

## **Phần 2. YÊU CẦU VỀ KỸ THUẬT**

### **Chương V. YÊU CẦU VỀ KỸ THUẬT**

#### **I. GIỚI THIỆU CHUNG VỀ DỰ ÁN, GÓI THẦU:**

- Tên gói thầu: Thuê dịch vụ nền tảng trực chia sẻ LGSP; kết nối với NGSP
- Địa điểm cung cấp dịch vụ: tỉnh Tuyên Quang.
- Hình thức hợp đồng: Trọn gói.
- Nguồn vốn: Quyết định số 1526/QĐ-UBND ngày 10 tháng 12 năm 2025 của UBND tỉnh Tuyên Quang.
- Hình thức lựa chọn nhà thầu: Đấu thầu rộng rãi, trong nước qua mạng.
- Phương thức lựa chọn nhà thầu: Một giai đoạn, một túi hồ sơ.
- Thời gian thực hiện hợp đồng: 10 tháng.

#### **II. NỘI DUNG VÀ QUY MÔ THUÊ DỊCH VỤ**

##### **1. Các hạng mục chính cần thuê**

Các hạng mục chính cần thuê gồm:

- a) Dịch vụ tích hợp và Hạ tầng vận hành Nền tảng trực chia sẻ LGSP, kết nối với NGSP (*Đã bao gồm: Dịch vụ bảo mật; Quản trị, vận hành hệ thống; Bảo trì dịch vụ*)
- b) Các nội dung liên quan đến cung cấp dịch vụ:

- Đào tạo, hướng dẫn sử dụng phần mềm

##### **2. Mục tiêu**

Thuê dịch vụ công nghệ thông tin “Dịch vụ tích hợp và Hạ tầng vận hành Nền tảng trực chia sẻ LGSP, kết nối với NGSP” nhằm:

##### **Mục tiêu chung:**

- Đảm bảo việc tuân thủ Khung kiến trúc chính phủ điện tử Việt Nam phiên bản 4.0 (*được ban hành tại Quyết định số 292/QĐ-BKHCN ngày 25 tháng 3 năm 2025 của Bộ Khoa học và Công nghệ ban hành Khung Kiến trúc Chính phủ số Việt Nam, phiên bản 4.0;*) và Khung kiến trúc Chính quyền điện tử tỉnh Tuyên Quang phiên bản 4.0 (*được ban hành tại Quyết định số 800/QĐ-UBND ngày 07/10/2025 của UBND tỉnh Tuyên Quang*) trong triển khai và mở rộng các hệ thống thông tin trên địa bàn tỉnh;
- Đảm bảo chất lượng hệ thống cốt lõi, nền tảng cho các hệ thống thông tin trên địa bàn tỉnh kết nối và chia sẻ dữ liệu, đặc biệt là với các CSDL, hệ thống chuyên ngành của Quốc gia nhằm đẩy nhanh tiến độ hoàn thành nhiệm vụ Chính phủ, Thủ tướng Chính phủ, Ủy ban Quốc gia về chuyển đổi số, Ban Chỉ đạo cải cách hành chính của Chính phủ, Tổ công tác triển khai Đề án 06, Tổ công tác Cải cách TTHC của Thủ tướng Chính phủ, Văn phòng Chính phủ, Bộ Nội vụ, Bộ Khoa học và Công nghệ, Bộ Công

an... giao cho tỉnh về việc thực hiện cải cách TTHC, thực hiện cơ chế một cửa, một cửa liên thông, thực hiện TTHC trên môi trường điện tử, cung cấp dịch vụ công trực tuyến.

- Đảm bảo hạ tầng kỹ thuật, tạo nền tảng phát triển Chính quyền điện tử hướng tới Chính quyền số; đảm bảo an toàn, an ninh thông tin. Tích hợp, kết nối các hệ thống thông tin, tạo lập môi trường chia sẻ thông tin qua mạng rộng khắp giữa các cơ quan.

### **Mục tiêu cụ thể:**

- Đáp ứng các yêu cầu, tiêu chuẩn kỹ thuật về Nền tảng tích hợp và chia sẻ dữ liệu (LGSP) cấp tỉnh theo quy định; đảm bảo phù hợp với Kiến trúc Chính quyền điện tử hướng đến chính quyền số tỉnh Tuyên Quang, phiên bản 4.0; tuân thủ Nghị định số 278/2025/NĐ-CP ngày 20/10/2025 của Chính phủ Quy định về kết nối, chia sẻ dữ liệu bắt buộc giữa các cơ quan thuộc hệ thống chính trị; đáp ứng kết nối, chia sẻ dữ liệu với các Hệ thống thông tin giải quyết TTHC, CSDL Quốc gia và CSDL, hệ thống thông tin chuyên ngành khác có liên quan trên địa bàn tỉnh

- Đảm bảo các quy định về an toàn thông tin; được phát triển dưới hình thức ứng dụng trực tuyến, đảm bảo vận hành liên tục trên mạng Internet, mạng truyền số liệu chuyên dùng; đáp ứng các yêu cầu chức năng, nghiệp vụ theo các quy định; Đảm bảo hoạt động xuyên suốt, lưu thông thông tin liên tục không bị gián đoạn;

- Góp phần đẩy mạnh cải cách hành chính, nâng cao hiệu quả hoạt động của các cơ quan nhà nước, hướng tới xây dựng Chính quyền số, hỗ trợ, phục vụ người dân và doanh nghiệp thực hiện giải quyết thủ tục hành chính trên môi trường mạng.

- Giảm chi phí đầu tư từ nguồn ngân sách nhà nước, tạo tiền đề trong chiến lược xây dựng chính quyền điện tử tại địa phương, đẩy mạnh đầu tư ứng dụng CNTT trong hoạt động CQNN tỉnh Tuyên Quang.

### **3. Nội dung và quy mô**

Thuê dịch vụ công nghệ thông tin “Dịch vụ tích hợp và Hạ tầng vận hành Nền tảng trực chia sẻ LGSP, kết nối với NGSP” gồm: Các module tích hợp mở rộng, hạ tầng vận hành chính thức hệ thống (*Đã bao gồm: Dịch vụ bảo mật; Quản trị, vận hành hệ thống; Bảo trì dịch vụ*) đảm bảo an toàn thông tin phục vụ liên thông kết nối chia sẻ dữ liệu nội tỉnh và chia sẻ dữ liệu quốc gia.

Triển khai cho đối tượng sử dụng là các cơ quan, đơn vị thực hiện kết nối, chia sẻ thông tin, dữ liệu với các hệ thống thông tin chuyên ngành trên địa bàn tỉnh và các hệ thống thông tin, CSDL chuyên ngành của Quốc gia.

### **4. Địa điểm, cơ quan và đơn vị sử dụng dịch vụ**

- Cơ quan chủ trì thuê: Sở Khoa học và Công nghệ tỉnh Tuyên Quang

- Đơn vị sử dụng dịch vụ:

Sở Khoa học và Công nghệ tỉnh Tuyên Quang; các Sở, ban, ngành; UBND các xã/phường/ và các cơ quan hành chính nhà nước trên địa bàn tỉnh Tuyên Quang; Cơ quan, tổ chức có nhu cầu sử dụng dịch vụ tích hợp, chia sẻ dữ liệu chuyên ngành.

