UBND TỈNH LẠNG SƠN **SỞ KHOA HỌC VÀ CÔNG NGHỆ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:3033 /SKHCN-CĐS	*Lạng Sơn, ngày 22 tháng 5 năm 2026*

THÔNG BÁO MỜI BÁO GIÁ

Thực hiện dịch vụ Kiểm tra đánh giá định kỳ an toàn thông tin cho các hệ thống thông tin của tỉnh và hệ thống cho trung tâm tích hợp dữ liệu tỉnh.

Kính gửi: Các công ty, doanh nghiệp cung cấp dịch vụ.

Căn cứ Kế hoạch số 333/KH-UBND ngày 31/12/2025 của UBND tỉnh Chuyển đổi số trên địa bàn tỉnh Lạng Sơn năm 2026. Sở Khoa học và Công nghệ tỉnh Lạng Sơn đang có nhu cầu lựa chọn các Công ty, đơn vị cung cấp: ***dịch vụ tư vấn công nghệ thông tin, dịch vụ tư vấn Đấu thầu và dịch vụ thẩm định giá để tham khảo,*** làm cơ sở xây dựng dự toán mua sắm dịch vụ "Kiểm tra đánh giá định kỳ an toàn thông tin cho các hệ thống thông tin của tỉnh và hệ thống cho trung tâm tích hợp dữ liệu tỉnh".

Sở Khoa học và Công nghệ tỉnh Lạng Sơn tổ chức tiếp nhận hồ sơ báo giá với nội dung cụ thể như sau:

I. Thông tin yêu cầu:

1. Đơn vị yêu cầu báo giá: Sở Khoa học và Công nghệ tỉnh Lạng Sơn (*Địa chỉ: Số 01, đường Mai Thế Chuẩn, phường Lương Văn Tri, tỉnh Lạng Sơn)*

2. Địa điểm tiếp nhận báo giá: Sở Khoa học và Công nghệ tỉnh Lạng Sơn.

3. Thời gian tiếp nhận báo giá: Từ ngày 22/5/2026 đến ngày 26/5/2026. Các báo giá gửi sau thời điểm trên sẽ không được xem xét.

II. Nội dung yêu cầu báo giá:

- Xem chi tiết tại các Phụ lục đính kèm.

- Thông tin trao đổi: ông Dương Anh Quân, Chuyên viên Phòng Chuyển đổi số, Sở Khoa học và Công nghệ tỉnh Lạng Sơn, điện thoại: 0949.269.811.

Sở Khoa học và Công nghệ tỉnh Lạng Sơn trân trọng thông báo và rất mong nhận được sự hợp tác của các đơn vị quan tâm tham gia./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở;
- Các phòng, đơn vị thuộc Sở;
- Lưu: VT, CĐS.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ KHOA HỌC VÀ CÔNG NGHỆ
TỈNH LẠNG SƠN

Trần Hữu Giang

PHỤ LỤC: MẪU BÁO GIÁ

Kính gửi: Sở Khoa học và Công nghệ tỉnh Lạng Sơn

Ngày …. /05/2026 chúng tôi (ghi tên công ty) nhận được công văn số …. của Quý đơn vị, chúng tôi xin báo giá các hạng mục công việc theo yêu cầu của Quý đơn vị như sau:

TT	Nội dung	Đơn vị tính	Số lượng	Đơn giá (VNĐ)	Thuế (VAT)	Thành tiền (VNĐ)	Ghi chú
I	**Kiểm tra đánh giá định kỳ an toàn thông tin cho các hệ thống thông tin của tỉnh và hệ thống cho trung tâm tích hợp dữ liệu lĩnh:**	Gói	1				
1	Kiểm tra đánh giá an toàn thông tin đối với hạ tầng thiết bị mạng và tường lửa tại Trung tâm tích hợp dữ liệu tỉnh số lượng 15 thiết bị.						Danh mục thiết bị và nội dung yêu cầu chi tiết tại Phụ lục 01
2	Kiểm tra, đánh giá phát hiện mã độc cho 110 máy chủ ảo, 70 máy chủ vật lý.						Danh mục máy chủ và nội dung yêu cầu chi tiết tại Phụ lục 02
3	Kiểm tra đánh giá an toàn thông tin đối với các phần mềm, ứng dụng, web số lượng 25.						Danh mục hệ thống thông tin và nội dung yêu cầu chi tiết tại Phụ lục 03

