CHƯƠNG V - YÊU CẦU KỸ THUẬT

Mục 1. Yêu cầu về kỹ thuật

I. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu

- **Tên dự án:** "Giải pháp phòng chống thất thoát dữ liệu tại PVcomBank năm 2025".
- **Tên gói thầu:** "Giải pháp phòng chống thất thoát dữ liệu tại PVcomBank năm 2025".
- **Mục tiêu đầu tư:**

  Dự án sau khi được triển khai phải đảm bảo đáp ứng các mục tiêu chính như sau:

  + Đảm bảo tuân thủ quy định của NHNN trong báo cáo 285/BC-NHNN ngày 16/8/2024.
  + Giảm thiểu nguy cơ thất thoát dữ liệu quan trọng của Ngân hàng ra bên ngoài bởi các hành vi vô tình/hành vi cố ý của người dùng.
  + Giám sát, lưu vết và điều tra, quy trách nhiệm đối với những đối tượng có hành vi gây thất thoát dữ liệu của Ngân hàng.
  + Hỗ trợ Ngân hàng đáp ứng các yêu cầu về bảo mật dữ liệu của tiêu chuẩn bảo mật dữ liệu thẻ thanh toán PCI DSS, tuân thủ quy định về bảo mật/bảo vệ dữ liệu nhạy cảm trong Thông tư 09/2020/TT-NHNN ngày 21/10/2020 và nhiều văn bản chỉ đạo từ NHNN.
  + Phát hiện, cảnh báo sớm các hành vi truy cập trái phép có dấu hiệu khai thác/tấn công hệ thống CNTT tại PVcomBank.
- **Quy mô dự án:** Dự án Giải pháp phòng chống thất thoát dữ liệu tại PVcomBank năm 2025 bao gồm:

STT	Hạng mục	Đơn vị tính	Số lượng
1	Giải pháp phòng chống thất thoát dữ liệu cho Network.	User	1.000
2	Giải pháp phòng chống thất thoát dữ liệu cho Endpoint.	User	1.000
3	Mã hoá máy trạm.	Thiết bị	100
4	Giải pháp Gán nhãn.	User	1.000
5	Giải pháp Discover.	Thiết bị/máy chủ/node	250

STT	Hạng mục	Đơn vị tính	Số lượng
6	Giải pháp phòng chống thất thoát dữ liệu cho Cloud.		
6.1	Giải pháp phòng chống thất thoát dữ liệu cho Office 365.	User	1.000
6.2	Giải pháp phòng chống thất thoát dữ liệu cho AWS S3 (dung lượng 5TB, 40 nguồn dịch vụ).	Gói	01
7	Dịch vụ triển khai phân loại dữ liệu, xây dựng chính sách/quy trình /quy định về phòng chống thất thoát dữ liệu (DLP); triển khai công cụ DLP (triển khai cài đặt và đào tạo chuyển giao công nghệ); bảo hành, bảo trì.	Gói	01

- **Địa điểm:** Triển khai tại Hội sở và các địa điểm do PVcomBank chỉ định trên toàn quốc.
- **Thời gian thực hiện gói thầu:** Tối đa 365 ngày (12 tháng) (bao gồm cả ngày nghỉ, ngày lễ) kể từ ngày hợp đồng có hiệu lực.

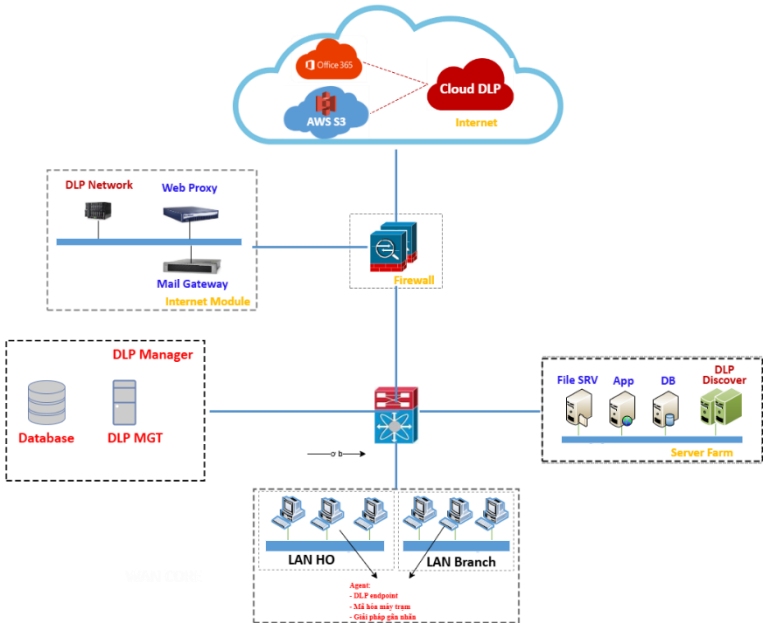
II. Yêu cầu về kỹ thuật:

