Chương V. YÊU CẦU VỀ KỸ THUẬT

1. Giới thiệu chung về dự toán, gói thầu:

- Tên gói thầu: DV-02: "Dịch vụ phân tán nội dung, chống tấn công mạng trên hệ thống phân tán nội dung toàn cầu cho báo điện tử, dịch vụ thư điện tử bảo mật".

- Địa điểm thực hiện: Số 7 Phan Đình Phùng, phường Hoàn Kiếm, Tp Hà Nội.

- Nội dung chính của gói thầu: Cung cấp Dịch vụ phân tán nội dung, chống tấn công mạng trên hệ thống phân tán nội dung toàn cầu cho báo điện tử, dịch vụ thư điện tử bảo mật của Báo Quân đội nhân dân.

- Thời gian thực hiện gói thầu: 365 ngày.

2. Mục tiêu công việc:

Cung cấp dịch vụ phân tán nội dung, chống tấn công mạng trên hệ thống phân tán nội dung toàn cầu cho báo điện tử, dịch vụ thư điện tử bảo mật của Báo Quân đội nhân dân.

3. Yêu cầu kỹ thuật của gói thầu:

3.1. Yêu cầu chung:

- Dịch vụ cung cấp cho gói thầu phải đồng bộ, có nguồn gốc chính hãng.

- Dịch vụ phải được cài đặt, vận hành hoàn toàn tương thích với hạ tầng trang thiết bị của Báo Quân đội nhân dân, không gây ảnh hưởng và gián đoạn vận hành an toàn của toàn bộ hệ thống.

3.2. Yêu cầu kỹ thuật cụ thể:

Tóm tắt yêu cầu của dịch vụ phải đáp ứng các thông số kỹ thuật và tiêu chuẩn sau đây:

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn (*)
1.	Dịch vụ phân tán nội dung (CDN)	- Là giải pháp mạng phân phối nội dung Content Delivery Network (CDN). Một hệ thống mạng nhiều máy chủ được đặt ở nhiều nơi khác nhau trên thế giới và chứa những bản sao dữ liệu của nội dung website trong hệ thống và khi người dùng truy cập vào thì các bản sao đó nằm tại một máy chủ gần với người dùng nhất sẽ được thay thế với dữ liệu nội dung gốc của website. Giả sử như máy chủ website ở Châu Âu nhưng khi một người dùng ở Việt Nam truy cập vào thì những dữ liệu mà người dùng nhận được là bản sao của máy chủ gốc được lưu trữ tại những máy chủ trong hệ thống CDN ở khu vực Đông Nam Á hoặc hoặc tại Việt Nam nơi gần người dùng nhất. - Giải pháp được cung cấp bởi nhà cung cấp uy tín trên thị trường. Nhà cung cấp có sẵn hoặc hợp tác chia sẻ sử dụng nhiều máy chủ ở nhiều vùng địa lý khác nhau trong nước và trên thế

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn (*)
		giới để đảm bảo khi người đọc truy cập nội dung hình ảnh, âm thanh, video clip, văn bản… từ trang web của Báo Quân đội nhân dân thì máy chủ gần người đọc nhất sẽ cung cấp nội dung, giúp tăng tốc độ phản hồi nội dung cho người đọc, và giảm tải áp lực về xử lý dữ liệu trên máy chủ chính của Báo Quân đội nhân dân. - Ngoài mục đích chính nâng cao băng thông – Bandwidth đạt tốc độ cao nhất của bạn đọc đến máy chủ, cải thiện tốc độ tải dữ liệu, một ưu điểm khác là: sẽ có nhiều máy chủ dự phòng, các máy chủ có thể thay nhau hoạt động ngay lập tức nếu có 1 máy chủ nào đó bị gặp sự cố. - Yêu cầu về dung lượng, băng thông, mạng máy chủ và hạ tầng: + Thời gian dịch vụ CDN: 12 tháng. + Dung lượng lữu trữ CDN: 2TB; + Băng thông trong nước CDN: 130TB/tháng; + Băng thông quốc tế CDN: 10TB/tháng; + Băng thông Trung Quốc: 500GB/tháng + Mạng lưới POP (Points of Presence): ▪ Tại Hà Nội: có ít nhất 03 máy chủ; ▪ Tại TP Hồ Chí Minh: có ít nhất 03 máy chủ; ▪ Có hạ tầng trong và ngoài nước (ít nhất 250 PoPs ở 30 quốc gia trên thế giới, cung cấp danh sách các quốc gia có đặt PoPs) ▪ Hạ tầng CDN đặt tại tối thiểu 03 ISP: VNPT, FPT, Viettel với băng thông tối thiểu là 500 Gbps (cung cấp tài liệu, hợp đồng chứng minh). + Có hạ tầng trong và ngoài nước (ít nhất 280 PoPs ở 33 quốc gia). + Khả năng mở rộng băng thông đến 600Gbps/ISP vào thời điểm cao điểm. + Băng thông tổng hạ tầng CDN tối thiểu đạt 1 Tbps. + Hệ thống CDN phải sử dụng giải pháp High Available / Failover, tự động cô lập vùng/thiết bị sự cố. - Yêu cầu về năng lực kỹ thuật: + Khả năng chịu tải hơn 10,000,000 CCU cùng lúc. + Bảo đảm tính liên tục của CDN: CDN sử dụng giải pháp định tuyến (routing) theo GEO/ISN của remote address (địa chỉ IP) của end-user để quyết định phản hồi thông tin IP của một máy chủ node để end-user thiết lập kết nối khi truy cập. + Ẩn IP máy chủ gốc giúp bảo vệ máy chủ không bị lộ thông tin IP tránh các rủi ro khai thác lỗ hổng từ các dịch vụ web được chạy trên server như: database, storage, vv… + Mid-Cache (Origin Shield): Nhằm giúp giảm số lượng

