng, một số nội dung:  - Tại phòng máy chủ Trung tâm THDL, nếu sự cố xảy ra, người cán bộ trực vận hành phải báo cáo ngay cơ quan cấp trên quản lý trực tiếp, phối hợp với Sở TT&TT để được hướng dẫn, hỗ trợ khắc phục. |
| **Yêu cầu 07** | Có quy định về cơ chế phối hợp với các cơ quan chức năng, các chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố ATTT. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án quy định về cơ chế phối hợp với các cơ quan chức năng, các chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố ATTT, một số nội dung:  - Trong đó tuân thủ theo quy định tại Điều 2, của Quyết định số 2979/QĐ-UBND, ngày 29/09/2017 về Việc thành lập Đội ứng cứu sự cố ATTT mạng tỉnh Hải Dương.  Đó là thực hiện trách nhiệm thành viên đầu mối của tỉnh trong mạng lưới ứng cứu sự cố máy tính, ATTT mạng trên toàn quốc. Liên kết phối hợp với các bộ phận ứng cứu máy tính, mạng máy tính của các tỉnh, thành phố khác nhằm ứng phó kịp thời khi xảy ra sự cố máy tính, mạng máy tính, mạng Internet dưới sự điều phối của Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT). |
| **Yêu cầu 08** | Định kỳ tổ chức diễn tập phương án xử lý sự cố ATTT. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Trung tâm CNTT&TT có phương án đáp ứng quy định về định kỳ tham gia diễn tập phương án xử lý sự cố ATTT.  Trong đó tuân thủ theo quy định tại Điều 2, của Quyết định số 2979/QĐ-UBND, ngày 29/09/2017 về Việc thành lập Đội ứng cứu sự cố ATTT mạng tỉnh Hải Dương. Đó là:  - Sở TT&TTthường xuyên cử cán bộ kỹ thuật của mình (thuộc Đội ứng cứu sự cố ATTT mạng tỉnh Hải Dương) tham gia diễn tập chuyên đề hằng năm về an toàn thông tin, ứng cứu sự cố mạng trên địa bàn tỉnh; phối hợp tham gia các cuộc diễn tập quốc gia, quốc tế (nếu được tham gia) do cơ quan điều phối quốc gia, Bộ Thông tin và Truyền thông tổ chức. Tham gia các chương trình bồi dưỡng, tập huấn, đào tạo, hội thảo nhằm nâng cao trình độ, nghiệp vụ, tăng cường nhận thức, phổ biến kiến thức liên quan bao gồm đào tạo về quy trình, quản lý rủi ro, chuẩn quốc tế về an toàn thông tin mạng; đào tạo nâng cao kiến thức pháp luật, đạo đức nghề nghiệp. |