Lưu ý:

- Báo giá có giá trị 120 ngày và đã bao gồm thuế, các loại phí liên quan (nếu có).
- Thời gian thực hiện: Kể từ thời điểm hợp đồng có hiệu lực.
- Thời gian triển khai: 60 ngày kể từ ngày ký hợp đồng.

ĐẠI DIỆN CÔNG TY

PHỤ LỤC 01: NỘI DUNG KIỂM TRA, ĐÁNH GIÁ AN TOÀN THÔNG TIN ĐỐI VỚI THIẾT BỊ MẠNG

STT	Nội dung công việc thực hiện
1	**Khảo sát, thu thập các thông tin liên quan đến mục tiêu cần đánh giá**
2	**Nhận diện thiết bị (Audit)**
2.1	Nhận diện hostname, loại hệ điều hành, phần mềm lớp giữa
2.2	Xác định các cổng mở, các dịch vụ hoạt động trên các thiết bị
3	**Dò quét lỗ hổng bảo mật (VA)**
3.1	Sử dụng các các hệ thống/ công cụ để xác định các lỗ hổng, điểm yếu đang tồn tại trong các thành phần được cài đặt/ cấu hình trên thiết bị
3.2	Kiểm tra các bản các bản patch, update đã cài đặt
3.3	Kiểm tra các chính sách, cấu hình an ninh, an toàn trên thiết bị
3.4	Kiểm tra chính sách mật khẩu

PHỤ LỤC 02: KIỂM TRA, ĐÁNH GIÁ PHÁT HIỆN MÃ ĐỘC CHO 110 MÁY CHỦ ẢO, 70 MÁY CHỦ VẬT LÝ

STT	Nội dung công việc thực hiện
1	-Khảo sát, thu thập các thông tin liên quan đến mục tiêu cần đánh giá
2	- Dò quét, phát hiện mã độc, lỗ hổng, điểm yếu của hệ thống, thử nghiệm tấn công xâm nhập đối với các thiết bị hệ thống, hệ điều hành, ứng dụng, cơ sở dữ liệu và các thành phần khác liên quan trong hệ thống;
3	- Đưa ra phương án và kế hoạch xử lý lỗ hổng, điểm yếu và phương án cấu hình, tăng cường bảo mật đối với các nội dung kiểm tra được đánh giá là chưa đạt