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn (*)
		request và traffic gửi về Origin trong trường hợp có nhiều nội dung chưa được cache và cùng lúc có rất nhiều server DA gọi về origin. + Rate limit: hạn chế số lượng request gửi/nhận đến origin nhằm giảm thiểu tấn công DDoS. + Custom CNAME: tạo các custom CNAME trong một phạm vi nhỏ các CNAME theo nhà mạng hoặc tùy chọn các CNAME riêng theo ISP. + Load Balancing: cấu hình các mode load balancing: Round Robin, IP Hash hoặc Weighted ở back-end khi có yêu cầu. + Multiple Origin: Cho phép có thể sử dụng nhiều Origin cho domain dịch vụ CDN; domain sử dụng nhiều Origin có thể được cấu hình Override SNI và Headers riêng biệt cho từng Origin. + Origin Control: Hỗ trợ quản lý Origin IP server, Override SNI hoặc tuỳ chỉnh Origin Headers + Failover: Mặc định khi thêm nhiều Origin cho domain thì hệ thống đã hỗ trợ failover, khi CDN không thể kết nối tới một Origin trong danh sách (status code là 502 hoặc 503), hệ thống sẽ tự động chuyển sang một Origin tiếp theo để kết nối, thứ tự sẽ lần lượt từ trên xuống. + Origin Override Headers: Ứng với mỗi Origin, có thể tùy chọn override Headers bằng cách thêm thuộc tính với định dạng JSON vào trường Headers khi thiết lập Origin, các key được thêm vào sẽ được thay thế khi có bất kỳ request nào được yêu cầu từ *end-user đi đến các máy chủ CDN và đến Origin*. + Origin Protocol: có thể sử áp dụng các protocol khi kết nối đến Origin như: HTTP, HTTPS, Follow. + Origin S3 Protocol. + Origin Root Directory (Base Directory): có thể sử dụng Origin URL vào path mà muốn sử dụng làm root directory. + Hỗ trợ HTTP/2 và HTTP3. + Hỗ trợ IPV6 + HTTP Strict Transport Security (HSTS): Cho phép dùng tính năng Override Response Headers của dịch vụ CDN để thiết lập header Strict Transport Security. + Force HTTPS: Hỗ trợ người dùng áp dụng redirect toàn bộ traffic đi qua hệ thống CDN. + Access Control: Hỗ trợ thiết lập các phương thức Whitelist, Blacklist và Token cho domain sử dụng qua dịch vụ CDN. + Cache Control: Có thể tạo một hoặc nhiều Cache Control policy khác nhau cho từng domain khác nhau của mình mà không bị giới hạn.