### 5. 9. Quản lý an toàn người sử dụng đầu cuối

|  |  |
| --- | --- |
| **Yêu cầu 01** | Có quy định về quản lý truy cập, sử dụng tài nguyên nội bộ đối với người sử dụng đầu cuối |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | - Việc sử dụng, chia sẻ và lưu trữ dữ liệu, thông tin số trên mạng nội bộ, mạng Internet phải tuân thủ các quy định của cơ quan, đơn vị và quy định của pháp luật về viễn thông, công nghệ thông tin.  - Thường xuyên cập nhật chính sách, quy trình bảo đảm ATTT của đơn vị, hướng dẫn của cán bộ chuyên trách.  - Một số quy định về quản lý truy cập, sử dụng tài nguyên tại Phòng máy chủ Trung tâm THDL, một số nội dung như sau:  +Tổ chức quản lý chặt chẽ về tài khoản, định danh người dùng truy cập trong các hệ thống thông tin như: tạo mới, kích hoạt và loại bỏ tài khoản.  +Đối với tài khoản người dùng sử dụng để đăng nhập các hệ thống thông tin, phần mềm ứng dụng, cơ sở dữ liệu và các ứng dụng chuyên ngành khác phải thiết lập mật khẩu có mức bảo mật cao; Giới hạn số lần đăng nhập sai liên tiếp vào hệ thống; Hệ thống tự động khóa tài khoản trong một thời gian nhất định. |
| **Yêu cầu 02** | Có quy định về quản lý truy cập mạng và tài nguyên trên Internet |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Áp dụng Điều 3, Quy chế bảo đảm ATTT kèm theo Quyết định số 29/2013/QĐ-UBND ngày 11 tháng 12 năm 2013 của Ủy ban nhân dân tỉnh Hải Dương. Tại khoản 7 quy định:  Tạo tài khoản và phân quyền người dùng để truy nhập hệ thống thông tin; yêu cầu người dùng đặt mật khẩu với độ an toàn cao; thiết lập giới hạn một số hữu hạn lần đăng nhập sai liên tiếp vào hệ thống thông tin, nếu liên tục đăng nhập sai vượt quá số lần quy định thì hệ thống thông tin phải tự động khóa tài khoản hoặc cô lập tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập. |
| **Yêu cầu 03** | Có quy định về cài đặt và sử dụng máy tính an toàn |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | Áp dụng Điều 3, Quy chế bảo đảm ATTT kèm theo Quyết định số 29/2013/QĐ-UBND ngày 11 tháng 12 năm 2013 của Ủy ban nhân dân tỉnh Hải Dương, Tại khoản 1, 2, 3, 4, 5 quy định:  1. Tổ chức hệ thống mạng phù hợp để tăng cường tính bảo mật. Các cơ quan, đơn vị có nhiều phòng, ban, đơn vị trực thuộc không nằm trong cùng một khu vực, cần thiết lập mạng riêng ảo để bảo đảm an ninh cho mạng nội bộ. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin, hạn chế sử dụng các chức năng, cổng giao tiếp, giao thức và dịch vụ mạng không cần thiết.  2. Đối với việc lắp đặt mạng không dây để kết nối với mạng nội bộ, cần thiết lập, cấu hình các thông số, đặt mật khẩu và thường xuyên thay đổi mật khẩu nhằm bảo đảm công tác bảo mật.  3. Trang bị thiết bị chuyển mạch bảo đảm khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng.  4. Trang bị, cài đặt tường lửa bảo đảm khả năng xử lý được số lượng kết nối đồng thời cao và chịu được thông lượng cao, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu, cung cấp đầy đủ các cơ chế bảo mật, quản lý luồng dữ liệu ra vào và có khả năng bảo vệ hệ thống thông tin trước các loại tấn công từ chối dịch vụ; trang bị thiết bị phát hiện hoặc phòng chống xâm nhập trái phép.  5. Bố trí phòng máy chủ độc lập, bảo đảm khô, thoáng, nguồn điện cung cấp ổn định cao, được trang bị máy điều hòa nhiệt độ và cho vận hành liên tục, được lắp đặt thiết bị chống sét và hệ thống phòng cháy chữa cháy. Phòng máy chủ được giao cho cán bộ có chuyên môn về công nghệ thông tin trực tiếp quản lý, các cán bộ không liên quan không được vào phòng máy chủ. |

**PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT CẤP ĐỘ 3**

**1. Bảo đảm an toàn mạng**

**1. 1. Thiết kế hệ thống**

a) Các vùng mạng trong hệ thống:

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Vùng mạng nội bộ | Không có | Vùng mạng nội bộ độc tập, tách riêng khỏi hệ thống của trung tâm tích hợp dữ liệu |
| 2 | Vùng DMZ cổng | Có | Vùng máy chủ dịch vụ, cung cấp dịch vụ trực tiếp ra bên ngoài Internet |
| 3 | Vùng Core Cổng | Có | Vùng máy chủ core lưu trữ và quản lý cở sở dữ liệu của các hệ thống thành phần |
| 4 | Vùng máy chủ LGSP | Có | Cung cấp dịch vụ liên thông thông tin, danh mục dùng chung và dịch vu công trực tuyến |
| 5 | Vùng quản trị | Có | Server Management (Quản lý hạ tầng) cài đặt một tập hợp các công cụ quản trị và giám sát toàn bộ các thiết bị mạng, bảo mật, máy chủ và lưu trữ. |
| 6 | Vùng giao ban trực tuyến | Có | Quản lý và kết nối các điểm cầu giao ban hội nghi giao ban trực tuyến. |