### III. YÊU CẦU VỀ CHẤT LƯỢNG THỰC HIỆN, TRIỂN KHAI THUÊ DỊCH VỤ

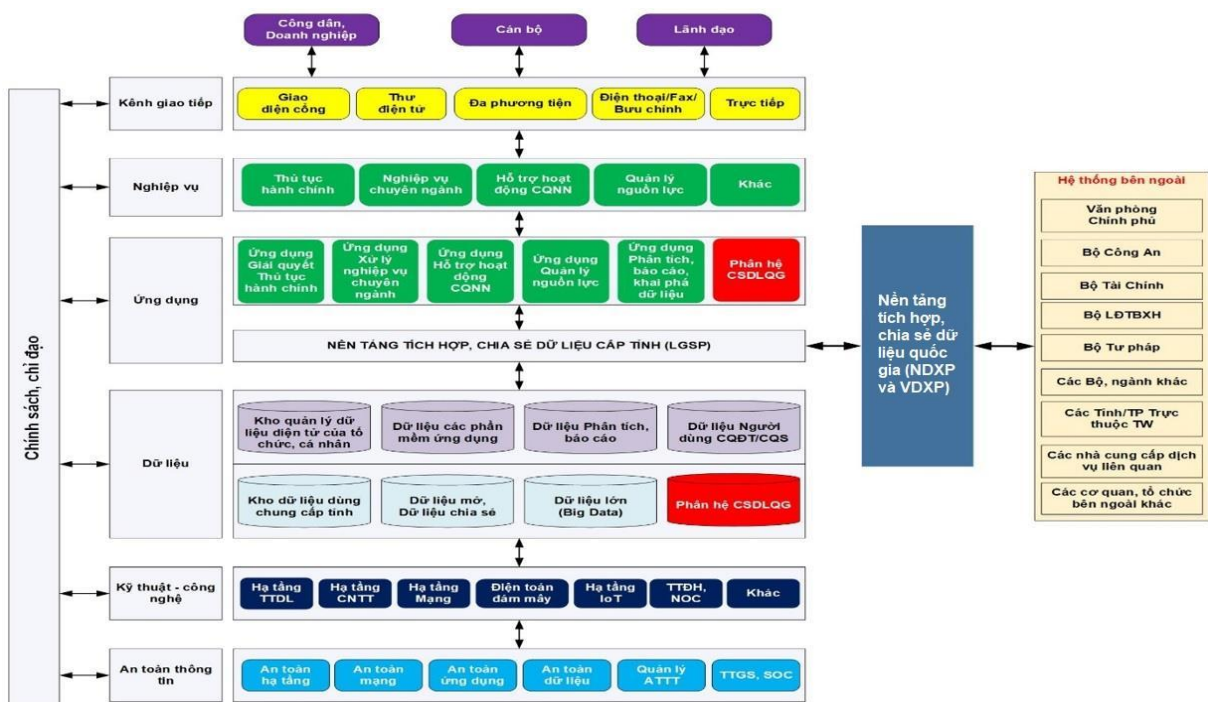
#### 1. Yêu cầu chung

Dịch vụ tích hợp và Hạ tầng vận hành Nền tảng trực chia sẻ LGSP, kết nối với NGSP bảo đảm đáp ứng các yêu cầu sau:

- Việc thuê dịch vụ CNTT tuân thủ đúng các nguyên tắc, quy định của pháp luật hiện hành về thuê dịch vụ CNTT và các quy định liên quan. Đảm bảo tính đồng bộ, kế thừa, khai thác và kết nối với các hạ tầng, hệ thống, CSDL hiện có; Tương thích, kết nối đảm bảo tính an toàn, không xung đột; khắc phục kịp thời khi có sự cố. Hệ thống hạ tầng được thuê cần đảm bảo tính hiện đại, đồng bộ, có khả năng mở rộng và phù hợp với sự phát triển của công nghệ trong tương lai.

- Hệ thống khi triển khai đáp ứng được yêu cầu về tính sẵn sàng phục vụ chuyển đổi số tỉnh Tuyên Quang đảm bảo tuân thủ các quy định hiện hành; Bảo đảm khả năng truy cập thuận tiện, an toàn, bảo mật cho người dùng và các hệ thống kết nối chia sẻ dữ liệu.

- Tuân thủ Khung kiến trúc Chính phủ điện tử, và Kiến trúc Chính quyền điện tử tỉnh Tuyên Quang (*Dịch vụ tích hợp và Hạ tầng vận hành Nền tảng trực chia sẻ LGSP, kết nối với NGSP sau khi triển khai đảm bảo LGSP là thành phần Dịch vụ chia sẻ và tích hợp thuộc Khung kiến trúc chính quyền điện tử tỉnh Tuyên Quang được ban hành tại Quyết định số 800/QĐ-UBND ngày 07/10/2025 của Ủy ban nhân dân tỉnh Tuyên Quang Ban hành Khung kiến trúc Chính quyền số tỉnh Tuyên Quang, phiên bản 4.0*)



Khung kiến trúc chính quyền điện tử tỉnh Tuyên Quang (phiên bản 4.0)

- Kết nối, chia sẻ, khai thác dữ liệu với các hệ thống thông tin, cơ sở dữ liệu của các cơ quan nhà nước (gồm Công Dịch vụ công quốc gia; các hệ thống thông tin nội bộ của tỉnh; các cơ sở dữ liệu quốc gia; hệ thống thông tin có quy mô, phạm vi từ trung ương đến địa phương) để sử dụng lại thông tin, dữ liệu đã có, phục vụ giải quyết thủ tục hành chính trên môi trường mạng.

- Các cơ quan, đơn vị liên quan có trách nhiệm chỉ đạo tổ chức triển khai thực hiện kế hoạch đảm bảo tiến độ, sử dụng đạt hiệu quả cao các dịch vụ. Bảo đảm khả năng kết nối, chia sẻ dữ liệu khác theo quyết định của Chủ tịch Ủy ban nhân dân tỉnh Tuyên Quang.

## **2. Các tiêu chí, yêu cầu chất lượng cụ thể và yêu cầu đầu ra của dịch vụ**

### **2.1 Yêu cầu về Công nghệ áp dụng**

Hệ thống sau khi triển khai cần tuân thủ đáp ứng theo công văn số 631/THH-THHT về việc hướng dẫn yêu cầu về chức năng, tính năng kỹ thuật của nền tảng chia sẻ, tích hợp dùng chung cấp tỉnh và Công văn số 677/BTTTT-THH ngày 03/3/2022 của Bộ Thông tin và Truyền thông về việc hướng dẫn kết nối và chia sẻ dữ liệu qua nền tảng tích hợp, chia sẻ dữ liệu quốc gia; Đảm bảo tính tương thích về công nghệ, khả năng nâng cấp, mở rộng, cập nhật (nếu có); Đảm bảo chất lượng các kết nối hiện có và cung cấp bổ sung các phân hệ kết nối liên thông dữ liệu mới, bao gồm:

- Kết nối dịch vụ Cơ sở dữ liệu đất đai
- Kết nối dịch vụ công chức viên chức
- Kết nối Cơ sở dữ liệu Đăng kiểm phương tiện
- Kết nối dịch vụ Cấp Mã số ngân sách
- Kết nối Dịch vụ Tài nguyên môi trường
- Kết nối Dịch vụ công Bộ Xây dựng
- Kết nối Dịch vụ EVN
- Kết nối Dịch vụ Bộ Giao thông vận tải
- Kết nối Dịch vụ DMDC Ngân hàng nhà nước
- Kết nối Dịch vụ DMDC Bộ Tài chính
- Kết nối Cơ sở dữ liệu quốc gia về giá
- Kết nối hệ thống thông tin Nguồn trung ương

### **2.2 Yêu cầu về hạ tầng vận hành dịch vụ**

#### **a) Yêu cầu về địa điểm cài đặt**

Hạ tầng máy chủ được triển khai tại Hệ thống hạ tầng của Nhà cung cấp dịch vụ.

#### **a) Yêu cầu về chuẩn bị hạ tầng cài đặt.**

- Phương án, danh mục thiết bị tối thiểu bảo đảm an toàn, an ninh mạng theo quy định tại Văn bản số 708/BTTTT - CATT ngày 02/03/2024 của Bộ Thông tin và Truyền thông V/v sử đổi, thay thế nội dung về an toàn, an ninh mạng tại Công văn số 1552/BTTTT-THH.

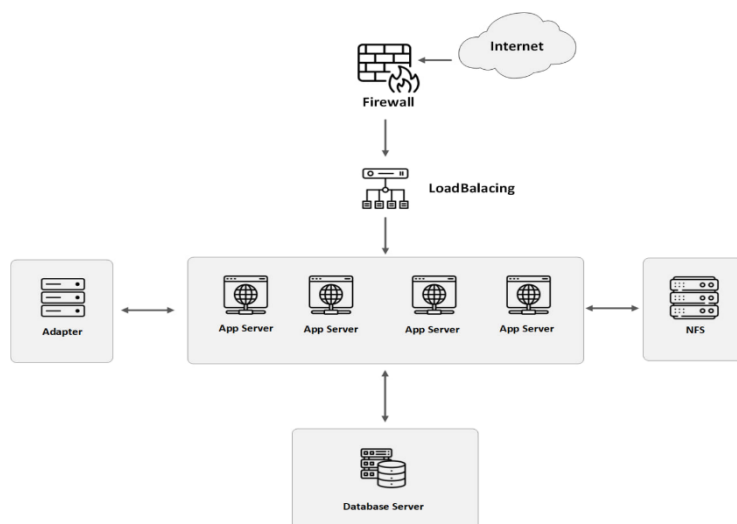
- Danh mục kết nối hiện có và cấu hình Máy chủ đang được sử dụng thực tế của hệ thống như sau:

- (1) Dịch vụ danh mục dùng chung
- (2) Dịch vụ liên thông văn bản
- (3) Dịch vụ liên thông hồ sơ hành chính công
- (4) Nhóm dịch vụ xác thực, cấp quyền người dùng tập trung (SSO)
- (5) Nhóm dịch vụ thanh toán điện tử
- (6) Tiếp nhận và trả kết quả giải quyết thủ tục hành chính qua dịch vụ bưu chính/bưu chính công ích
- (7) Dịch vụ liên thông với Cổng dịch vụ công quốc gia
- (8) Dịch vụ liên thông với hệ thống báo cáo Quốc gia GRIS
- (9) Dịch vụ liên thông Lý lịch tư pháp và Hộ Tịch tư pháp
- (10) Dịch vụ tra cứu Thông tin đăng kí doanh nghiệp
- (11) Dịch vụ tra cứu Thông tin bảo hiểm xã hội
- (12) Dịch vụ tra cứu Thông tin hộ tịch, lý lịch tư pháp