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn (*)
		+ Redirect Control: Có thể sử dụng redirect status code 301 và 302. Redirect policy có thể được tạo nhiều đường dẫn khác nhau cho nhiều domain khác nhau, Redirect policy chỉ hoạt động đúng với domain tương ứng. + CORS Control: Hỗ trợ thêm hoặc override CORS header của domain đi qua dịch vụ CDN mà không cần phải sửa đổi gì thêm Origin. + Purge Control: Hỗ trợ xóa theo prefix hoặc là xoá toàn bộ đường dẫn bao gồm cả queryString. Purge Cache hỗ trợ 5 phương thức: - Xóa Cache theo đường dẫn tuyệt đối - Xóa Cache bao gồm có chứa "ký tự" nhập vào - Xóa Cache theo bắt đầu một ký tự - Xóa Cache theo kết thúc bằng ký tự - Xóa Cache theo đuôi file (ví dụ .mp4, .m3u8...) Hỗ trợ HTTP Range *GEO Block nâng cao:* - IIỗ trợ cấu hình "Cho phép ngoại trừ Quốc gia/Lãnh thổ" - Hỗ trợ cấu hình "Chặn tất cả ngoại trừ Quốc gia/Lãnh thổ" *Condition Rules - Cho phép tùy biến các tham số:* - File Extension - HTTP Referer - HTTP Method - HTTP User-Agent - Client IP - File Name - URI PATH Áp dụng các quyền: Thiết lập TTL, Access Deny, Redirect, No-Cache, Max-age Security Token nâng cao: Basic Token Schema v2, Canal+ Token + BLOS Whitelist Referrer & App Package để kiểm soát truy cập nội dung Rate limit kết hợp IP + URL theo thời gian + Prefetch Control: Khi thao tác prefetch toàn bộ server DA sẽ tự động request về server Origin để kéo dữ liệu lên các POPs của CDN ngay cả khi không được yêu cầu từ người dùng cuối. + TLSs Control: Hỗ trợ phiên bản TLS 1.2 và 1.3. + Content Compression: Có hỗ trợ Gzip ở Origin. + Minify HTML, JS, CSS: tự động xử lý remove các khoảng trắng và các ký tự không dùng đến để giảm kích thước của tập tin.

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn (*)
		+ Image Resize, Convert Webp: Hỗ trợ nén và giảm kích thước ảnh để tiết kiệm băng thông nhưng vẫn giữ nguyên chất lượng hình ảnh. + Access Logs: Hỗ trợ tải các tập tin Access Log (đã được nén .gz) về để xem thêm các thông tin của người dùng cuối như: IP, Quốc Gia, Thời gian, User-Agent, Referrer, IP server DA, TTFB, Service Time, … + Audit Logs: có thể xem các hành động đã được thao tác trên portal, bao gồm các thông tin: email truy cập, hành động và thời gian. + SSL Certificate Management: Hỗ trợ thông báo thời gian hết hạn, domain đang được assign, thông tin của SSL. + API: Hỗ trợ khách hàng sử dụng API để tương tác với dịch vụ mà không cần sử dụng trên portal. + Live Streaming Low Latency: PUSH Method: • Đầu vào: RTMP • Chứng thực thông qua Whitelist IP • Chứng thực thông qua Credential (user/pass) • Cho phép tạo nhiều RTMP Application (Live Entrypoint) • Đầu ra: • Hỗ trợ một trong các định dạng sau: HTTP-FLV hoặc HTTP-HLS • Hỗ trợ giao thức đầu ra HTTPS cho định dạng HTTP-FLV, hoặc HTTP-HLS • Đảm bảo độ trễ so với luồng tín hiệu đầu vào ≤ 2 giây Bảo mật link đầu ra: • Hỗ trợ tắt / bật tính năng bảo mật link đầu ra • Bảo mật link đầu ra hỗ trợ việc kết hợp một trong các tham số: IP remote client, đường dẫn file, expiretime, chuỗi text bảo mật (secrect key) • Cho phép vô hiệu hóa token đã tạo ra: với các stream được bảo vệ bởi token đang được truy cập hợp lệ bởi IP của người dùng. Trong trường hợp cần thiết, tính năng cho phép vô hiệu token và chặn truy cập từ IP đó của người dùng, ngay cả khi token vẫn còn chưa hết hạn (expire time) • Cho phép chỉ ứng dụng cụ thể được quyền phát stream. • Cho phép chỉ website cụ thể được quyền phát stream. + Storage: Hỗ trợ giao thức FTP, SFTP và S3, có thể sử dụng