b) Phương án bảo đảm an toàn thông tin

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn | Có | Các thiết bị hệ thống / máy chủ được thiết lập cấu hình VPN cho phép quản trị từ xa an toàn. |
| 2 | Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập | Có | Hệ thống sử dụng các tường lửa : Checkpoint 4200, fortinet, fortimail, fortigate. Chủng loại để kiểm soát truy cập và phòng chống xâm nhập giữa các vùng mạng của hệ thống. |
| 3 | Phương án cân bằng tải và dự phòng nóng cho các thiết bị mạng chính | Có | Các thiết bị mạng chính được thiết kế và cấu hình hoạt động ở chế độ A-A. Cụ thể:  - Firewall: FortiADC 300F, Fortinet (Dự phòng cho web app)  - Switch: Core switch Cisco WS-C3850  - SAN Storage: Dell SVC 2000 4TBx12 |
| 4 | Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu | Có | - Quản lý truy cập CSDL Checkpoint 4200  - Không kết nối internet trực tiếp cho các máy chủ CSDL.  - Cài đặt Phần mềm virus và cập nhật định kỳ cho máy chủ CSDL. (BKAV) |
| 5 | Phương án chặn lọc phần mềm độc hại trên môi trường mạng | Có | Hệ thống sử dụng các thiết bị Checkpoint 4200, license IPS, antivirus, DoS protection trên Firewall để chặn lọc phần mềm độc hại trên môi trường mạng |
| 6 | Phương án phòng chống tấn công từ chối dịch vụ | Không | Hệ thống sử dụng giải pháp AntiDDos được triển khai ở vùng mạng biên để thực hiện phát hiện và phòng chống tấn công DoS / DDoS |
| 7 | Phương án phòng, chống tấn công mạng cho ứng dụng web | Có | Sử dụng sản phẩm Tường lửa ứng dụng web để phòng, chống tấn công cho ứng dụng web |
| 8 | Phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử | Có | Hệ thống sử dụng Giải pháp Email Security Gateway để bảo đảm an toàn thông tin cho hệ thống thư điện tử công vụ. |
| 9 | Phương án quản lý truy cập lớp mạng | Không | Hệ thống sử dụng Giải pháp NAC |
| 10 | Phương án giám sát hệ thống thông tin tập trung | Không | Đầu tư giải pháp giám sát hệ thống thông tin tập trung (Network monitoring), để giám sát hiệu năng, trạng thái các thiết bị trong hệ thống. |
| 11 | Phương án giám sát an toàn hệ thống thông tin tập trung | KHông | Hệ thống sử dụng giải pháp ArcSight /Splunk / Qradar / LogRhythm được triển khai ở vùng mạng quản trị, cho phép quản trị tập trung nhật ký hệ thống từ các thiết bị / máy chủ |
| 12 | Phương án quản lý sao lưu dự phòng tập trung | Có | Sử dụng hệ thống SAN, có năng lực quản lý và lưu trữ T dữ liệu. |
| 13 | Có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ / máy tính người dùng tập trung | Có | Sử dụng giải pháp AntiVirus có chức năng quản lý tập trung hoặc hệ thống EDR. |
| 14 | Có phương án phòng, chống thất thoát dữ liệu | Không | Sử dụng giải pháp / Thiết bị DLP (Data loss prevention). |
| 15 | 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 | Có | Sử dụng đồng thời hai kết nối Internet của hai nhà cung cấp dịch vụ khác nhau để đảm bảo kết nối không bị gián đoạn |
| 16 | Có phương án bảo đảm an toàn cho mạng không dây (nếu có) | N/A |  |

**1. 2. Kiểm soát truy cập từ bên ngoài mạng**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | 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 | Có | Hệ thống được thiết lập trên FW Checkpoint 4200 |
| 2 | 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 | Có | Hệ thống được thiết lập chỉ cho phép kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể.  Chính sách được thiết lập trên FW theo chiều từ bên ngoài vào vùng DMZ. |
| 3 | Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng. | Có | Thiết lập giới hạn thời gian chờ để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng được thiết lập trên các FW |
| 4 | 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. | Có | Thực hiện chính sách trên thiết bị VPN Gateway tại vùng mạng biên. Mỗi người sử dụng sẽ có tài khoản khác nhau, khi kết nối VPN sẽ nhận được địa chỉ IP và chính sách truy cập vào hệ thống khác nhau. |
| 5 | 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 | Có | 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 thiết lập trên các FW Checkpoint |