Danh sách máy chủ cài đặt hệ thống:

TT	Tên máy chủ	Cấu hình	Số lượng	Ghi chú
1	<b>Cụm Máy chủ ứng dụng (App)</b>	22 vCPU; 28 RAM; 200 GB HDD	6	
2	<b>Cụm Máy chủ CSDL (Database)</b>	16 vCPU; 32 RAM; 1000 GB HDD	2	
3	<b>Cụm lưu trữ - chia sẻ file (NFS)</b>	10000 GB HDD	1	Bổ sung 5000 TB
4	<b>Máy chủ chuyển đổi kết nối (Adapter)</b>	4 vCPU; 8 RAM; 70 GB HDD	1	

Mô hình máy chủ cài đặt hệ thống:



### 2.3 Yêu cầu về tính sẵn sàng, ổn định của hệ thống vận hành phần mềm

TT	Nội dung	Yêu cầu
1	Thời gian uptime	$\geq 99.95\%$ (trung bình theo tháng)
2	Tính ổn định	Hệ thống gây trung bình dưới 7 lỗi/tháng trong 3 tháng vận hành đầu tiên. Dưới 10 lỗi/năm trong 3 năm vận hành tiếp theo và dưới 3 lỗi/năm trong các năm vận hành tiếp theo (Lỗi gây dừng/tổn hại hệ thống) Thời gian trung bình giữa hai sự cố phải lớn hơn 4 giờ. Lỗi chấp nhận là lỗi trung bình không gây tổn hại trầm trọng hệ thống và có thể phục hồi trong thời gian dưới 5 phút nhưng không được quá 7 lỗi/tháng khi triển khai. Khi xảy ra các sự cố làm ngừng vận hành hệ thống, hệ thống phải đảm bảo phục hồi 70% trong vòng 1 giờ và 100% trong vòng 24 giờ.
3	Tính hỗ trợ	Hệ thống được hỗ trợ 24/24.
4	Tiếp nhận, phản hồi, xử lý sự cố	Thời gian tiếp nhận và phản hồi khi có sự cố dưới 1h giờ. Thời gian xử lý lỗi hệ thống dưới 24 giờ. Thời gian hướng dẫn xử lý các lỗi, sai sót dữ liệu dưới 48 giờ.

Các tiêu chuẩn kỹ thuật khác cần tuân thủ:

- Thông tư số 01/2023/VBHN - BTTTT ngày 13/02/2023 của Bộ Thông tin và Truyền thông quy định áp dụng tiêu chuẩn, quy chuẩn kỹ thuật đối với trung tâm dữ liệu;

- Nghị định số 278/2025/NĐ-CP ngày 20/10/2025 của Chính phủ Quy định về kết nối, chia sẻ dữ liệu bắt buộc giữa các cơ quan thuộc hệ thống chính trị;

- TCVN 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

- Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông hướng dẫn Nghị định số 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Công văn số 1145/BTTTT-CATTT ngày 03/4/2020 của Bộ Thông tin và Truyền thông về việc hướng dẫn bộ tiêu chí, chỉ tiêu kỹ thuật để đánh giá và lựa chọn giải pháp nền tảng điện toán đám mây phục vụ Chính phủ điện tử/chính quyền điện tử.

- Công văn số 2612/BTTTT-CATTT ngày 17/07/2021 của Bộ Thông tin và

Truyền thông về việc bổ sung bộ tiêu chí, chỉ tiêu kỹ thuật để đánh giá và lựa chọn giải pháp nền tảng điện toán đám mây phục vụ Chính phủ điện tử

### **3. Mô tả yêu cầu kỹ thuật cần đáp ứng của dịch vụ**

#### **3.1. Yêu cầu về quy trình nghiệp vụ cần được tin học hóa**

Đáp ứng theo Tài liệu kỹ thuật của 12 bộ dịch vụ tích hợp mới bao gồm: (1) Kết nối Cơ sở dữ liệu quốc gia về giá; (2) Kết nối dịch vụ Cơ sở dữ liệu đất đai; (3) Kết nối dịch vụ công chức viên chức; (4) Kết nối Cơ sở dữ liệu Đăng kiểm phương tiện; (5) Kết nối dịch vụ Cấp Mã số ngân sách; (6) Kết nối hệ thống thông tin Nguồn trung ương; (7) Kết nối Dịch vụ Tài nguyên môi trường; (8) Kết nối Dịch vụ công Bộ Xây dựng; (9) Kết nối Dịch vụ EVN; (10) Kết nối Dịch vụ Bộ Giao thông vận tải; (11) Kết nối Dịch vụ DMDC Ngân hàng nhà nước; (12) Kết nối Dịch vụ DMDC Bộ Tài chính.

#### **3.2. Các yêu cầu phi chức năng**

##### **3.2.1. Yêu cầu cần đáp ứng đối với cơ sở dữ liệu**

- Hệ thống sẽ thực thi các khái niệm về phiên của người sử dụng, đặc biệt là với đối tượng người dùng nghiệp vụ, trong đó các thông tin về hoạt động của người sử dụng từ lúc đăng nhập đến khi đăng xuất (tức là các phiên làm việc) được lưu lại trong cơ sở dữ liệu.

- Hệ quản trị CSDL cho phép giám sát hoạt động lâu dài, sử dụng giao diện công cụ GUI để dễ dàng thao tác.

- Hệ quản trị CSDL hỗ trợ khả năng advanced-queuing có sẵn.

- Hệ quản trị CSDL hỗ trợ cho mức độ truy vấn song song tự động.

- Hệ quản trị CSDL hỗ trợ việc sao chép và chia sẻ tải với một hệ thống khôi phục dự phòng.

- Hệ quản trị CSDL sẽ cung cấp các công cụ tự động mở rộng để lưu trữ dữ liệu định kỳ.

- Hệ quản trị CSDL sẽ cung cấp các công cụ tự động để định kỳ “làm sạch” dữ liệu nhằm đảm bảo sự nhất quán và toàn vẹn dữ liệu. Các công cụ phải lưu trữ các dữ liệu quá khứ để rollback nếu cần.

- Cơ sở dữ liệu phải có khả năng lưu trữ với dung lượng lớn, trong thời gian lâu dài.

- Có khả năng lưu trữ được nhiều định dạng dữ liệu khác nhau như dữ liệu có cấu trúc, bán cấu trúc, phi cấu trúc dưới dạng tệp gắn kèm (dữ liệu tệp văn bản, dữ liệu phim, ảnh, âm thanh).

##### **3.2.2. Yêu cầu về an toàn thông tin**

- Xác thực:

Phần mềm sử dụng phương pháp xác thực là username/password.

Kiểm soát truy cập: Hệ thống cấp tài khoản và được phân quyền tương ứng với chức năng nhiệm vụ của tài khoản đảm bảo cấp tài khoản nào chỉ được xem các nội dung tương ứng với đặc quyền.

Nhật ký hệ thống: Hệ thống ứng dụng được giám sát và ghi nhật ký (log hệ thống) 24/7. Dữ liệu log được lưu trữ biệt lập và được bảo vệ bởi các giải pháp an toàn thông tin.

- Bảo mật thông tin liên lạc

Các thông tin liên lạc của người dùng được bảo vệ trước các truy cập trái phép thông qua biện pháp phân quyền và mã hóa.

- Chống chối bỏ

Mỗi người sử dụng được gắn với một tài khoản đặc quyền duy nhất, việc truy cập, chỉnh sửa dữ liệu ứng dụng được ghi log.