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn (*)
		thông tin S3 Credential để sử dụng với các SDK hỗ trợ quản lý file bằng S3 như AWS hoặc Minio. + Large File Download – LFD là lưu trữ tích hợp cho nhu cầu sử dụng lưu trữ và quản lý trên cùng một portal quản trị. + Hệ thống storage sử dụng đường truyền network 20Gbps và khả năng chịu tải đáp ứng được trên 30,000 request/s. + Replication: Hệ thống được xây dựng theo cơ chế Replication để đảm bảo dữ liệu luôn được lưu trữ ở nhiều server để giúp cho việc đọc ghi đạt được performance tốt nhất. + Có hệ thống monitor giúp theo dõi hiệu suất hoạt động một cách tường minh các chỉ số về lượng request per second, traffic, bandwidth, HIT rate và HTTP Status Code với độ trễ dưới 5 phút. *+ Tính năng lưu trữ Cloud Storage S3:* - S3 Compatible: Hoàn toàn tương thích với các API và công cụ AWS S3 - High Performance: Truy cập được tăng tốc bởi CDN với SLA 99.99% - Multiple Interfaces: Bảng điều khiển web, SDK, công cụ dòng lệnh CLI, REST API - Secure: Mã hóa hoặc lưu trữ phân tán, phân quyền ở mức bucket *+ Tính năng Web Accelerator:* - Hỗ trợ Cache cho các định dạng: Image (png, gif, jpeg), Javascript, CSS, HTML5 Audio/Video. - Tối ưu dữ liệu cho các thiết bị di động. - Cho phép vô hiệu hóa / kích hoạt tính năng Web Accelerator theo từng object. - Image Optimization: Hỗ trợ WebP/AVIF sử dụng các thuật toán nén tiên tiến. *+ Tính năng phân tích nâng cao (Advanced Analytics):* - Dashboard theo dõi Bandwidth/Traffic theo từng ISP và Domain - Theo dõi các mã lỗi HTTP status code - Lọc theo thời gian (giờ/ngày/tháng), Domain, vị trí địa lý - Xem báo cáo lượng truy cập theo nhà mạng (ISP) - User Agent: thống kê Browsers, Operating Systems, Devices - Referrer: theo dõi nguồn truy cập website - Most Popular Content: thống kê nội dung được truy cập nhiều nhất. - Visitor: thống kê tổng lượng unique visitors. Xuất báo cáo theo thời gian đối với tất cả domain Quản trị phân quyền: Cho phép tạo người dùng quản trị, phân quyền admin/report.

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn (*)
		Định tuyến CDN theo ISP: Nhận dạng IP thuộc ISP nào và tự động định tuyến tối ưu.
2.	Dịch vụ chống tấn công mạng trên hệ thống phân tán nội dung toàn cầu	- Dịch vụ được cài đặt hợp nhất và quản lí cùng hệ thống CDN hiện có trên cùng platform (Multi CDN), giúp tăng cường thêm khả năng chịu tải, tăng tốc độ load web, giảm thiểu khả năng tấn công Website lên mức tốt nhất. - Bảo vệ cho website QDND.VN (1 domain và 7 record). - Doanh nghiệp phải là doanh nghiệp bảo mật và có giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng do Bộ Thông tin và Truyền thông cấp (đính kèm giấy chứng nhận còn hiệu lực). - Có thể dễ dàng mở rộng trên hạ tầng trên portal kết nối với tất cả các nền tảng cloud như: GOOGLE, AWS, AKAMAI, ALIBABA Cloud, VNCDN. - Các nhà cung cấp có ít nhất 6 POP lớn tại Việt Nam, bao gồm Hà Nội và Thành phố Hồ Chí Minh có đặt đủ các ISP lớn VNPT, FPT, Viettel, Mobiphone. Yêu cầu về Băng thông dịch vụ (Băng thông của mỗi POP): - 6 Tbps (Hỗ trợ trong khoảng thời gian triển khai dịch vụ kể cả trường hợp có tăng trưởng băng thông) Domain/application : - DNS được quản lý có hỗ trợ DNS Security - Nhà cung cấp hỗ trợ triển khai cả di chuyển Máy chủ định danh và di chuyển từng phần CNAME Orgin selector: WAF có khả năng lựa chọn origin để lấy nội dung theo điều kiện được thiết lập sẵn: Host header, IP client, ... Monitoring: Hỗ trợ giám sát đồ trễ và uptime của website bằng các hình thức Real User Monitoring hoặc Synthetic monitoring. ZeroSSL, Let's Encrypt SSL: Nhà cung cấp hỗ trợ ZeroSSL hoặc Let's Encrypt SSL. **Tính năng DdoS:** *Tính năng phòng chống DDoS lớp 7* - Nhà cung cấp có liên kết với tất cả các ISP/Telecommunication company Việt Nam: FPT, VNPT, Viettel, Mobiphone và tất cả các đơn vị cung cấp như GOOGLE, AWS, AKAMAI, ALIBABA Cloud, VNCDN để giám sát và ngăn chặn tấn công trên Layer 3,4,7 của mô