PHỤ LỤC 03: NỘI DUNG KIỂM TRA, ĐÁNH GIÁ AN TOÀN THÔNG TIN ĐỐI VỚI PHẦN MỀM, ỨNG DỤNG, WEB

Danh sách ứng dụng, web	
1	Hệ thống nền tảng tích hợp, chia sẻ dữ liệu của tỉnh (LGSP)
2	Nền tảng Cửa khẩu số
3	Hệ thống Thư điện tử công vụ
4	Hệ thống CSDL Số hóa thủ tục hành chính
5	Cổng khai thác dữ liệu chuyển đổi số
6	Chuyển đổi số trong các ngành Giao thông vận tải, Tài nguyên và Môi trường, Nội vụ, Thông tin và Truyền thông, Nông nghiệp và Phát triển nông thôn, Xây dựng.
7	Nền tảng danh tính số
8	Kho dữ liệu dùng chung (data lake) phục vụ phân tích, dự báo hỗ trợ quá trình ra quyết định của tỉnh
9	Hệ thống họp hội nghị truyền hình trực tuyến
10	Hệ thống thông tin nguồn
11	Hệ thống trung tâm giám sát, điều hành an toàn, an ninh mạng (SOC)
12	Nền tảng CLOUD
13	Chuyển đổi số trong các ngành Tài chính, Kế hoạch và Đầu tư
14	Hệ thống phần mềm Quản lý hồ sơ cán bộ, công chức, viên chức
15	Sổ tay đảng viên
16	Hệ thống quản lý cơ sở dữ liệu Xây dựng tỉnh Lạng Sơn
17	Hệ thống quản lý CSDL dự án đầu tư xây dựng cơ bản
18	Hệ thống quản lý thông tin đất đai - Elis cloud
19	Hệ thống thi đua khen thưởng tỉnh Lạng Sơn
20	Hệ thống đánh giá, xếp loại chỉ số CCHC tỉnh

21	Hệ thống hỗ trợ thu thập, quản lý, khai thác cơ sở dữ liệu ngành và trung tâm điều hành giáo dục tỉnh Lạng Sơn
22	Hệ thống phần mềm cơ sở dữ liệu về công tác dân tộc
23	Nền tảng quản lý giá tỉnh Lạng Sơn
24	Hệ thống nền tảng phục vụ sản xuất nông nghiệp thông minh trên địa bàn tỉnh Lạng Sơn
25	Phần mềm Quản lý cấp giấy chứng nhận vệ sinh an toàn thực phẩm và kết quả thanh kiểm tra vệ sinh an toàn thực phẩm tỉnh Lạng Sơn

Nội dung công việc thực hiện		
STT	**Nội dung**	**Mô tả chi tiết công việc thực hiện**
1	Thu thập thông tin (Information Gathering)	
1.1	Sử dụng công cụ tìm kiếm và các công cụ khác để tìm kiếm thông tin	Thông tin về hệ thống được thu thập thông qua các search engine phổ biến như: Google, Bing, Baidu.
1.2	Xem thông tin web server để tìm kiếm thông tin	Thu thập các lỗ hổng đã được công bố từ thông tin web server, phiên bản cũ hơn hoặc các lỗ hổng tồn tại ở các version khác nhau.
1.3	Xem nội dung comment và thông tin meta data để tìm kiếm thông tin	Thông tin được thu thập trong quá trình này bao gồm: - Danh sách thư mục, đường dẫn thư mục trên hệ thống. - Danh sách các thư mục mà Spider hoặc Crawler không truy cập tới.
1.4	Xác định các điểm vào của ứng dụng	Tìm kiếm các đầu vào dữ liệu của ứng dụng ví dụ: ô tìm kiếm, đăng nhập, truy vấn dữ liệu từ người dùng.
1.5	Ánh xạ các đường dẫn thực thi	Phân tích trang báo lỗi nhằm thu được những thông tin về hệ thống: thông tin phiên bản ứng dụng, đường dẫn thư mục web.
1.6	Điều tra về nền tảng và công nghệ web server	Nhận diện framework mà ứng dụng web đang sử dụng, ví dụ: DotNetNuke, Drupal, Joomla.
2	Kiểm tra cấu hình (Configuration and Management Testing)	