- Đảm bảo an toàn cơ bản đối với phần mềm nội bộ theo quy định tại Quyết định số 742/QĐ-BTTTT ngày 22/4/2022 của Bộ Thông tin và Truyền thông, cụ thể phải đáp ứng yêu cầu đối với hệ thống có cấp độ 3 như sau:

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

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu
		<p>d) Có chức năng cho phép thiết lập thời gian mật khẩu hợp lệ.</p> <p>đ) Khóa tài khoản và yêu cầu nhập mật khẩu mới khi mật khẩu của tài khoản đó hết hạn thời gian hợp lệ.</p> <p>e) Mở khóa tài khoản khi thay đổi mật khẩu thành công đối với trường hợp mật khẩu hết hạn thời gian hợp lệ.</p>
1.4	Có chức năng cho phép hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định.	<p>a) Có giao diện cho phép thiết lập chính sách về giới hạn số lần đăng nhập sai trong khoảng thời gian nhất định.</p> <p>b) Có chức năng cảnh báo tới người sử dụng khi vi phạm chính sách.</p> <p>c) Có chức năng tự động ngăn cản việc đăng nhập tự động khi vi phạm chính sách trên.</p> <p>đ) Có chức năng tự động vô hiệu hóa tài khoản nếu vi phạm chính sách trên.</p>
1.5	Có chức năng cho phép mã hóa thông tin xác thực trước khi gửi qua môi trường mạng	Chức năng bảo đảm mật khẩu được mã hóa trước khi gửi qua môi trường mạng.
<b>2.</b>	<b>Kiểm soát truy cập</b>	
2.1	Có chức năng cho phép thiết lập giới hạn thời gian chờ (timeout).	<p>a) Có chức năng cho phép thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi Phần mềm không nhận được yêu cầu từ người dùng.</p> <p>b) Hiển thị thông báo, đóng phiên kết nối đã hết hạn thời gian timeout và yêu cầu đăng nhập lại.</p>
2.2	Có chức năng cho phép giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị Phần mềm từ xa.	a) Có giao diện cho phép quản trị viên quản lý chính sách về giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị Phần mềm từ xa.

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu
		b) Có chức năng thực thi chính sách về giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị Phần mềm từ xa ở trên.
2.3	Có chức năng cho phép phân quyền và cấp quyền tối thiểu truy cập, quản trị, sử dụng tài nguyên khác nhau của Phần mềm với người sử dụng/ nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau.	<p>a) Có giao diện cho phép quản trị viên quản lý chính sách về phân quyền tài khoản theo từng nhóm tài khoản.</p> <p>b) Phân loại nhóm tài khoản theo ít nhất 03 nhóm:</p> <ul style="list-style-type: none"> <li>i. Tài khoản người sử dụng thông thường;</li> <li>ii. Tài khoản quản trị mức sử dụng;</li> <li>iii. Tài khoản quản trị mức phát triển, vận hành.</li> </ul> <p>c) Có chức năng thực thi chính sách phân quyền và cấp quyền tối thiểu truy cập, quản trị, sử dụng tài nguyên khác nhau ở trên</p>
2.4	Có chức năng cho phép thiết lập quyền tối thiểu (quyền truy cập, quản trị) cho tài khoản quản trị ứng dụng theo quyền hạn	<p>a) Có giao diện cho phép quản trị viên thiết lập quyền cho các tài khoản.</p> <p>b) Có chức năng thực thi chính sách phân quyền cho các tài khoản ở trên.</p>
<b>3.</b>	<b>Nhật ký hệ thống</b>	
3.1	Có chức năng cho phép ghi nhật ký hệ thống gồm những thông tin.	<p>a) Phần mềm cung cấp chức năng ghi nhật ký hệ thống.</p> <p>b) Nhật ký hệ thống được phân loại theo ít nhất 05 nhóm:</p> <ul style="list-style-type: none"> <li>i. Nhật ký truy cập Phần mềm;</li> <li>ii. Nhật ký đăng nhập khi quản trị Phần mềm;</li> <li>iii. Nhật ký các lỗi phát sinh trong quá trình hoạt động;</li> <li>iv. Nhật ký quản lý tài khoản;</li> <li>v. Nhật ký thay đổi cấu hình Phần mềm</li> </ul>

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu
3.2	Có chức năng cho phép quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung.	<p>a) Có giao diện cho phép quản trị viên quản lý chính sách về nhật ký hệ thống.</p> <p>b) Cho phép quản trị viên cấu hình khoảng thời gian lưu trữ nhật ký qua giao diện trên.</p> <p>c) Lưu trữ nhật ký với ít nhất 05 thông tin:</p> <ul style="list-style-type: none"> <li>i. Thời điểm sinh nhật ký;</li> <li>ii. Phân nhóm nhật ký;</li> <li>iii. Mô tả thao tác/lỗi;</li> <li>iv. Đối tượng thực hiện thao tác/sinh lỗi;</li> <li>v. Mức độ quan trọng.</li> </ul>
4.	<b>An toàn ứng dụng và mã nguồn</b>	
4.1	Có chức năng cho phép kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý.	Có chức năng thực thi việc kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý
4.2	Có chức năng cho phép bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSR	Phần mềm được kiểm tra, đánh giá, kiểm thử xâm nhập theo tiêu chuẩn OWASP và không tồn tại điểm yếu cho phép kẻ tấn công khai thác thông qua các dạng tấn công: SQL Injection, OS command injection, RFI, LFI, Xpath Injection, XSS, CSRF.
4.3	Có chức năng cho phép kiểm soát lỗi, thông báo lỗi từ ứng dụng.	<p>a) Có chức năng kiểm soát lỗi, chỉ hiển thị các thông báo lỗi được kiểm soát đến người dùng và không hiển thị các lỗi bên trong hệ thống</p> <p>b) Có chức năng hiển thị thông báo lỗi đến người sử dụng.</p>
4.4	Có chức năng cho phép bảo đảm không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng.	a) Thông tin xác thực, bí mật không được đưa trực tiếp vào mã nguồn ứng dụng mà phải được thiết lập thông qua giao diện cấu hình hệ thống.
5	<b>Bảo mật thông tin liên lạc</b>	

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu
5.1	Có chức năng cho phép mã hóa thông tin, dữ liệu trước khi truyền đưa, trao đổi qua môi trường mạng (đối với các ứng dụng yêu cầu sử dụng chữ ký số).	Có chức năng cho phép mã hóa dữ liệu trước khi truyền đưa, trao đổi qua môi trường mạng sử dụng chữ ký số.
<b>6</b>	<b>Sao lưu dự phòng</b>	
6.1	Có chức năng cho phép tự động sao lưu dự phòng	a) Có giao diện cho phép quản trị viên thiết lập chính sách về sao lưu dự phòng cơ sở dữ liệu và cấu hình hệ thống
		b) Có chức năng cho phép thực hiện việc sao lưu dự phòng theo chính sách ở trên.

### 3.2.3. Các yêu cầu cần đáp ứng về thời gian xử lý, độ phức tạp xử lý của các phần mềm

-Hạ tầng phần cứng của hệ thống phải đáp ứng yêu cầu về các chức năng, số lượng người dùng tham gia khai thác, sử dụng hệ thống; khả năng tích hợp dữ liệu với các bộ, ngành, địa phương như đã nêu trên và các yêu cầu sau đây:

+ Về thời gian: Thời gian cho phép để hệ thống phản hồi lại các thao tác, hành động của người dùng trên Nền tảng chia sẻ, tích hợp dùng chung (LGSP) tỉnh Hà Giang tối đa là 5 giây (s), đối với các yêu cầu phức tạp (báo cáo, thông kê, ...) thì cho phép tối đa 30 giây (s);

+ Về tài nguyên sử dụng: Tài nguyên lưu trữ chiếm dụng của hệ thống trong trạng thái hoạt động bình thường không được phép lớn hơn 80% tài nguyên lưu trữ được phép sử dụng hoặc 20% tài nguyên lưu trữ dùng chung tại mọi thời điểm; tài nguyên vi xử lý mà các phần mềm ứng dụng thuộc hệ thống chiếm dụng của các máy chủ không được phép lớn hơn 40% tài nguyên vi xử lý dùng chung tại mọi thời điểm; bộ nhớ truy cập ngẫu nhiên mà các phần mềm ứng dụng thuộc hệ thống chiếm dụng của các máy chủ không được phép lớn hơn 50% bộ nhớ truy cập ngẫu nhiên của máy chủ.

+ Hiệu năng không bị ảnh hưởng từ các yếu tố như: thời gian, sự tăng trưởng về dữ liệu chính, bảo đảm có khả năng hoạt động không bị ảnh hưởng về dữ liệu trong tối thiểu 3 năm.

Các yêu cầu về ràng buộc xử lý logic đối với việc nhập (hay chuyển đổi) dữ liệu thông qua sử dụng các ô nhập liệu do giao diện chương trình cung cấp

Thực hiện kiểm tra các trường, kiểu dữ liệu đúng thì mới cho phép người dùng thực hiện thao tác lưu trữ dữ liệu.

Cần hiển thị thông báo cho người dùng khi người dùng thực hiện sai thao tác.

### **3.2.4. Các yêu cầu về cài đặt, hạ tầng, đường truyền, an toàn vận hành, khai thác, sử dụng**

#### **a) Yêu cầu chung**

- Hệ thống phải được cài đặt tại Trung tâm Dữ liệu đáp ứng tiêu chuẩn tối thiểu đạt Tier 3; có hệ thống dự phòng thảm họa (DR site) và dự phòng tối thiểu 1:1 với đường truyền, hệ thống, dữ liệu.