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn (*)
		hình mạng OSI. - Hỗ trợ phát hiện và ngăn chặn các cuộc tấn công Zero-day DDOS attack. - Cho phép phòng chống DDoS mitigation layer 7 không giới hạn bất kể số lần, kích thước hoặc thời lượng tấn công mà không tính thêm phí. - Trong vòng 1 phút Nhà cung cấp phải đảm bảo giảm thiểu 90% các cuộc tấn công DDoS. - Nhà cung cấp cung cấp các hành động quy tắc DDoS ứng dụng khác nhau bao gồm block hoặc deny, log hoặc monitor, allow. - Nhà cung cấp cho phép người dùng điều chỉnh độ nhạy và hành động của quy tắc DDoS của ứng dụng cho mỗi quy tắc riêng lẻ. Tính năng phòng chống DDoS lớp 4 - Cho phép phòng chống và giảm thiểu DDoS layer 4 (TCP và UDP, ICMP) - Có khả năng chống DDoS Layer 4 tại từng PoP trên toàn cầu mà không cần chuyển về các trung tâm chống DDoS tập trung gây thêm độ trễ. *Chi tiết các loại tấn công DDoS được chống:* + Chống SYN Flood + Chống UDP Flood + Chống ICMP/ICMP Fragmentation Flood + Chống SYN-ACK / ACK+PSH Flood + Chống Fraggle/Smurf/Land Attack + Chống Slowloris Attack + Chống HTTP Flood + Kiểm soát cổng (Port) truy cập + Giới hạn số lượng kết nối/tần số từng IP, có thể đặt theo đơn vị giây. Tính năng WAF - Nhà cung cấp có tường lửa ứng dụng web (WAF) bao gồm tối thiểu bộ quy tắc được cấu hình trước để phát hiện chống lại các cuộc tấn công OWASP hàng đầu, lỗ hổng zero-day. Các bộ quy tắc được cập nhật tự động và thường xuyên để đối phó với các cuộc tấn công mới. - Nhà cung cấp cho phép người dùng điều chỉnh hành động của bất kỳ ID quy tắc WAF riêng lẻ nào. Các hành động bao gồm chặn, cho phép, lưu nhật ký, bỏ qua. - Nhà cung cấp có tối thiểu 100 quy tắc WAF tùy chỉnh với khả năng khớp với nhiều trường khác nhau bao gồm số địa

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn (*)
		chỉ IP, quốc gia, lục địa, tiêu đề giới thiệu HTTP, đường dẫn URI, chuỗi truy vấn - Có thể dễ dàng mở rộng trên hạ tầng trên portal kết nối với tất cả các nền tảng cloud như: GOOGLE, AWS, AKAMAI, ALIBABA Cloud, VNCDN. - Nhà cung cấp cung cấp cách kiểm tra quy tắc tường lửa (xem trước quy tắc) trước khi triển khai để đảm bảo rằng quy tắc sẽ hoạt động như mong đợi. - Nhà cung cấp hỗ trợ việc giải mã các truy cập Web qua SSL/TLS (HTTPS) - Có cơ chế ngăn chặn dò mật khẩu theo: HTTP status code hoặc thông báo trả về từ origin Tính năng phát hiện và phản ứng với BOT - Nhà cung cấp cung cấp khả năng phát hiện, phân loại và giảm thiểu lưu lượng truy cập bot hoặc tự động. - Nhà cung cấp có thể tạo các quy tắc tùy chỉnh để so khớp các yêu cầu với điểm số bot cụ thể (hoặc phạm vi) cùng với các trường khác để thực hiện các hành động cụ thể bao gồm ngăn chặn, ghi log, CAPTCHA và thử thách được quản lý - Nhà cung cấp có khả năng xác định các bot tốt bằng cách sử dụng cơ sở dữ liệu chữ ký được cập nhật tự động lên các bot tốt mới. - Nhà cung cấp cung cấp một cơ chế để đưa Javascript vào trình duyệt để giúp xác định bot. - Nhà cung cấp cung cấp bảng điều khiển phân tích bot trong đó thể hiện xác suất khả năng request đến từ bot cũng như nguồn gốc truy cập của bot. - Bảng điều khiển có thể lọc và đi sâu vào điểm số bot cụ thể hoặc một loạt điểm số bot. - Hành động phản ứng với Bot: Block hoặc Allow hoặc Challenge **Các tính năng bảo mật bổ sung** Tính năng Rate Limiting - Cho phép Rate Limiting với các quy tắc tùy chỉnh để đặt giới hạn số lượng request cho một URL/zone) - Cho phép Rate Limiting theo quốc gia. - Cung cấp khả năng đếm số lượng yêu cầu theo địa chỉ IP nguồn, tiêu đề HTTP và cookie. - Thông báo lỗi cho máy khách có thể tùy chỉnh được. - Hỗ trợ khả năng chuyển tiếp thông tin IP Client thực của người dùng cho backend - Hỗ trợ các giao thức mới nhất: HTTP/3, TLS 1.3