2.1	Kiểm tra cấu hình ứng dụng	Đánh giá cấu hình của ứng dụng dựa vào các file cấu hình tìm thấy.
2.2	Kiểm tra khả năng xử lý các định dạng file.	Đánh giá quá trình xử lý của ứng dụng Web với những tập tin có phần mở rộng đặc biệt, có tên dài.
2.3	Xem lại các file cũ, file backup, các file dư thừa	Tìm kiếm tập tin cũ, backup, sample chưa được xóa trên hệ thống.
2.4	Tìm kiếm, liệt kê trang admin	Tìm kiếm giao diện quản trị của ứng dụng.
2.5	Kiểm tra các phương thức HTTP	Xác định những giao thức được hỗ trợ ngoài GET và POST (bao gồm OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, CONNECT).
2.6	Kiểm tra vấn đề bảo mật tầng vận chuyển HTTP	Kiểm tra ứng dụng có bắt buộc trình duyệt sử dụng kênh an toàn để truyền dữ liệu hay không.
3	Đánh giá quản lý định danh (Indentity Management Testing)	
3.1	Kiểm tra định nghĩa các vai trò	Kiểm tra các tài khoản đã được phân quyền đúng đắn phù hợp với nhu cầu công việc hay chưa
3.2	Kiểm tra quá trình đăng ký người dùng	Đánh giá quá trình đăng ký tài khoản có an toàn: có cơ chế chống bot đăng ký tự động, cơ chế xác nhận khi đăng ký thành công.
3.3	Kiểm tra khả năng liệt kê, tìm tài khoản	Đánh giá hệ thống thông qua bài test: - Đăng nhập tên tài khoản đúng và mật khẩu sai. - Đăng nhập tên tài khoản sai với mật khẩu bất kỳ. Sau đó so sánh sự đáp trả của hệ thống đối với hai bài test trên.
4	Đánh giá quá trình xác thực (Authentication Testing)	
4.1	Kiểm tra kênh truyền nội dung thông tin đăng nhập	Kiểm tra các thông tin đăng nhập có được mã hóa khi truyền hay không

4.2	Kiểm tra các xác thực mặc định	Thực hiện thử nghiệm đăng nhập đối với một số tài khoản mặc định thông dụng ví dụ: admin, administrator, system, manager, super, user, supperuser, root.
4.3	Kiểm tra khả năng leo thang đặc quyền	Thử nghiệm các phương pháp nhằm truy cập được tài nguyên của hệ thống mà không cần phải xác thực: truy cập thẳng tới tài nguyên, dò đoán SesionID, thay đổi tham số request, SQL Injection.
4.4	Kiểm tra các đối tượng liên kết trực tiếp không an toàn	Đánh giá quá trình xác thực trên các kênh truyền khác: mobile, tablet.
4.5	Kiểm tra tính năng ghi nhớ mật khẩu	Đánh giá chức năng ghi nhớ mật khẩu của ứng dụng có an toàn hay không.
4.6	Kiểm tra chức năng lưu cache trên trình duyệt	Kiểm tra chức năng lưu cache trên trình duyệt có lưu lại các thông tin nhạy cảm như user, password, cookies.
4.7	Kiểm tra chính sách đặt mật khẩu	Tiến hành đánh giá chính sách về mật khẩu an toàn trên hệ thống thông qua quá trình:
		- Tạo tài khoản mới trên hệ thống.
		- Thay đổi mật khẩu của tài khoản.
4.8	Kiểm tra tính năng đổi mật khẩu, reset mật khẩu	Đánh giá thông qua các bài kiểm tra:
		- Người dùng có thể thay đổi mật khẩu của người dùng khác hay không.
		- Người dùng có thể vượt qua hoặc phá vỡ cơ chế reset mật khẩu hay không: đoán token, can thiệp vào địa chỉ e-mail nhận token.
		- Hệ thống có tồn tại điểm yếu CSRF hay không.
4.9	Kiểm tra cơ chế xác thực qua các thành phần liên quan	Kiểm tra cơ chế xác thực qua các thành phần liên quan.
5	Đánh giá quá trình quản lý phân quyền (Authorization Testing)	