- Hệ thống cần được triển khai và vận hành trên hệ thống hạ tầng đảm bảo bảo mật mức cao có những quy định về quản lý an toàn, bảo mật hệ thống mạng và quản lý các thiết bị đầu cuối của toàn bộ hệ thống mạng. Hệ thống cần chia tách các vùng mạng khác nhau: phân vùng mạng riêng cho máy chủ của Hệ thống; phân vùng mạng trung gian (DMZ) để cung cấp dịch vụ trên mạng Internet.

- Có phương án dự phòng cho các thiết bị mạng chính, bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm

- Các máy chủ CSDL luôn đồng bộ dữ liệu với nhau và chạy ở chế độ sẵn sàng cao đảm bảo tính sẵn sàng và toàn vẹn về mặt dữ liệu của hệ thống, đảm bảo hệ thống vẫn hoạt động khi có một máy chủ CSDL gặp sự cố.

#### **b) Yêu cầu đối với Hạ tầng máy chủ điện toán đám mây**

Sử dụng thuê dịch vụ máy chủ điện toán đám mây (máy chủ cloud) của các đơn vị cung cấp dịch vụ, đáp ứng yêu cầu về kỹ thuật đối với nền tảng điện toán đám mây phục vụ Chính phủ điện tử quy định tại Công văn số 1145/BTTTT-CATTT ngày 03/4/2020 và Công văn số 2612/BTTTT-CATTT ngày 17/07/2021 của Bộ Thông tin và Truyền thông.

### **3.2.5. Các ràng buộc đối với hệ thống gồm: ràng buộc môi trường, sự phụ thuộc vào hệ thống nền tảng**

- Hệ thống phần mềm có thể dễ dàng cài đặt và vận hành trên các nền tảng hệ điều hành phổ biến như Windows server, Centos, Unix, Ubuntu. Cho phép triển khai được trên nền tảng ảo hóa.

- Phía người sử dụng cuối sẽ thực hiện truy cập dịch vụ và thực hiện các yêu cầu định danh và xác thực điện tử qua môi trường internet bằng các trình duyệt phổ biến như Firefox, Chrome... được cài đặt trên các máy tính cá nhân (PC, Laptop..) trong các hệ điều hành Windows, MacOS,...

#### **3.2.6. Yêu cầu về tính sẵn sàng với IPv6**

- Hệ thống được triển khai xây dựng phù hợp để sẵn sàng hoạt động tốt trên môi trường mạng IPv6.

- Đường truyền kết nối Internet cho Webserver sẵn sàng hỗ trợ IPv6

- Webserver sẵn sàng lắng nghe được các kết nối qua mạng IPv6

- Hệ thống sẵn sàng khai báo bản ghi AAAA cho tên miền trên hệ thống DNS Hosting.

- Sẵn sàng hỗ trợ địa chỉ Internet thế hệ mới IPv6, DNSSEC. Triển khai HTTPS sử dụng giao thức TLS v1.2 trở lên với các bộ mã hóa an toàn trong xác thực người dùng và truyền nhận các thông tin nhạy cảm (thông tin cá nhân, thông tin thanh toán).

### **3.2.7. Yêu cầu về mỹ thuật, kỹ thuật cần đạt được của các giao diện chương trình**

- Hệ thống cho phép lưu trữ tất cả dữ liệu theo định dạng Unicode, chấp nhận tất cả các ký tự tiếng việt có dấu.

- Giao diện màn hình, các thông báo lỗi và trợ giúp là ngôn ngữ tiếng việt theo chuẩn TCVN 6909:2001 dựa trên bảng mã Unicode (ISO 10646), với trợ giúp các bộ gõ Unikey, Vietkey.

- Các biểu tượng, hình ảnh được thống nhất trong toàn bộ chương trình.

- Các màn hình cập nhật dữ liệu về cơ bản thống nhất về các nút lệnh cũng như về màu sắc, phông chữ.

- Hiển thị ngày, giờ theo dạng DD/MM/YYYY và hh:mm:ss.

- Các trường thông tin dạng text thì căn lề trái.

- Hệ thống cung cấp giao diện trực quan, thân thiện với người sử dụng và phù hợp đối với các nhóm người sử dụng khác nhau.

- Các giao diện thiết kế một cách đơn giản nhưng hiệu quả cao về thao tác, giảm thiểu việc mở quá nhiều cửa sổ, hiển thị và xử lý hình ảnh nhanh, màu sắc không gây cảm giác nhàm chán cho người sử dụng và theo một chuẩn giao diện thống nhất.

- Tất cả các ngày tháng sẽ được lưu với 4 chữ số cho phần Năm.

- Các thành phần trong giao diện màn hình nhập liệu được focus tuần tự liên tiếp nhau khi thực hiện phím Enter.

- Trong các màn hình nhập số liệu, các trường bắt buộc phải nhập được đánh dấu (\*) bên cạnh để phân biệt.

- Trong mỗi màn hình cập nhật thông tin, các trường được phép cập nhật có màu khác để phân biệt.

## **4. Yêu cầu về an toàn thông tin, dữ liệu và các yêu cầu khác.**

### **4.1. Xác định cấp độ hệ thống thông tin**

Căn cứ khoản 2, Điều 9 Nghị định số 85/2016/NĐ-CP của Thủ tướng Chính phủ ngày 01/07/2016 về đảm bảo an toàn hệ thống thông tin theo cấp độ. Hệ thống thông tin cấp độ 3 là hệ thống thông tin có một trong các tiêu chí cụ thể sau:

*“2. Hệ thống thông tin phục vụ người dân, doanh nghiệp thuộc một trong các loại hình sau:*

a) Cung cấp thông tin và dịch vụ công trực tuyến từ mức độ 3 trở lên theo quy định của pháp luật.

b) Cung cấp dịch vụ công trực tuyến thuộc danh mục kinh doanh có điều kiện;

c) Cung cấp dịch vụ công trực tuyến khác có xử lý thông tin riêng, thông tin cá nhân từ 10.000 người sử dụng trở lên.”

“Nền tảng tích hợp và chia sẻ dữ liệu (LGSP) tỉnh Tuyên Quang” có các tiêu chí phù hợp với các nội dung tại khoản 2, Điều 9, Nghị định số 85/2016/NĐ-CP nêu trên. Vậy “Nền tảng tích hợp và chia sẻ dữ liệu (LGSP) tỉnh Tuyên Quang **được xác định là an toàn Hệ thống thông tin cấp độ 3**. Hệ thống thông tin phải đáp ứng các yêu cầu an toàn cấp độ 3 theo quy định tại Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ. Hệ thống phải triển khai phương án giám sát theo quy định của pháp luật trước khi đưa vào khai thác, sử dụng; Thực hiện công tác kiểm tra, đánh giá an toàn thông tin trước khi đưa hệ thống vào vận hành, khai thác sử dụng và định kỳ kiểm tra, đánh giá hoặc đột xuất khi có yêu cầu theo quy định của pháp luật.

## 4.2. Phương án đảm bảo an toàn thông tin theo cấp độ

Phương án kỹ thuật Hệ thống phải đáp ứng phương án đảm bảo an toàn thông tin theo cấp độ, được nêu tại Phụ lục 3 Thông tư số: 12/2022/TT-BTTTT ngày 12 tháng 08 năm 2022 của Bộ Thông tin và truyền thông về việc Quy định chi tiết và hướng dẫn một số điều của nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ 3, cụ thể như sau:

### 4.2.1. Yêu cầu thiết kế hệ thống

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

- i. Vùng mạng nội bộ;
- ii. Vùng mạng biên;
- iii. Vùng DMZ;
- iv. Vùng máy chủ nội bộ;
- v. Vùng mạng máy chủ cơ sở dữ liệu;
- vi. Vùng quản trị.

b) **Có phương án thiết kế bảo đảm các yêu cầu sau:**

i. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương; sử dụng sản phẩm Mạng riêng ảo đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định số 85/2016/NĐ-CP;

ii. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập sử dụng sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc sản phẩm Phòng, chống xâm nhập lớp mạng;

iii. Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng chính, tối thiểu bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm, tường lửa ứng dụng web, hệ thống lưu trữ tập trung, tường lửa cơ sở dữ liệu (nếu có);

iv. Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu; sử dụng sản phẩm Tường lửa cơ sở dữ liệu đối với hệ thống cơ sở dữ liệu tập trung, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định số 85/2016/NĐ-CP;

v. Có phương án chặn lọc phần mềm độc hại trên môi trường mạng sử dụng Tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc phương án tương đương;

vi. Có phương án phòng chống tấn công từ chối dịch vụ; sử dụng dịch vụ của doanh nghiệp hoặc sản phẩm Phòng, chống tấn công từ chối dịch vụ đối với các hệ thống Trung tâm dữ liệu, điện toán đám mây, hệ thống Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số và hệ thống Kết nối tích hợp, chia sẻ dữ liệu, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định số 85/2016/NĐ-CP;

vii. Có phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng sản phẩm Tường lửa ứng dụng web đối với các hệ thống thông tin được quy định tại khoản 2, Điều 9 Nghị định số 85/2016/NĐ-CP;

viii. Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử; sử dụng sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với hệ thống Thư điện tử, đáp ứng tiêu chí quy định tại khoản 2 Điều 9 Nghị định số 85/2016/NĐ-CP;

ix. Có phương án quản lý truy cập lớp mạng; sử dụng sản phẩm Quản lý truy cập lớp mạng đối với hệ thống Mạng nội bộ, Trung tâm giám sát điều hành an toàn thông tin mạng, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định số 85/2016/NĐ-CP;