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn (*)
		Yêu cầu quản trị và giám sát Có quản trị qua Web - Hỗ trợ tính năng xác thực đa nhân tố với các tài khoản quản trị - Cho phép cảnh báo chứng chỉ sắp hết hạn - Hỗ trợ tính năng Configuration version control/audit log cho phép theo dõi sự thay đổi cấu hình phục vụ audit và khôi phục cấu hình cũ (nếu cần) Hỗ trợ báo cáo và điều tra sự cố: - Attack Types - Time frame - Top source IP/Country - Throughput Status (Response code)
3.	Dịch vụ thư điện tử bảo mật	- Đáp ứng nhu cầu sử dụng email theo tên miền và lưu trữ dữ liệu. Hệ thống email được bảo mật toàn diện cả chiều nhận và chiều gửi với lớp bảo mật thông minh để đảm bảo email đến người dùng là email sạch. - Hệ thống email phải có tường lửa bảo mật, có áp dụng công nghệ Machine Learning và vùng ảo (Virtual area) thông minh để kiểm duyệt email trước khi nhận vào hệ thống mail server. - Nhà cung cấp hệ thống email phải thực hiện lưu trữ dữ liệu tại Việt Nam (theo quy định tại Nghị định số 53/2022/NĐ-CP ngày 15/8/2023 của Chính phủ Quy định chi tiết một số điều của Luật An ninh mạng). - Hệ thống tường lửa email đạt tiêu chuẩn và được chứng nhận bởi Garner, Rapid7 *hoặc tương đương* - Hệ thống đáp ứng 100% các yêu cầu kỹ thuật của Bộ quy tắc bảo mật Email toàn cầu ITU-T X.1236 *hoặc tương đương* - Chi tiết dịch vụ: + Dịch vụ xác thực tên miền SSL cho mail.qdnd.vn. + Tổng dung lượng: 130GB (130 account). *Các tính năng kỹ thuật:* - Đồng bộ hóa email dễ dàng với Outlook và các ứng dụng client khác bằng giao thức Exchange (MAPI/EWS). - Gửi email nhanh chóng và nâng cao tỉ lệ email vào inbox. - Bảo vệ email với bộ lọc email giảm tỉ lệ spam đến 99%, bảo mật 2 lớp (multi Authenticator), chứng chỉ số, mã hóa email/kết nối. - Đồng bộ công việc hàng ngày với tính năng Lưu trữ tập tin, Quản lý danh bạ, Lịch hẹn, Ghi chú - tất cả trong một nền tảng. - Giảm thiểu mất thông tin với MX dự phòng, tự động lưu trữ và điều phối email khi máy chủ gặp sự cố. - Cho phép gửi/nhận email với khối lượng và số lượng lớn.

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn (*)
		- Kiểm soát mỗi account email không chiếm quá nhiều tài nguyên. - Nhanh chóng nâng cấp dung lượng lưu trữ và email theo yêu cầu của đơn vị sử dụng. - Bảo vệ dữ liệu truyền đến máy chủ an toàn với các giao thức mã hóa đa dạng: SMTPS, IMAPS, POP3S. - Tường lửa email dựa trên AI và máy học có thể chống lại các cuộc tấn công Social Engineering thông qua việc phân tích hành vi. - Hệ thống tường lửa email thể hiện trạng thái thư như: Mail Spam, mail sai DKIM, mail whitelist, mail blacklist, mail chặn URL độc hại, mail có code độc hại. - Hệ thống tường lửa email phát hiện và ngăn chặn giả mạo địa chỉ Email: Ngăn chặn các hành vi trộm cắp thông tin và Email lừa đảo và kiểm tra tính hợp lệ của Email đến. - Theo dõi định tuyến gửi & nhận: Nếu lộ trình Email bị thay đổi, hệ thống sẽ phát hiện và cảnh báo cho người nhận và xác thực Email đến. - Phát hiện và ngăn chặn tên miền tương tự: Phát hiện các Email giả mạo tên miền tương tự như Email thật và ngăn chặn các tên miền Email giả khó phát hiện nhất, chuyển Email đáng ngờ thành hình ảnh. - Vùng ảo (VA): kiểm tra tất cả địa chỉ được liên kết với thư bằng cách mở trước trong VA để kiểm tra các mã độc được ẩn đi. Loại bỏ các mối nguy hại tiềm ẩn khác bằng cách kiểm tra tất cả các URL có trong email, nếu nhận thấy có một liên kết khác, hệ thống sẽ tự động mở liên kết đó đến khi đảm bảo không còn URL nào sót lại. - Phát hiện và ngăn chặn mã độc mới: HệThống kiểm tra mã độc tệp đính kèm, phân tích hành vi người dùng và phân tích URL, Link lồng Link đến *n lần. - Lọc malware và các yếu tố nguy hiểm trong mail: Công nghệ AI và phân vùng ảo giúp lọc malware. Phát hiện các đường link nguy hiểm, các tên miền gần giống với tên miền nhận tránh tấn công phishing. - Đẩy mail bị chặn và whitelist email: Một số doanh nghiệp cấu hình email chưa chuẩn (thiếu SPF, DKIM, hoặc tên miền bị đánh dấu spam đối với các tổ chức quốc tế) có thể được đẩy mail đến với người dùng và whitelist để trao đổi mail. - Blacklist mail: Chặn email khách hàng cho dù đó là mail sạch, mail cấu hình chuẩn với tất cả giá trị và không có malware hay bất cứ nguy hiểm nào. - Kiểm tra mail bị chặn trực tiếp trên Secu E Cloud: Người dùng có thể tự kiểm tra mail chặn không cần nhờ người quản trị. - Báo cáo: Quản trị viên được chủ động bật hoặc tắt tính năng thiết lập gửi báo cáo tình trạng các mail bị chặn trong ngày đến người dùng cuối và tùy chỉnh theo khung giờ nhận báo cáo.