1. Phạm vi cung cấp:

STT	Hạng mục	Đơn vị tính	Số lượng
1	Giải pháp phòng chống thất thoát dữ liệu cho Network.	User	1.000
2	Giải pháp phòng chống thất thoát dữ liệu cho Endpoint.	User	1.000
3	Mã hoá máy trạm.	Thiết bị	100
4	Giải pháp Gán nhãn.	User	1.000
5	Giải pháp Discover.	Thiết bị/máy chủ/node	250
6	Giải pháp phòng chống thất thoát dữ liệu cho Cloud.		
6.1	Giải pháp phòng chống thất thoát dữ liệu cho Office 365.	User	1.000
6.2	Giải pháp phòng chống thất thoát dữ liệu cho AWS S3 (dung lượng 5TB, 40 nguồn dịch vụ).	Gói	01

STT	Hạng mục	Đơn vị tính	Số lượng
7	Dịch vụ triển khai phân loại dữ liệu, xây dựng chính sách/quy trình/quy định về phòng chống thất thoát dữ liệu (DLP); triển khai công cụ DLP (triển khai cài đặt và đào tạo chuyển giao công nghệ); bảo hành, bảo trì.	Gói	01

2. Yêu cầu về kiến trúc triển khai

STT	Hạng mục	Yêu cầu
TEC.1	Mô hình kiến trúc triển khai	Giải pháp DLP triển khai ở PVcomBank phải đảm bảo mô hình kiến trúc triển khai và các thành phần tối thiểu như sau để phù hợp với hiện trạng hệ thống CNTT:  - Giải pháp phòng chống thất thoát dữ liệu cho Network (DLP Network): bao gồm 2 thành phần là DLP prevent WEB và DLP prevent Email - Thành phần quản trị tập trung cho giải pháp DLP (DLP Manager): bao gồm DLP MGT và máy chủ database, thực hiện chức năng quản trị tập trung cho các thành phần triển khai ở máy trạm (dạng agent) như sau: + Giải pháp phòng chống thất thoát dữ liệu cho Endpoint (DLP Endpoint). + Mã hóa máy trạm. + Giải pháp Gán nhãn. - Giải pháp Discover.