**1. 3 Kiểm soát truy cập từ bên trong mạng**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | 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 | Có | Chính sách kiểm soát truy cập từ các vùng mạng trong hệ thống đi ra các mạng bên ngoài và mạng Internet được thiết lập trên các cặp tương ứng như kiểm soát truy cập từ bên ngoài trên các FW |
| 2 | Giới hạn truy cập các ứng dụng, dịch vụ bên ngoài theo thời gian | Có | Giới hạn truy cập các ứng dụng, dịch vụ bên ngoài theo thời gian được thiết lập trên FW |
| 3 | 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 | Chưa có | Trung tâm dữ liệu có vùng mạng nội bộ. Do đó, yêu cầu này sẽ nghiên cứu áp dụng trong trường hợp cụ thể. |

**1. 4. Nhật ký hệ thống**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yêu cầu** | Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống | Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian | Lưu trữ và quản lý tập trung nhật ký hệ thống | Lưu trữ nhật ký hệ thống của thiết bị tối thiểu 03 tháng |
| **Thiết bị** |
| FW Checkpoint 4200 | + | + | + | + |
| FW Fortinet, fortiADC, fortimail,  fortiGate  (Hệ thống LGSP) | + | + | + | + |
| SAN | + | + | + | + |

**1. 5. Phòng chống xâm nhập**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống | Chưa có | Các vùng mạng được triển khai hệ thống NIPS01-05, hoạt động ở chế độ Inline cho phép phát hiện và phòng chống xâm nhập. |
| 2 | Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng | Chưa có | Đã thiết lập chức năng tự động cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng đều được thiết lập trên các thiết bị IDS/IPS NIPS01-05. |
| 3 | 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 | Chưa có | Các IDS/IPS NIPS01-05 có năng lực xử lý đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp. |

**1. 6. Phòng chống phần mềm độc hại trên môi trường mạng**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Có phương án phòng chống phần mềm độc hại trên môi trường mạng | Có | Chức năng phòng chống phần mềm độc hại trên môi trường mạng được tích hợp trên các Firewall. Các Firewall Checkpoint 4200, FortiADC, fortiNet, fortiMail, fortiGate được thiết lập cấu hình để có thể phát hiện ra các hành vi mã độc trên môi trường mạng. |
| 2 | Định kỳ cập nhật dữ liệu cho hệ thống phòng chống phần mềm độc hại | Có | Đã thiết lập chức năng cập nhật dữ liệu cho hệ thống phòng chống phần mềm độc hại trên các Firewall có tích hợp chức năng phòng chống phần mềm độc hại trên môi trường mạng. |
| 3 | 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 | Có | Các Firewall có tích hợp chức năng phòng chống phần mềm độc hại trên môi trường mạng có năng lực xử lý đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp. |

**1. 7. Bảo vệ thiết bị hệ thống**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Yêu cầu** | Cấu hình chức năng xác thực trên các thiết bị | Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa | Hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa | Hạn chế được số lần đăng nhập sai | Phân quyền truy cập, quản trị thiết bị | Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng |
| **Thiết bị** |
| FW Checkpoint 4200 | + | + | + | + | + | + |
| SAN | + | + | + | + | + | + |

**2. Bảo đảm an toàn máy chủ**

**2. 1. Xác thực**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Yêu cầu** | Thiết lập chính sách xác thực trên máy chủ | Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa | Thiết lập chính sách mật khẩu an toàn | Hạn chế số lần đăng nhập sai | vô hiệu hóa tài khoản nếu tài khoản đó đăng nhập sai nhiều lần vượt số lần quy định |
| **Máy chủ** |
| Dell Power Edge R730/  Cài đặt Web-frontend01/  Vùng DMZ/  HĐH Window server 2019 | + | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-frontend02/  Vùng DMZ/  HĐH Window server 2019 | + | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-DB01/  Vùng Core/  HĐH Window server 2019 | + | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-DB02/  Vùng Core/  HĐH Window server 2019 | + | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-App\_farm/  Vùng Core/  HĐH Window server 2019 | + | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-AD01/  Vùng Core/  HĐH Window server 2019 | + | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-AD02/  Vùng Core/  HĐH Window server 2019 | + | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-ServerHosting/  Vùng DMZ/  HĐH Window server 2012R2 | + | + | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10  /Máy vật lý dùng ảo hóa 01 /  Vùng LGSP/  HĐH Window server 2019 | + | + | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10  /Máy vật lý dùng ảo hóa 02 /  Vùng LGSP/  HĐH Window server 2019 | + | + | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10/  Máy ESB 01/  Vùng LGSP/  HĐH RedHat | + | + | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10/  Máy ESB 02/  Vùng LGSP/  HĐH RedHat | + | + | + | + | + |