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn (*)
		- Quản lý mail gửi ra và hỗ trợ lọc mail đầu ra, sẽ kiểm soát được tình trạng spam mã độc sang các mail của đối tác. - Hệ thống tường lửa thể hiện phân loại thư như: Mail bình thường, mail bị chặn, mail nguy hiểm, mail được duyệt và có tính năng Filter để truy suất dữ liệu nhanh chóng. - Log: kiểm tra lịch sử đăng nhập và filter log. - Tạo nhóm mail: mỗi nhóm tối đa 100 địa chỉ. - Bộ lọc virus/malware: Bộ lọc virus/malware cho các mail gửi ra giúp lọc mail users gửi ra luôn sạch và đảm bảo uy tín cho doanh nghiệp. - Khóa Người Dùng Gửi Ra khi có dấu hiệu tấn công ra bên ngoài: Ngăn chặn việc gửi ra của một người dùng chỉ định - việc này sẽ hạn chế tối đa rủi ro khi một trong những máy tính của khách hàng bị nhiễm virus, mã độc. - Phê duyệt gửi mail: Người quản trị có thể quản lý duyệt mail gửi trên webmail - Quản lý mail gửi ra: Người quản trị có thể giới hạn số lượng, dung lượng mail gửi ra, cài đặt DKIM, thu hồi email, cài đặt báo cáo linh động đến người quản trị và người dùng thông thường. - Hẹn giờ gửi mail: Đặt lịch và hẹn giờ gửi mail theo ngày, giờ, phút… Người dùng có thể gửi mail công việc cho nhau và xác nhận công việc dựa trên mail. - Báo cáo: Quản trị viên được chủ động bật hoặc tắt tính năng thiết lập gửi báo cáo tình trạng các mail bị chặn trong ngày đến người dùng cuối và tùy chỉnh theo khung giờ nhận báo cáo. - Hệ thống mail bảo mật có khả năng loại bỏ tất cả các URL độc hại, kiểm tra URL tới điểm endpoint. Ngăn chặn tất cả các tệp độc hại, Ransomware... và những tác nhân gây hại mới nhất. Từ đó, giúp cho tòa soạn sử dụng email an toàn hơn, tránh các thiệt hại về mặt tài chính cũng như tránh bị mất các thông tin cá nhân hoặc các dữ liệu công việc quan trọng qua email.

(*)*Ghi chú:* Trường hợp nhà thầu đề xuất giải pháp công nghệ, kỹ thuật khác so với yêu cầu thì nhà thầu cần chứng minh kèm theo tài liệu:

- Tính tương đương và vượt trội về công nghệ của giải pháp kỹ thuật khác đó trong việc đảm bảo khai thác sử dụng hiệu quả theo các yêu cầu của gói thầu (có kèm theo tài liệu để chứng minh).

- Tính tương thích của giải pháp kỹ thuật khác đó ứng dụng trên hạ tầng phần cứng và phần mềm của Báo Quân đội nhân dân hiện có là hoàn toàn tương thích, phù hợp, không gây xung đột mà vẫn đảm bảo an toàn, hiệu quả, hiệu năng khai thác sử dụng hệ thống.