5.1	Kiểm tra lỗi Directory traversal/file	Kiểm tra Directory traversal/file include thông qua các thành phần cho phép nhập liệu: URL, webform.
5.2	Kiểm tra khả năng vượt qua cơ chế phân quyền	Thực hiện kiểm tra:
		- Truy cập tài nguyên khi chưa xác thực.
		- Truy cập tài nguyên sau khi đã đăng xuất.
		- Truy cập tới tài nguyên yêu cầu tài khoản mức cao hơn.
		- Truy cập tới các chức năng của quản trị viên.
5.3	Kiểm tra khả năng leo thang đặc quyền	Thử nghiệm nâng cao quyền hiện tại của người dùng hoặc tạo ra một tài khoản có quyền cấp cao hơn
5.4	Kiểm tra các đối tượng liên kết trực tiếp không an toàn	Thực hiện thay đổi tham số nhằm cố gắng truy cập các tài nguyên khác, các tài nguyên có độ bí mật cao hơn hoặc vượt qua cơ chế cấp quyền.
6	Đánh giá quản lý phiên (Session Management Testing)	
6.1	Kiểm tra khả năng vượt qua cơ chế quản lý phiên	Kiểm tra các thành phần của một session nhằm đảm bảo các thông tin được tạo ra an toàn và không thể dò đoán được
6.2	Kiểm tra các thuộc tính của cookie	Tiến hành phân tính các thuộc tính trong cookie, bao gồm: thuộc tính Secure, HttpOnly, Domain, Path, Expires
6.3	Kiểm tra lỗi Session Fixation	Kiểm tra hệ thống có tồn tại điểm yếu Session Fixation hay không
6.4	Kiểm tra các biến có khả năng lộ thông tin	Kiểm tra các thông tính trong Session Token có được giữ bí mật bao gồm Cookie, SessionID, Hidden Field; Session Token có thể tái sử dụng hay không
6.5	Kiểm tra lỗi Cross Site Request Forgery	Tiến hành các bài kiểm tra nhằm tìm kiếm, xác định điểm yếu CSRF có tồn tại trên ứng dụng hay không.
6.6	Kiểm tra tính năng đăng xuất	- Đánh giá về giao diện đăng xuất cho người dùng có trực quan, tiện lợi, dễ thao tác.
		- Hệ thống có tự động đăng xuất khi người dùng không thao tác sau một khoảng thời gian hay không.

		- Session có bị ngắt sau khi đăng xuất hay không.
7	Đánh giá quá trình kiểm tra dữ liệu đầu vào (Data Validation Testing)	
7.1	Kiểm tra lỗi Cross Site Scripting	Kiểm tra hệ thống có tồn tại điểm yếu Reflected, DOM-Base, Stored XSS hay không
7.2	Kiểm tra lỗi HTTP Parameter pollution	Kiểm tra hệ thống có tồn tại điểm yếu HTTP Parameter pollution hay không
7.3	Kiểm tra lỗi SQL Injection: Oracle, MySQL, SQL Server, PostgreSQL, MS Access, NoSQL	Kiểm tra hệ thống có tồn tại điểm yếu SQL Injection hay không
7.4	Kiểm tra lỗi LDAP Injection	Kiểm tra hệ thống có tồn tại điểm yếu LDAP Injection hay không
7.5	Kiểm tra lỗi ORM Injection	Kiểm tra hệ thống có tồn tại điểm yếu ORM Injection hay không
7.6	Kiểm tra lỗi XML Injection	Kiểm tra hệ thống có tồn tại điểm yếu XML Injection hay không
7.7	Kiểm tra lỗi SSI Injection	Kiểm tra hệ thống có tồn tại điểm yếu SSI Injection hay không
7.8	Kiểm tra lỗi XPath Injection	Kiểm tra hệ thống có tồn tại điểm yếu Xpath Injection hay không
7.9	Kiểm tra lỗi IMAP/SMTP Injection	Kiểm tra lỗi IMAP/SMTP Injection có tồn tại trên ứng dụng hay không.
7.1	Kiểm tra lỗi Code Injection: Local File Inclusion, Remote File Inclusion	Kiểm tra hệ thống có tồn tại điểm yếu Code Injection hay không:
		- Local File Inclusion.
		- Remote File Inclusion.
7.1	Kiểm tra lỗi Command Injection	Kiểm tra hệ thống có cho phép nhập và xử lý các câu lệnh mức hệ điều hành (Command) hay không
7.1	Kiểm tra lỗi Buffer overflow: Heap overflow, Stack overflow,	Kiểm tra hệ thống có tồn tài điểm yếu tràn bộ đệm hay không, bao gồm:

	Format string	- Heap Overflow.
		- Stack Overflow.
		- Format String.
7.1	Kiểm tra các lỗi có thể phát sinh khi vận hành	Đây là bài kiểm tra phức tạp, bao gồm một số bước kiểm tra:
		- Thành phần upload: cơ chế lọc file, có thể bị bypass hay không.
		- Điểm yếu liên quan đến SQL/XPATH Injection cho phép hacker upload nội dung vào cơ sở dữ liệu
		- Cấu hình hệ thống có cho phép cài đặt các gói hoặc thành phần ứng dụng hay không.
7.1	Kiểm tra lỗi HTTP Splitting/Smuggling	Kiểm tra khả năng bị tấn công trên nền của giao thức HTTP bao gồm:
		- HTTP splitting.
		- HTTP smuggling.
8	Kiểm tra xử lý lỗi (Testing for Error Handling)	
9	Kiểm tra mã hóa (Cryptography)	
9.1	Kiểm tra các mã hóa SSL/TLS yếu, các cơ chế bảo vệ tầng vận chuyển không hiệu quả	Đánh giá mức độ an toàn của SSL/TLS: giao thức, thuật toán mã hóa, độ dài khóa, BEAST, CRIME, Heart Bleed, Poodle.
9.2	Kiểm tra lỗi Padding Oracle	Kiểm tra hệ thống có tồn tại điểm yếu Padding Oracle hay không
9.3	Kiểm tra các thông tin nhạy cảm trên các kênh không mã hóa	Bao gồm 2 bài kiểm tra:
		- Ứng dụng có sử dụng HTTPS khi truyền dữ liệu nhạy cảm hay không.
		- Ứng dụng có bắt buộc người dùng sử dụng HTTPS hay không nếu người dùng chỉ nhập HTTP.
10	Đánh giá hoạt động nghiệp vụ (Business Logic Testing)	

10.1	Kiểm tra khả năng xác thực dữ liệu logic	Kiểm tra dữ liệu logic đầu vào cần được kiểm tra, thẩm định kỹ càng trước khi được thực thi
10.2	Kiểm tra khả năng ép buộc các yêu cầu	Thử nghiệm thực hiện các biện pháp phá vỡ cấu trúc luồng công việc để tiến tới bước cuối cùng trong luồng
10.3	Kiểm tra vấn đề tích hợp	Bao gồm quá trình:
		- Quan sát, phân tích các giá trị ẩn trong hệ thống.
		- Phân tích sự thay đổi (nếu có) của giá trị này trong toàn bộ quá trình hoạt động của ứng dụng.
		- Thực hiện thao tác thay đổi giá trị nhằm đánh giá ứng dụng có tồn tại điểm yếu hay không.
10.4	Kiểm tra vấn đề giới hạn số lần liên tiếp thực thi cùng một chức năng trong một khoảng thời gian	Tiến hành kiểm tra với mỗi chức năng, thành phần có thể tương tác một lần hay nhiều lần, đồng thời thực hiện các bài đánh giá nhằm vượt qua, phá vỡ chính sách kiểm soát đó
10.5	Kiểm tra sự xung đột trong luồng hoạt động	Thử nghiệm khả năng lạm dụng các chức năng:
		- Thử nghiệm truy cập vào tập tin không được phép tải về
		- Thay dấu nháy đơn (‘) vào vị trí của ID number.
		- Thay đổi GET thành POST.
		- Thêm các tham số vào request.
		- Gửi request có tham số, giá trị trùng lặp.