**2. 2. Kiểm soát truy cập**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yêu cầu** | Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa | Thiết lập giới hạn thời gian chờ (timeout) | Thay đổi cổng quản trị mặc định của máy chủ | Giới hạn địa chỉ mạng được phép truy cập, quản trị máy chủ từ xa |
| **Máy chủ** |
| Dell Power Edge R730/  Cài đặt Web-frontend01/  Vùng máy DMZ/  HĐH Window server 2019 | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-frontend02  /Vùng máy DMZ/  HĐH Window server 2019 | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-DB01/  Vùng Core/  HĐH Window server 2019 | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-DB02/  Vùng Core/  HĐH Window server 2019 | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-App\_farm/  Vùng Core/  HĐH Window server 2019 | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-AD01/  Vùng Core/  HĐH Window server 2019 | + | + | + | + |
| Dell Power Edge R730 /  Cài đặt Web-AD02/  Vùng Core /  HĐH Window server 2019 | + | + | + | + |
| Dell Power Edge R730 /  Cài đặt Web-ServerHosting /  Vùng DMZ /  HĐH Window server 2012R2 | + | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10  /Máy vật lý dùng ảo hóa 01 /  Vùng LGSP/  HĐH Window server 2019 | + | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10  /Máy vật lý dùng ảo hóa 02 /Vùng LGSP/HĐH Window server 2019 | + | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10 /  Máy ESB01 (Enterprise Service Bus) /  Vùng LGSP/  Red Hat | + | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10  /Máy ESB02 (Enterprise Service Bus) /  Vùng LGSP/  Red Hat | + | + | + | + |

**2. 3. Nhật ký hệ thống**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Yêu cầu** | Thiết lập lập chức năng ghi nhật ký hệ thống trên các máy chủ | Đồng bộ thời gian giữa máy chủ với máy chủ thời gian | Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống để không mất hoặc tràn nhật ký hệ thống | Quản lý và lưu trữ tập trung nhật ký hệ thống thu thập được từ máy chủ | Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 03 tháng |
| **Máy chủ** |
| Dell Power Edge R730/  Cài đặt Web-frontend01/  Vùng máy DMZ/  HĐH Window server 2019 | + | + | + | + | + |
| Dell Power EdgeR730/  Cai đặt Web-frontend02/ Vùng máy DMZ/  HĐH Window server 2019 | + | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-DB01/  Vùng Core/  HĐH Window server 2019 | + | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-DB02/  Vùng Core/  HĐH Window server 2019 | + | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-AD01/  Vùng Core/  HĐH Window server 2019 | + | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-AD02/  Vùng Core/  HĐH Window server 2019 | + | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web Server Hosting/  Vùng DMZ/  HĐH Window server 2012R2 | + | + | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10  /Máy vật lý dùng ảo hóa 01 /Vùng LGSP/HĐH Window server 2019 | + | + | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10  /Máy vật lý dùng ảo hóa 02 /Vùng LGSP/HĐH Window server 2019 | + | + | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10  /Máy ESB01/Vùng LGSP/HĐH  RED HAT | + | + | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10  /Máy ESB02/Vùng LGSP/HĐH RED HAT | + | + | + | + | + |