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

xi. Có phương án giám sát an toàn hệ thống thông tin tập trung sử dụng sản phẩm Quản lý và phân tích sự kiện an toàn thông tin hoặc sản phẩm tương đương;

xii. Có phương án quản lý sao lưu dự phòng tập trung sử dụng hệ thống lưu trữ tập trung và sản phẩm quản lý lưu trữ tập trung;

xiii. Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng, sử dụng sản phẩm Phòng, chống mã độc và/hoặc sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối, có chức năng quản lý tập trung;

xiv. Có phương án phòng, chống thất thoát dữ liệu; sử dụng sản phẩm Phòng, chống thất thoát dữ liệu đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định số 85/2016/NĐ-CP;

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

#### 4.2.2. Yêu cầu về thiết lập, cấu hình hệ thống

STT	Yêu cầu	TCVN 11930:2017
<b>1.1</b>	<b>Bảo đảm an toàn mạng</b>	<b>Mục 7.2.1</b>
1.1.1	Kiểm soát truy cập từ bên ngoài mạng	Mục 7.2.1.2
1.1.2	Kiểm soát truy cập từ bên trong mạng	Mục 7.2.1.3
1.1.3	Nhật kí hệ thống	Mục 7.2.1.4
1.1.4	Phòng chống xâm nhập	Mục 7.2.1.5
1.1.5	Phòng chống phần mềm độc hại trên môi trường mạng	Mục 7.2.1.6
1.1.6	Bảo vệ thiết bị hệ thống	Mục 7.2.1.7
<b>1.2</b>	<b>Bảo đảm an toàn máy chủ</b>	<b>Mục 7.2.2</b>
1.2.1	Xác thực	Mục 7.2.2.1
1.2.2	Kiểm soát truy cập	Mục 7.2.2.2
1.2.3	Nhật ký hệ thống	Mục 7.2.2.3
1.2.4	Phòng chống xâm nhập	Mục 7.2.2.4
1.2.5	Phòng chống phần mềm độc hại	Mục 7.2.2.5
1.2.6	Xử lý máy chủ khi chuyển giao	Mục 7.2.2.6
<b>1.3</b>	<b>Bảo đảm an toàn ứng dụng</b>	<b>Mục 7.2.3</b>
1.3.1	Xác thực	Mục 7.2.3.1
1.3.2	Kiểm soát truy cập	Mục 7.2.3.2
1.3.3	Nhật kí hệ thống	Mục 7.2.3.3
1.3.4	Bảo mật thông tin liên lạc	Mục 7.2.3.4
1.3.5	Chống chối bỏ	Mục 7.2.3.5

1.3.6	An toàn ứng dụng và mã nguồn	Mục 7.2.3.6
<b>1.4</b>	<b>Bảo đảm an toàn dữ liệu</b>	<b>Mục 7.2.4</b>
1.4.1	Nguyên vẹn dữ liệu	Mục 7.2.4.1
1.4.2	Bảo mật dữ liệu	Mục 7.2.4.2
1.4.3	Sao lưu dự phòng	Mục 7.2.4.3

#### 4.3. Yêu cầu phương án, thiết bị bảo đảm an toàn, an ninh mạng

- Có phương án, thiết bị thiết bị tối thiểu phục vụ bảo đảm an toàn, an ninh mạng theo hướng dẫn tại Công văn số 708/BTTTT-CATTTT ngày 02/03/2024 của Bộ Thông tin và Truyền thông sửa đổi, thay thế nội dung về an toàn, an ninh mạng tại Công văn số 1552/BTTTT-THH.

STT	Yêu cầu	Phương án đáp ứng
<b>Cấp độ 3</b>		
1	Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương; sử dụng Sản phẩm Mạng riêng ảo đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP	1. Đối với hệ thống thông tin cấp độ 3 có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP yêu cầu Hệ thống sử dụng Sản phẩm VPN. 2. Sản phẩm VPN phải đáp ứng tối thiểu các yêu cầu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSDXCD. - Minh chứng Sản phẩm/chức năng VPN tích hợp trên Thiết bị Tường lửa được cấu hình trên Hệ thống thực.
2	Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập sử dụng Sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc Sản phẩm Phòng, chống xâm nhập lớp mạng	1. Đối với hệ thống thông tin cấp độ 3 có thể sử dụng Tường lửa tích hợp chức năng phòng, chống xâm nhập hoặc sử dụng Sản phẩm phòng, chống xâm nhập chuyên dụng. 2. Sản phẩm/Tường lửa tích hợp chức năng phòng, chống xâm nhập phải đáp ứng tối thiểu các yêu cầu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm/Tường lửa tích hợp chức năng phòng, chống xâm nhập đáp ứng

		<p>đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSDXCĐ.</p> <p>- Minh chứng Sản phẩm/Tường lửa tích hợp chức năng phòng, chống xâm nhập được cấu hình để giám sát, bảo vệ đầy đủ các vùng mạng trong hệ thống được thuyết minh trong HSDXCĐ.</p>
3	<p>Có phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng Sản phẩm Tường lửa ứng dụng web đối với các hệ thống thông tin được quy định tại khoản 2, Điều 9 Nghị định 85/2016/NĐ-CP</p>	<p>1. Đối với các hệ thống thông tin cấp độ 3 được quy định tại khoản 2, Điều 9 Nghị định 85/2016/NĐ-CP Yêu cầu sử dụng Sản phẩm Tường lửa ứng dụng web. Sản phẩm Tường lửa ứng dụng web phải đáp ứng tối thiểu các yêu cầu sau:</p> <p>- Thiết lập cấu hình bảo mật cho Sản phẩm Tường lửa ứng dụng web đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSDXCĐ.</p> <p>- Tường lửa ứng dụng web được cấu hình để bảo vệ đầy đủ các ứng dụng được thuyết minh trong HSDXCĐ.</p>
4	<p>Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng chính, tối thiểu bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm, tường lửa ứng dụng web, hệ thống lưu trữ tập trung, tường lửa cơ sở dữ liệu (nếu có)</p>	<p>1. Đối với hệ thống thông tin cấp độ 3 yêu cầu các thiết bị mạng chính trong hệ thống đều có thiết bị dự phòng nóng và cấu hình để thực hiện chức năng cân bằng tải, tối thiểu bao gồm: Thiết bị chuyển mạch trung tâm hoặc tương đương; Thiết bị tường lửa trung tâm; Tường lửa ứng dụng web; Hệ thống lưu trữ tập trung; Tường lửa cơ sở dữ liệu (nếu có).</p> <p>(Đối với Hệ thống lưu trữ tập trung yêu cầu thiết bị chuyển mạch được trang bị theo cặp. Thiết bị lưu trữ phải được phân tách 02 vùng logic độc lập)</p> <p>2. Có sơ đồ thiết kế vật lý để minh chứng các thiết bị có thiết bị dự phòng.</p> <p>3. Có cấu hình của các thiết bị mạng chính để chứng minh chức năng cân bằng tải và dự phòng nóng.</p>
5	<p>Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu; sử dụng Sản phẩm Tường lửa cơ sở dữ liệu đối với hệ thống cơ sở dữ liệu tập trung, đáp ứng tiêu chí quy</p>	<p>1. Đối với hệ thống thông tin cấp độ 3 là hệ thống cơ sở dữ liệu tập trung, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP.</p> <p>Yêu cầu sử dụng Sản phẩm Tường lửa cơ sở dữ liệu hoặc Sản phẩm bảo vệ cơ sở dữ liệu. Sản phẩm Tường lửa cơ sở dữ liệu hoặc Sản phẩm bảo vệ cơ sở dữ liệu phải đáp ứng tối thiểu các yêu cầu sau:</p>