STT	Hạng mục	Yêu cầu
		- Giải pháp phòng chống thất thoát dữ liệu cho Cloud (DLP Cloud) bao gồm tối thiểu: + Giải pháp phòng chống thất thoát dữ liệu cho Office 365. + Giải pháp phòng chống thất thoát dữ liệu cho AWS S3.
TEC.2	Giải pháp phòng chống thất thoát dữ liệu cho Network	DLP mức mạng (web, email): tích hợp với hệ thống web proxy và email gateway để phòng chống thất thoát dữ liệu cho luồng truy cập web hoặc luồng truyền gửi email tại cổng kết nối internet.
TEC.3	Giải pháp phòng chống thất thoát dữ liệu cho Endpoint	DLP tại máy trạm, máy chủ vật lý: đảm bảo dữ liệu nhạy cảm trên máy trạm, máy chủ vật lý được kiểm soát và hạn chế thất thoát ra ngoài, sao chép sang USB, in ấn... Riêng đối với hệ thống máy chủ ảo hóa thì không cần cài agent vì không có khả năng thất thoát qua kênh sao chép USB hoặc in ấn. Trong trường hợp thất thoát qua việc truyền gửi ra bên ngoài thì đã được bảo vệ bởi kênh DLP mức mạng (DLP network). Ngoài ra trên máy chủ đã có các giải pháp PAM để kiểm soát các thao tác thực hiện trên máy chủ.
TEC.4	Mã hoá máy trạm	Thực hiện chức năng mã hóa dữ liệu trên máy trạm (PC, laptop), dùng để phòng chống thất thoát dữ liệu máy trạm ở mức vật lý trong trường hợp ổ cứng bị mất hoặc kẻ xấu dùng USB boot để truy cập trái phép máy tính người dùng.
TEC.5	Giải pháp Gán nhãn	Cung cấp tính năng để ngay khi người dùng thực hiện phân loại, dữ liệu sẽ được gán nhãn vào Header/Footer/Watermark hoặc vào meta data của dữ liệu.
TEC.6	Giải pháp Discover	DLP cho hệ thống lưu trữ: áp dụng cho các thành phần file server, folder lưu trữ. Cho phép rà soát, tìm kiếm và phân loại các file chứa dữ liệu nhạy cảm trên các hệ thống lưu trữ tại máy trạm, máy chủ.
TEC.7	Giải pháp phòng chống thất thoát dữ liệu cho Cloud	DLP cloud: giải pháp sẽ tích hợp trực tiếp với các cloud service qua API để phòng chống thất thoát dữ liệu. Giải pháp áp dụng cho các dịch vụ lưu trữ S3 của PVcomBank trên AWS và O365.

STT	Hạng mục	Yêu cầu
TEC.8	Thành phần quản trị tập trung DLP Manager	Bao gồm tối thiểu 2 thành phần là cấu phần quản trị tập trung (DLP MG) và máy chủ cơ sở dữ liệu (Database) cung cấp khả năng chạy HA và thực hiện chức năng quản trị tập trung: - Triển khai Agent tập trung, định nghĩa và áp dụng chính sách tập trung. - Thu nhận và lưu trữ sự kiện an ninh, giám sát và báo cáo tập trung cho toàn bộ hệ thống bảo mật (DLP endpoint, mã hóa máy trạm, gán nhãn, DLP Network, DLP Cloud).

3. Yêu cầu về tính năng kỹ thuật

a. Yêu cầu kỹ thuật chung

STT	Hạng mục	Yêu cầu
TEC.9	Yêu cầu về hỗ trợ ngôn ngữ	- Giải pháp phải hỗ trợ giao diện người sử dụng tối thiểu bằng tiếng Anh. - Giải pháp hỗ trợ font Unicode đối với dữ liệu (bao gồm dữ liệu do người dùng nhập vào hệ thống và dữ liệu tích hợp, xử lý trong hệ thống). - Giải pháp phải có khả năng nhận diện và áp dụng chính sách phòng chống thất thoát dữ liệu đầy đủ cho dữ liệu/tài liệu bằng ít nhất 02 ngôn ngữ Tiếng Việt, Tiếng Anh.
TEC.10	Tương thích với các trạng thái của dữ liệu	Giải pháp phải cho phép nhận diện và áp dụng biện pháp phòng chống thất thoát đối với dữ liệu ở tất cả trạng thái đang được lưu trữ, đang được xử lý và đang được truyền tải (data at rest, data in use và data in motion).
TEC.11	Tương thích với cấu trúc dữ liệu	Giải pháp cho phép nhận diện và áp dụng biện pháp phòng chống thất thoát đối với dữ liệu có cấu trúc, dữ liệu phi cấu trúc và dữ liệu bán cấu trúc và nhà thầu phải mô tả cụ thể cách thức giải pháp nhận diện như thế nào đối với từng loại dữ liệu này.

b. Yêu cầu kỹ thuật cho giải pháp phòng chống thất thoát dữ liệu cho Network

STT	Hạng mục	Yêu cầu
TEC.12	Giám sát luồng và kiểm soát	- Giải pháp ghi nhận và theo dõi và lưu trữ toàn bộ luồng truyền gửi (bao gồm cả luồng vi phạm chính sách, cũng như luồng không vi phạm chính sách) để phục vụ các nhu cầu điều tra thất thoát dữ liệu sau này.