**2. 4. Phòng chống xâm nhập**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yêu cầu** | Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ | Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ | Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng | Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng |
| **Máy chủ** |
| Dell Power Edge R730/  Cài đặt Web-frontend01/  Vùng máy DMZ/  HĐH Window server 2019 | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-frontend02/  Vùng máy DMZ/  HĐH Window server 2019 | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-DB01/  Vùng Core/  HĐH Window server 2019 | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-DB02/  Vùng Core/  HĐH Window server 2019 | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-AD01/  Vùng Core/  HĐH Window server 2019 | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-AD02/  Vùng Core/  HĐH Window server 2019 | + | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-ServerHosting/  Vùng DMZ/  HĐH Window server 2012R2 | + | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10  /Máy vật lý dùng ảo hóa 01 /  Vùng LGSP/  HĐH Window server 2019 | + | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10  /Máy vật lý dùng ảo hóa 02 /  Vùng LGSP/  HĐH Window server 2019 | + | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10  /Máy ESB01/  Vùng LGSP/  HĐH Window server 2019 | + | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10  /Máy ESB02 /  Vùng LGSP/  HĐH Window server 2019 | + | + | + | + |

**2. 5. Phòng chống phần mềm độc hại**

|  |  |  |  |
| --- | --- | --- | --- |
| **Yêu cầu** | Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật | Kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt | Quản lý tập trung các phần mềm phòng chống mã độc cài đặt trên máy chủ |
| **Máy chủ** |
| Dell Power Edge R730/  Cài đặt Web-frontend01/  Vùng máy DMZ/  HĐH Window server 2019 | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-frontend02/  Vùng máy DMZ/  HĐH Window server 2019 | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-DB01/  Vùng Core/  HĐH Window server 2019 | + | + | + |
| Dell Power Edge R730/  Cài đặt WebDB02/  Vùng Core/  HĐH Window server 2019 | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-AD01/  Vùng Core/  HĐH Window server 2019 | + | + | + |
| Dell Power Edge R730/  Cài đặt Web-AD02/  Vùng Core/  HĐH Window server 2019 | + | + | + |
| Dell Power Edge R730/Cài đặt Web-ServerHosting  /Vùng DMZ/  HĐH Window server 2012R2 | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10  /Máy vật lý dùng ảo hóa 01 /Vùng LGSP/HĐH Window server 2019 | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10  /Máy vật lý dùng ảo hóa 02 /  Vùng LGSP/  HĐH Window server 2019 | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10 /Máy ESB01 /Vùng LGSP/  HĐH Window server 2019 | + | + | + |
| Máy chủ HPE ProLiant DL360 Gen10 /Máy ESB02 / Vùng LGSP/  HĐH Window server 2019 | + | + | + |

**2. 6. Xử lý máy chủ khi chuyển giao**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng | Có | Sử dụng giải pháp đi kèm HĐH |
| 2 | 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 | Có | Sử dụng các giải pháp sao lưu trên các hệ thống máy chủ, SAN để thực hiện sao lưu dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành |
| 3 | Có biện pháp kiểm tra, bảo đảm dữ liệu không thể khôi phục sau khi xóa | Có | Format cấp thấp hệ thiết bị.  Hủy thiết bị cũ/hỏng |

**3. Bảo đảm an toàn ứng dụng**

**3. 1. Xác thực**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Yêu cầu** | Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng | Lưu trữ có mã hóa thông tin xác thực hệ thống | Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng | Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định | Mã hóa thông tin xác thực trước khi gửi qua môi trường mạng | Thiết lập cấu hình ứng dụng để ngăn cản việc đăng nhập tự động đối với các ứng dụng |
| **Ứng dụng** |
| Cổng thông tin điển từ | + | + | + | + | + | + |
| Hệ thống thư điện tử công vụ tỉnh Hải Dương | + | + | + | + | + | + |
| Hệ thống dịch vụ công trực tuyến tỉnh Hải Dương | + | + | + | + | + | + |
| Hệ thống Giao ban trực tuyến tỉnh Hải Dương | + | + | + | + | + | + |
| Hệ thống LGSP | + | + | + | + | + | + |

**3. 2. Kiểm soát truy cập**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Yêu cầu** | Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa | Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng | Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa | Phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của ứng dụng với từng người/nhóm sử dụng | Giới hạn số lượng các kết nối đồng thời (kết nối khởi tạo và đã thiết lập) đối với các ứng dụng |
| **Ứng dụng** |
| Cổng thông tin điện tử | + | + | + | + | + |
| Hệ thống thư điện tử công vụ tỉnh Hải Dương | + | + | + | + | + |
| Hệ thống dịch vụ công trực tuyến tỉnh Hải Dương | + | + | + | + | + |
| Hệ thống Giao ban trực tuyến tỉnh Hải Dương | + | + | + | + | + |
| Hệ thống LGSP | + | + | + | + | + |