	định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP	- Thiết lập cấu hình bảo mật cho Sản phẩm Tường lửa cơ sở dữ liệu đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSDXCĐ.  - Tường lửa cơ sở dữ liệu được cấu hình để bảo vệ đầy đủ các cơ sở dữ liệu được thuyết minh trong HSDXCĐ.
6	Có phương án chặn lọc phần mềm độc hại trên môi trường mạng sử dụng Tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc phương án tương đương	1. Đối với hệ thống thông tin cấp độ 3 sử dụng Sản phẩm Tường lửa lớp mạng có tích hợp chức năng phòng, chống mã độc trên môi trường mạng.  Tường lửa lớp mạng có tích hợp chức năng phòng, chống mã độc trên môi trường mạng phải đáp ứng tối thiểu các yêu cầu sau:  Minh chứng chức năng phòng, chống mã độc trên môi trường mạng được cấu hình để giám sát, bảo vệ đầy đủ các vùng mạng trong hệ thống được thuyết minh trong HSDXCĐ.
7	Có phương án phòng chống tấn công từ chối dịch vụ; sử dụng dịch vụ của doanh nghiệp hoặc Sản phẩm Phòng, chống tấn công từ chối dịch vụ đối với các hệ thống Trung tâm dữ liệu, điện toán đám mây, hệ thống Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số và hệ thống Kết nối tích hợp, chia sẻ dữ liệu, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP	1. Đối với các hệ thống thông tin cấp độ 3 là hệ thống Trung tâm dữ liệu, điện toán đám mây, hệ thống Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số và hệ thống Kết nối tích hợp, chia sẻ dữ liệu, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP  Yêu cầu sử dụng dịch vụ của doanh nghiệp hoặc Sản phẩm Phòng, chống tấn công từ chối dịch vụ. Dịch vụ của doanh nghiệp hoặc Sản phẩm Phòng, chống tấn công từ chối dịch vụ phải đáp ứng một trong hai yêu cầu sau:  - Trường hợp sử dụng dịch vụ, yêu cầu có hợp đồng cung cấp dịch vụ.  - Trường hợp sử dụng Sản phẩm Phòng, chống tấn công từ chối dịch vụ, yêu cầu minh chứng chức năng Phòng, chống tấn công từ chối dịch vụ được cấu hình để bảo vệ hệ thống.
8	Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử; sử dụng Sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với	Hệ thống không cung cấp dịch vụ thư điện tử, không kết nối trực tiếp với hệ thống thư điện tử.

	<p>hệ thống Thư điện tử, đáp ứng tiêu chí quy định tại khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP</p> <p>(Chỉ áp dụng đối với hệ thống thư điện tử trực tiếp kết nối)</p>	
9	<p>Có phương án quản lý truy cập lớp mạng; sử dụng Sản phẩm Quản lý truy cập lớp mạng đối với hệ thống Mạng nội bộ, Trung tâm giám sát điều hành an toàn thông tin mạng, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP</p>	<p>1. Đối với hệ thống thông tin cấp độ 3 là hệ thống Mạng nội bộ, Trung tâm giám sát điều hành an toàn thông tin mạng, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP.</p> <p>Yêu cầu sử dụng Sản phẩm Quản lý truy cập lớp mạng. Sản phẩm Quản lý truy cập lớp mạng phải đáp ứng tối thiểu yêu cầu sau: Thiết lập cấu hình bảo mật cho Sản phẩm Quản lý truy cập lớp mạng đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSDXCĐ.</p>
10	<p>Có phương án giám sát hệ thống thông tin tập trung</p>	<p>1. Đối với các hệ thống thông tin cấp độ 3, yêu cầu phương án sử dụng giám sát được trạng thái hoạt động của toàn bộ thiết bị, máy chủ và ứng dụng được thuyết minh trong HSDXCĐ.</p> <p>2. Trạng thái giám sát tối thiểu bao gồm các thông tin hiệu năng của CPU, RAM, Storage và các giao diện mạng.</p>
11	<p>Có phương án giám sát an toàn hệ thống thông tin tập trung sử dụng Sản phẩm Quản lý và phân tích sự kiện an toàn thông tin hoặc Sản phẩm tương đương</p>	<p>1. Đối với các hệ thống thông tin cấp độ 3 sử dụng Sản phẩm Quản lý và phân tích sự kiện an toàn thông tin.</p> <p>Yêu cầu đối với Sản phẩm Quản lý và phân tích sự kiện an toàn thông tin đáp ứng các yêu cầu tối thiểu sau:</p> <ul style="list-style-type: none"> <li>- Thiết lập cấu hình bảo mật cho Sản phẩm Quản lý và phân tích sự kiện an toàn thông tin đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSDXCĐ.</li> <li>- Quản lý và phân tích sự kiện an toàn thông tin của toàn bộ thiết bị, máy chủ và ứng dụng được thuyết minh trong HSDXCĐ.</li> </ul>

		<p>2. Đối với các hệ thống thông tin cấp độ 3 sử dụng Sản phẩm tương đương đáp ứng tối thiểu các yêu cầu sau:</p> <ul style="list-style-type: none"> <li>- Có chức năng quản trị: Chức năng phân tích tương quan (Correlation); Chức năng lọc (Filters), Tạo các luật (Rules), Chức năng hiển thị (Dashboards), Chức năng cảnh báo và báo cáo (Alerts and Reports), Chức năng cảnh báo thời gian thực (Real Time Alert).</li> <li>- Có chức năng nhận log: Cho phép nhận log từ các nguồn với nhiều định dạng khác nhau từ các thiết bị mạng, máy chủ và ứng dụng; định dạng, chuẩn hóa log nhận được theo các trường thông tin tùy biến theo nhu cầu sử dụng.</li> </ul>
12	<p>Có phương án quản lý sao lưu dự phòng tập trung sử dụng hệ thống lưu trữ tập trung và Sản phẩm quản lý lưu trữ tập trung</p>	<p>Đối với các hệ thống thông tin cấp độ 3, yêu cầu hệ thống có hệ thống lưu trữ và Sản phẩm để phục vụ việc quản lý lưu trữ tập trung.</p> <p>Yêu cầu đối với Sản phẩm quản lý lưu trữ tập trung đáp ứng các yêu cầu tối thiểu sau:</p> <ul style="list-style-type: none"> <li>- Tối thiểu các dữ liệu sau yêu cầu được lưu trữ trên hệ thống quản lý tập trung: Ảnh hệ điều hành của các máy chủ trong hệ thống, tệp tin cấu hình các thiết bị hệ thống, cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có).</li> <li>- Dữ liệu phải được sao lưu, dự phòng tối thiểu trên 02 thiết bị vật lý lưu trữ khác nhau.</li> </ul>
13	<p>Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng, sử dụng Sản phẩm Phòng, chống mã độc và/hoặc Sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối, có chức năng quản lý tập trung</p>	<p>1. Đối với các hệ thống thông tin cấp độ 3, yêu cầu hệ thống sử dụng Sản phẩm Phòng, chống mã độc và/hoặc Sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối.</p> <p>Yêu cầu đối với Sản phẩm Phòng, chống mã độc và/hoặc Sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối phải đáp ứng tối thiểu các yêu cầu sau:</p> <ul style="list-style-type: none"> <li>- Có chức năng quản lý tập trung.</li> <li>- Minh chứng toàn bộ các máy chủ, máy trạm trong hệ thống được cài đặt Sản phẩm và được quản lý trên hệ thống quản lý tập trung.</li> </ul>

14	Có phương án phòng, chống thất thoát dữ liệu; sử dụng Sản phẩm Phòng, chống thất thoát dữ liệu đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP	1. Đối với hệ thống thông tin cấp độ 3 có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP. Yêu cầu sử dụng Sản phẩm Phòng, chống thất thoát dữ liệu. Bảo đảm tối thiểu các máy chủ cơ sở dữ liệu, máy tính quản trị cơ sở dữ liệu, máy tính phục vụ hoạt động nghiệp vụ xử lý dữ liệu được triển khai các giải pháp phòng, chống thất thoát dữ liệu.
15	Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ	Yêu cầu có kết nối dự phòng, Hệ thống duy trì tối thiểu 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau.
16	Có phương án bảo đảm an toàn cho mạng không dây  (Yêu cầu này chỉ áp dụng trong trường hợp hệ thống Mạng không dây kết nối trực tiếp với hệ thống Cơ sở dữ liệu quốc gia về dân cư, hệ thống định danh và xác thực điện tử)	Hệ thống không sử dụng kết nối mạng không dây

## 5. Yêu cầu về đào tạo, tập huấn

### 5.1. Nội dung đào tạo, tập huấn

- Đào tạo hướng dẫn sử dụng phần mềm.

### 5.2. Số lượng, thời gian, đối tượng đào tạo

Tổ chức tối thiểu 02 lớp tập huấn triển khai sử dụng phần mềm, bao gồm:

+ Lớp quản trị và tích hợp hệ thống: 05 cán bộ

+ Lớp quản lý, khai thác: 05 cán bộ

### 5.3. Yêu cầu về tổ chức đào tạo

a) Yêu cầu về môi trường lớp đào tạo

- Phòng đào tạo phải đảm bảo các điều kiện sau có điều hoà nhiệt độ, hệ thống điện chiếu sáng, máy chiếu, bàn, đường mạng, ghế, diện tích phòng đào tạo phải đảm bảo bố trí chỗ ngồi cho học viên.