STT	Hạng mục	Yêu cầu
	các luồng dữ liệu	- Giải pháp cho phép thử nghiệm/kiểm thử rule mới trên luồng truyền gửi đã ghi nhận để xem xét mức độ hiệu quả trước khi áp dụng chính thức.
TEC.13	Tùy biến chính sách theo luồng dữ liệu	Giải pháp cho phép lựa chọn luồng truyền gửi nào sẽ được ghi nhận và lưu trữ dựa trên các bộ tiêu chí nhất định (theo giao thức, nội dung).
TEC.14	Cảnh báo và ngăn chặn các hành vi của người dùng	Giải pháp thực hiện chặn hoặc đưa ra cảnh báo, hoặc cho phép người dùng thực hiện các hành vi sau đây: - Người dùng sao chép nội dung hoặc đính kèm file dữ liệu Mật/Nội bộ/Công khai vào email (sử dụng các email client bao gồm tối thiểu: MS Outlook, Gmail, Hotmail, Yahoo) gửi ra ngoài domain PVcomBank. - Cắt ghép, sao chép, soạn lại nội dung dữ liệu Mật/Nội bộ/Công khai và upload lên các trang web sử dụng các trình duyệt bao gồm tối thiểu: IE, Firefox, Chrome, Opera, Safari ngoài domain PVcomBank. Cho phép thiết lập chính sách dựa trên từng URL/Website.

c. Yêu cầu kỹ thuật cho giải pháp phòng chống thất thoát dữ liệu cho Endpoint

STT	Hạng mục	Yêu cầu
TEC.15	Tự động nhận diện và áp dụng các biện pháp phòng chống thất thoát dữ liệu theo dấu hiệu nhận biết	Giải pháp cho phép tự động nhận diện và áp dụng biện pháp phòng chống thất thoát theo một hoặc một tập hợp các dấu hiệu nhận biết nhất định, bao gồm nhưng không giới hạn: - Nhận diện theo mẫu văn bản (text pattern): tự động nhận diện các dữ liệu có chung một số đặc điểm về độ dài, số ký tự, định dạng ký tự (ví dụ như số điện thoại, số tài khoản, tên người…). - Nhận diện theo từ khóa (keywords): tự động nhận diện dữ liệu theo các từ khóa đặc thù. - Nhận diện theo vị trí lưu trữ dữ liệu. - Nhận diện theo ứng dụng tạo ra dữ liệu. - Nhận diện theo một số tiêu chí khác như định dạng file, trường thông tin trong file.
TEC.16	Tự động nhận diện và áp dụng	Giải pháp cho phép tự động nhận diện và áp dụng biện pháp phòng chống thất thoát dữ liệu cho các định dạng file bao gồm nhưng không