**3. 3. Nhật ký hệ thống**

|  |  |  |  |
| --- | --- | --- | --- |
| **Yêu cầu** | Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: (1) Thông tin truy cập ứng dụng (2) Thông tin đăng nhập khi quản trị ứng dụng; (3) Thông tin các lỗi phát sinh trong quá trình hoạt động (4) Thông tin thay đổi cấu hình ứng dụng | Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung | Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 03 tháng |
| **Ứng dụng** |
| Cổng thông tin điện tử | + | + | + |
| Hệ thống thư điện tử công vụ tỉnh Hải Dương | + | + | + |
| Hệ thống dịch vụ công trực tuyến tỉnh Hải Dương | + | + | + |
| Hệ thống Giao ban trực tuyến tỉnh Hải Dương | + | + | + |
| Hệ thống LGSP | + | + | + |

**3. 4. Bảo mật thông tin liên lạc**

|  |  |  |
| --- | --- | --- |
| **Yêu cầu** | 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. | 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 |
| **Ứng dụng** |
| Cổng thông tin điện tử | + | + |
| Hệ thống thư điện tử công vụ tỉnh Hải Dương | + | + |
| Hệ thống dịch vụ công trực tuyến tỉnh Hải Dương | + | + |
| Hệ thống Giao ban trực tuyến tỉnh Hải Dương | + | + |
| Quản lý LGSP | + | + |

**3. 5. Chống chối bỏ**

|  |  |
| --- | --- |
| **Yêu cầu** | Sử dụng chữ ký số khi trao đổi thông tin, dữ liệu quan trọng |
| **Ứng dụng** |
| Cổng thông tin điển tử | + |
| Hệ thống thư điện tử công vụ tỉnh Hải Dương | + |
| Hệ thống dịch vụ công trực tuyến tỉnh Hải Dương | + |
| Hệ thống Giao ban trực tuyến tỉnh Hải Dương | + |
| Hệ thông liên thông dữ liệu LGSP | + |

**3. 6. An toàn ứng dụng và mã nguồn**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yêu cầu** | Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý | Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu | Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa | 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 |
| **Ứng dụng** |
| Công thông tin điện tử | + | + | + | + |
| Hệ thống thư điện tử công vụ tỉnh Hải Dương | + | + | + | + |
| Hệ thống dịch vụ công trực tuyến tỉnh Hải Dương | + | + | + | + |
| Hệ thống Giao ban trực tuyến tỉnh Hải Dương | + | + | + | + |
| Hệ thống LGSP | + | + | + | + |

**4. Bảo đảm an toàn dữ liệu**

**4. 1. Nguyên vẹn dữ liệu**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn | Có | Dữ liệu quan trọng trên hệ thống bao gồm dữ liệu: dữ liệu nghiệp vụ, văn bản điện tử quan trọng và dữ liệu cấu hình hệ thống.  Dữ liệu được nén và được lưu trữ cùng mã kiểm tra MD5 trên hệ thống SAN. |

**4. 2. Bảo mật dữ liệu**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | 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 | Có | Dữ liệu quan trọng trên hệ thống bao gồm dữ liệu: dữ liệu nghiệp vụ, văn bản điện tử quan trọng và dữ liệu cấu hình hệ thống.  Dữ liệu được nén và được lưu trữ mã hóa sử dụng công cụ XXX (hỗ trợ các chuẩn mã hóa: DES, AES,…) trên hệ thống SAN. |

**4. 3. Sao lưu dự phòng**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | 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 | Có | Thông tin, dữ liệu được lưu trữ và quản lý tập trung trên hệ thống lưu trữ SAN. |
| 2 | Phân loại và quản lý các dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau | Có | Thông tin dữ liệu được phân theo từng nhóm theo đặc trưng nghiệp vụ hoặc chức năng. Được quy định về việc đặt tên các tập tin/thư mục khi lưu trữ trên hệ thống. |
| 3 | Có hệ thống/phương tiện lưu trữ độc lập để sao lưu dự phòng | Có | Hệ thống SAN được phân vùng lưu trữ riêng để phục vụ việc lưu trữ thông tin, dữ liệu. |