- Nhà thầu phải chuẩn bị, cấu hình hệ thống phần mềm thật hoặc hệ thống demo phục vụ đào tạo và cho các học viên thực hành.

- Giảng viên sử dụng máy chiếu, máy tính hướng dẫn lý thuyết và thực hành.

- Thiết lập phòng máy để học viên thực hành luôn trong buổi đào tạo, đảm bảo mỗi học viên 1 máy tính, và có đầy đủ tài liệu phát cùng.

b) Yêu cầu về chương trình đào tạo

- Chương trình đào tạo toàn diện: học viên được đào tạo về các kỹ năng sử dụng, thao tác được các chức năng của hệ thống. Kết thúc khóa học, học viên nắm được các chức năng sử dụng để có khả năng khai thác hệ thống một cách hiệu quả.

- Chương trình đào tạo cho người sử dụng phải đảm bảo đầy đủ các nội dung sau:

- + Giới thiệu nghiệp vụ chung về các quy trình trong hệ thống.

- + Hướng dẫn chi tiết từng chức năng của hệ thống.

- + Cách thức liên hệ khi cần hỗ trợ trong quá trình sử dụng.

- + Hướng dẫn thực hành theo từng vai trò. Các bài tập thực hành đảm bảo có dữ liệu mẫu và quy trình tuân tự phải thực hiện ứng với vai trò tương ứng của học viên.

## **6. Yêu cầu về kiểm thử và vận hành thử**

Đơn vị cung cấp dịch vụ chịu trách nhiệm kiểm thử phần mềm trong nội bộ của nhà thầu triển khai. Mọi chi phí liên quan do đơn vị cung cấp chi trả.

Hệ thống phải thực hiện vận hành thử trước khi tổ chức nghiệm thu, bàn giao sản phẩm đưa vào khai thác, sử dụng.

Công tác vận hành thử được thực hiện theo quy định tại Điều 34 của Nghị định số 73/2019/NĐ-CP ngày 05/9/2019 của Chính phủ và Điều 13 của Thông tư số 16/2024/TT-BTTTT ngày 30/12/2024 của Bộ Thông tin và Truyền thông.

Quy trình, thời gian và nội dung vận hành thử tuân thủ Điều 13 của Thông tư số 16/2024/TT-BTTTT ngày 30/12/2024 của Bộ Thông tin và Truyền thông quy định về hoạt động quản lý dự án, tư vấn và nghiệm thu dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

## **III. SỞ HỮU THÔNG TIN, DỮ LIỆU HÌNH THÀNH TRONG QUÁ TRÌNH CUNG CẤP DỊCH VỤ VÀ PHƯƠNG ÁN QUẢN LÝ, CHUYỂN GIAO CHO BÊN THUÊ**

**1. Xác định, làm rõ việc sở hữu các thông tin, dữ liệu hình thành trong quá trình cung cấp dịch vụ**

### **1.1. Quyền sở hữu thông tin**

Thực hiện theo Điều 48 Nghị định số 73/2019/NĐ-CP ngày 05 tháng 09 năm 2019 của Chính phủ: Thông tin, dữ liệu hình thành trong quá trình thuê dịch vụ CNTT thuộc sở hữu của cơ quan, đơn vị thuê. Nhà cung cấp dịch vụ có trách nhiệm bảo đảm an ninh,

an toàn thông tin, chuyển giao đầy đủ cho cơ quan, đơn vị thuê các thông tin, dữ liệu khi kết thúc hợp đồng thuê dịch vụ công nghệ thông tin.

## **1.2. Bản quyền, quyền sở hữu trí tuệ liên quan đến dịch vụ và các yêu cầu khác**

Thực hiện theo Điểm a Khoản 2 Điều 12 Thông tư số 16/2024/TT-BTTTT ngày 30/12/2024 Yêu cầu và quy trình chuyển giao thông tin và dữ liệu hình thành trong quá trình thuê dịch vụ, Chủ trì thuê dịch vụ và nhà cung cấp dịch vụ thỏa thuận, thống nhất các yêu cầu về bản quyền, quyền sở hữu trí tuệ liên quan đến dịch vụ và các yêu cầu khác tùy theo tính chất, đặc điểm, yêu cầu, nhu cầu thực tế của dịch vụ được cung cấp theo hợp đồng.

Toàn bộ thông tin, dữ liệu phát sinh trong quá trình sử dụng dịch vụ đều thuộc sở hữu của các cơ quan, đơn vị sử dụng dịch vụ và phải được bàn giao sau khi thanh lý hợp đồng.

## **2. Phương án quản lý, chuyển giao cho bên thuê**

Thực hiện theo Điểm a Khoản 2 Điều 12 Thông tư số 16/2024/TT-BTTTT ngày 30/12/2024 về việc quy định các nội dung đặc thù của hợp đồng thuê dịch vụ công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước, yêu cầu và quy trình chuyển giao thông tin và dữ liệu hình thành trong quá trình thuê dịch vụ với các nội dung chính sau:

- Sau khi kết thúc thời gian thuê, nhà cung cấp dịch vụ phải chuyển giao các thông tin và dữ liệu hình thành trong quá trình thuê dịch vụ cho chủ trì thuê dịch vụ theo phương án được quy định trong hợp đồng.

- Phương pháp, công cụ, quy trình và vai trò, trách nhiệm của mỗi bên trong quá trình chuyển giao; phương án kiểm tra xác định tình trạng thông tin và dữ liệu hình thành trước khi chuyển giao; phương án sao lưu, phục hồi dữ liệu trước khi chuyển giao (nếu cần thiết); phương án kiểm tra tình trạng thông tin và dữ liệu hình thành sau khi chuyển giao; phương án kiểm tra, đối soát dữ liệu sau khi chuyển giao; phương án xóa thông tin và dữ liệu liên quan đến chủ trì thuê dịch vụ trên các hệ thống tại nhà cung cấp dịch vụ sau khi chuyển giao.

- Các cam kết của nhà cung cấp dịch vụ sau khi chuyển giao.

- Các yêu cầu khác về chuyển giao thông tin và dữ liệu hình thành trong quá trình cung cấp dịch vụ.

## **3. Yêu cầu phát sinh trong quá trình khai thác, sử dụng dịch vụ**

Đơn vị cung cấp dịch vụ có cam kết khi phát sinh yêu cầu: về kỹ thuật, chức năng, tính năng của hệ thống, về kết nối, chia sẻ dữ liệu khi Chính phủ hoặc Bộ, ngành liên quan hoặc tỉnh yêu cầu hoặc khi có văn bản, quy định mới liên quan được ban hành. Ngoài ra, đơn vị cung cấp dịch vụ phải có trách nhiệm và cam kết cụ thể về thời gian cập nhật, bổ sung, nâng cấp chức năng trong hợp đồng khi đang trong giai đoạn

thuê.

Đối với hoạt động bảo trì và hỗ trợ hệ thống cần tuân thủ các yêu cầu:

+ Trong trường hợp hệ thống bổ sung, nâng cấp, cải thiện chất lượng các tính năng của hệ thống trong giờ làm việc chính thức, phải có thông báo bằng văn bản hoặc email đến khách hàng trước 24 giờ. Cơ quan đầu mối tiếp nhận thông tin: Sở Khoa học và Công nghệ tỉnh Tuyên Quang.

+ Yêu cầu lựa chọn thời điểm bảo trì ngoài giờ hành chính. Tổng thời gian bảo trì không ảnh hưởng tới thời gian sử dụng dịch vụ của khách hàng quá 02 giờ (120 phút).

+ Đối với các yêu cầu hỗ trợ sự cố của người dùng: Cam kết xử lý trong vòng không quá 4 giờ (giờ hành chính) kể từ khi được thông báo.

+ Bố trí nhân lực phụ trách xử lý, giải quyết các vấn đề vướng mắc, hỏi đáp của người dùng cũng như đơn vị thuê dịch vụ trong quá trình tham gia sử dụng dịch vụ.

+ Cam kết hỗ trợ vận hành 24/7 ngày trong suốt thời gian thuê dịch vụ

#### **4. Giải pháp và phương pháp luận:**

*Nhà thầu chuẩn bị đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định tại Chương V, gồm các phần như sau:*

- Giải pháp và phương pháp luận;

- Kế hoạch triển khai.

#### **5. Quy định về kiểm tra, nghiệm thu sản phẩm:**

*Nhà thầu chuẩn bị bộ hồ sơ để phục vụ công tác thanh, quyết toán hợp đồng, gồm các sản phẩm như sau:*

(1) Biên bản nghiệm thu đưa vào sử dụng dịch vụ;

(2) Biên bản nghiệm thu hoàn thành cung cấp dịch vụ từng tháng;

(3) Bảng xác định giá trị khối lượng công việc hoàn thành;

(4) Hóa đơn GTGT;

(5) Biên bản thanh lý hợp đồng (đối với kỳ thanh toán cuối cùng của năm 2026);