STT	Hạng mục	Yêu cầu
	các biện pháp phòng chống thất thoát dữ liệu theo định dạng tài liệu	giới hạn: file văn bản, file trang tính, file trình chiếu, file hình ảnh, file thiết kế và các định dạng file điện tử khác, cụ thể: - Đối với các file bảng tính excel hoặc tương tự (định dạng file bao gồm tối thiểu: *.xla, *.xlam, *.xll, *.xlm, *.xls, *.xlsm, *.xlsx, *.xlt, *.xltm, *.xltx), giải pháp có thể nhận diện dữ liệu trong từng ô của bảng tính. Với file có nhiều sheet có thể đọc được từng sheet. - Đối với các file văn bản soạn thảo dạng word, text, powerpoint hoặc tương tự (định dạng file bao gồm tối thiểu: *.doc, *.docm, *.docx, *.dot, *.dotx, *.dotm, *.ppsx, *.ppt, *.pptm, *.pptx, *.tmp, *.pdf) giải pháp có thể nhận diện trong toàn bộ nội dung của văn bản. - Đối với các file hình ảnh, đồ họa, tệp bản vẽ, file trình chiếu hoặc tương tự (định dạng file bao gồm tối thiểu: *.bmp, *.gif, *.jpeg, *.png, *.tiff). - Đối với các file nén (định dạng file bao gồm tối thiểu: *.7z, *.bin, *.rar, *.zip) giải pháp có cơ chế để phòng chống thất thoát dữ liệu cho từng file chứa trong file nén. Nhà thầu mô tả chi tiết về kỹ thuật, công nghệ áp dụng.
TEC.17	Xử lý đối với các tài liệu mã hóa, đặt mật khẩu, đính kèm trong tài liệu khác	- Các file dữ liệu có mật khẩu hoặc mã hóa, giải pháp phải xử lý để có thể nhận diện và cảnh báo phòng chống thất thoát như đối với file thông thường không có mật khẩu, mã hóa. - Giải pháp phải phát hiện và kiểm soát dữ liệu nhạy cảm trong một file được attach trong file khác.
TEC.18	Tính năng hiển thị cảnh báo cho người dùng	Giải pháp có hiển thị cảnh báo trên màn hình người dùng như "Chặn/Cảnh báo/Cho phép" đồng thời đưa ra hành động thực hiện theo phản hồi tương ứng khi người dùng thực hiện các hành vi sau đây: - Truyền gửi dữ liệu nhạy cảm lên các dịch vụ lưu trữ cloud bao gồm tối thiểu như Google Drive, Dropbox, OneDrive, Icloud, Box Sync. - Sao chép nội dung hoặc đính kèm file dữ liệu Mật/Nội bộ/Công khai vào email (sử dụng các email client bao gồm tối thiểu: MS

STT	Hạng mục	Yêu cầu
		Outlook, Gmail, Hotmail, Yahoo) gửi ra ngoài domain PVcomBank. - Cắt ghép, sao chép, soạn lại nội dung dữ liệu Mật/Nội bộ/Công khai và upload lên các trang web sử dụng các trình duyệt bao gồm tối thiểu IE, Firefox, Chrome, Opera ngoài domain PVcomBank. - Truyền gửi dữ liệu nhạy cảm ra các thiết bị lưu trữ ngoại vi bao gồm tối thiểu (USB, CD/DVD). - Thực hiện lệnh in để in ấn dữ liệu nhạy cảm. Cho phép thiết lập chặt chẽ theo các trường hợp máy in local hoặc máy in kết nối mạng.
TEC.19	Ngăn chặn sử dụng các ứng dụng ngang hàng	Ngăn chặn người dùng sử dụng các ứng dụng ngang hàng (P2P), các ứng dụng nhắn tin trực tuyến có mã hóa đầu cuối bao gồm tối thiểu (Zalo, Skype, Viber, Whatsapp) trên giao diện web để truyền gửi file chứa dữ liệu nhạy cảm.
TEC.20	Giám sát các giao thức mạng	Giải pháp cho phép giám sát người dùng truyền gửi dữ liệu nhạy cảm thông qua tất cả giao thức mạng (bao gồm cả TCP, UDP). Có khả năng thiết lập chặt chẽ dựa trên các tiêu chí: network direction, dải IP, dải port, ứng dụng/tiến trình khởi tạo kết nối truyền gửi.
TEC.21	Chống chụp màn hình	Giải pháp không cho phép người dùng chụp màn hình dữ liệu nhạy cảm (sử dụng phím Print screen và dùng các phần mềm trên máy tính để chụp màn hình).
TEC.22	Chống sao chép dữ liệu giữa các ứng dụng	Giải pháp có cảnh báo khi người dùng sử dụng Clipboard để copy/paste dữ liệu nhạy cảm: Kiểm soát được hành vi copy dữ liệu nhạy cảm từ giao diện ứng dụng nào và paste sang giao diện ứng dụng nào.
TEC.23	Chống thất thoát dữ liệu khi máy trạm không hoạt động ở chế độ bình thường (và	- Giải pháp có khả năng kiểm soát/phòng chống thất thoát kể cả trường hợp máy tính login chế độ Safemode (người dùng truy cập chế độ safemode rồi truyền gửi dữ liệu, làm biến dạng dữ liệu như thay đổi tên file, đổi đuôi/format file, nén, mã hóa) rồi gửi ra bên ngoài. - Giải pháp hỗ trợ áp dụng chính sách DLP trong các trường hợp máy tính không kết nối hệ thống PVcomBank (offline) – trong trường hợp không kết nối mạng vẫn phải áp dụng chính sách.