4. Quy định về kiểm tra, nghiệm thu sản phẩm:

Các kiểm tra cần tiến hành gồm có:

- Kiểm tra chung về dịch vụ (nhà cung cấp, chủng loại, nguồn gốc...).

- Kiểm tra thông số kỹ thuật (tính năng, chức năng) của dịch vụ, phần mềm.

Vận hành thử nghiệm các tính năng đảm bảo chất lượng và đặc tính kỹ thuật đáp ứng yêu cầu của hợp đồng.

- Phối hợp kiểm tra và nghiệm thu theo quy định của Bộ Quốc phòng.

5. Các yêu cầu khác:

- Nhà thầu phải là đơn vị có nhiều kinh nghiệm trong lĩnh vực của gói thầu; có áp dụng các hệ thống quản lý: ISO 27001, ISO 20000-1; đạt tiêu chuẩn Doanh nghiệp khoa học và công nghệ của Bộ Khoa học và Công Nghệ cấp (đính kèm giấy chứng nhận còn hiệu lực).

- Nhà thầu đã từng triển khai và cung cấp tối thiểu 02 hợp đồng cung cấp dịch vụ phân tán nội dung (CDN) và dịch vụ chống tấn công mạng trên hệ thống phân tán nội dung toàn cầu trong thời gian từ năm 2021 trở lại đây.

- Nhà thầu phải chịu hoàn toàn trách nhiệm về việc cung cấp dịch vụ của gói thầu khi triển khai trên hạ tầng của Báo Quân đội nhân dân nếu xảy ra sự cố hệ thống dẫn đến ảnh hưởng, gián đoạn quy trình sản xuất, xuất bản của Tòa soạn.

- Nhà thầu phải chịu hoàn toàn trách nhiệm nếu có bất kỳ khiếu kiện của bên thứ ba về vấn đề bản quyền của các dịch vụ cung cấp cho gói thầu này.

- Nhà thầu thuyết minh phương án kỹ thuật của gói thầu trong đó phải kèm theo thông tin tài khoản thử nghiệm (gồm đường dẫn link truy cập, tên và mật khẩu tài khoản thử nghiệm) để Bên mời thầu đánh giá tính năng, năng lực kỹ thuật dịch vụ mà nhà thầu đang vận hành so với đề xuất kỹ thuật của nhà thầu cho gói thầu này.

- Nhà thầu cần bố trí nhân sự có trình độ chuyên môn về kỹ thuật phù hợp trong lĩnh vực của gói thầu (Nộp scan bản gốc: văn bằng và chứng chỉ liên quan của nhân sự) để trực tiếp đảm nhiệm các công việc của gói thầu theo yêu cầu sau:

+ Cán bộ phụ trách kỹ thuật: 01 người; Kinh nghiệm: tối thiểu 05 năm trong lĩnh vực gói thầu; Trình độ chuyên môn: Đại học các chuyên ngành khoa học máy tính, truyền thông mạng máy tính, công nghệ thông tin, tin học ứng dụng, công nghệ kỹ thuật máy tính, điện tử-viễn thông, thông tin vô tuyến, điện-điện tử *hoặc tương đương*; Chứng chỉ chuyên môn: CISSP hoặc CRISC hoặc CEH hoặc BTL1 *hoặc tương đương*.

+ Cán bộ kỹ thuật: 01 người; Kinh nghiệm: tối thiểu 03 năm trong lĩnh vực gói thầu; Trình độ chuyên môn: Đại học, cao đẳng các chuyên ngành: khoa học máy tính, truyền thông mạng máy tính, công nghệ thông tin, tin học ứng dụng, công nghệ kỹ thuật máy tính, điện tử-viễn thông, thông tin vô tuyến, điện-điện tử *hoặc tương đương*; Chứng

chỉ chuyên môn: Certified Information Security Manager (CISM), Offensive Penetration Testing *hoặc tương đương*.

- Trong suốt thời gian thực hiện hợp đồng 12 tháng, nhà thầu cần:

+ Bố trí nhân sự hỗ trợ kỹ thuật 24giờ/ngày+7ngày/tuần trong suốt thời gian thực hiện hợp đồng 12 tháng.

+ Cam kết xử lý sự cố trong vòng 01 giờ kể từ khi nhận được yêu cầu của đơn vị sử dụng vào bất kỳ thời điểm nào.

+ Thực hiện kiểm tra để tối ưu tốc độ và hiệu quả các dịch vụ tối thiểu mỗi tháng 02 lần vào ngày 01 và ngày 15 hàng tháng, và cung cấp báo cáo, tài liệu cho chủ đầu tư sau khi hoàn thành công việc.