STT	Hạng mục	Yêu cầu
	kết nối mạng)	
TEC.24	Kiểm soát thiết bị ngoại vi	- Cho phép kiểm soát chặt chẽ, chính xác các thiết bị ngoại vi theo các tham số bao gồm tối thiểu: Bus Type, CD/DVD Drivers, Device Class, Device Compatible IDs, Device Instance ID, Device Instance Path, Device Name, File System Type, File System Access, File System Volume Label, File System Volume Serial Number, PCI VendorID/DeviceID, USB Class Code, USB Device Serial Number, USB vendor ID/ProductID. - Kiểm soát việc người dùng kết nối và sử dụng các thiết bị ngoại vi trên máy tính của PVcomBank, nhằm hạn chế tối đa các thất thoát dữ liệu qua kênh ngoại vi (Device Control): + Kiểm soát việc kết nối và sử dụng các thiết bị lưu trữ ngoại vi (removable storage), thiết bị plug-and-play. + Kiểm soát việc mở/chạy các file từ thiết bị ngoại vi. + Kiểm soát việc copy dữ liệu nhạy cảm ra các thiết bị ngoại vi. - Cung cấp cơ chế request & approve hoặc tương tự để cho phép bypass/sử dụng USB trong 1 khoảng thời gian.
TEC.25	Hình thức kiểm soát bảo vệ dữ liệu	Hỗ trợ các hành vi kiểm soát bao gồm: ngăn chặn việc sử dụng, giám sát việc sử dụng, thiết lập chế độ read-only, cảnh báo cho người dùng, lưu lại thông tin hành vi vi phạm của người dùng.
TEC.26	Giám sát và phát hiện việc truyền gửi dữ liệu qua các kênh chia sẻ tài liệu	Giải pháp phải giám sát được việc truyền gửi trên các kênh FTP, Remote Desktop với các hành vi cụ thể: - Người dùng truyền/upload file lên FTP bên ngoài domain PVcomBank. - Người dùng share file/truyền dữ liệu qua các chương trình Remote access (Remote desktop).

d. Yêu cầu kỹ thuật cho giải pháp mã hóa máy trạm

STT	Hạng mục	Yêu cầu
TEC.27	Yêu cầu về khóa mã hóa	- Mã hóa: Ổ cứng, File, folder, file server/File share, USB. - Sử dụng mã hóa an toàn khi mã hóa dữ liệu trên máy trạm, tối thiểu là AES-256.

		- Cung cấp sẵn công cụ kiểm tra tính tương thích của ổ đĩa/máy tính tự động trước khi thực hiện mã hóa đảm bảo tính an toàn cho dữ liệu khi mã hóa.
TEC.28	Yêu cầu về quản lý key	- Có khả năng sử dụng nhiều loại khóa mã hóa khác nhau như: Khóa mã hóa cá nhân, khóa nhóm, local Key. - Hỗ trợ quản lý key tập trung và có key backup offline để dự phòng.

e. Yêu cầu cho giải pháp Discover

STT	Hạng mục	Yêu cầu
TEC.29	Khả năng dò quét	- Giải pháp cho phép dò quét, khám phá các file được lưu trữ trong các folder trên tất cả các hệ thống bao gồm tối thiểu document repository (CIFS/NFS…), Database (MSSQL, Oracle...), Sharepoint để xác định dữ liệu nhạy cảm, từ đó phân loại và áp dụng chính sách phòng chống thất thoát phù hợp. - Giải pháp cung cấp chức năng phân tích hình ảnh (OCR), giúp quét và định danh các dữ liệu quan trọng trong hình ảnh đang lưu trữ trên các repository.
TEC.30	Đặt lịch quét	Giải pháp có khả năng lập lịch dò quét, thiết lập mức độ băng thông sử dụng dò quét
TEC.31	Chế độ dò quét dữ liệu	Giải pháp cung cấp nhiều chế độ dò quét dữ liệu, bao gồm tối thiểu chế độ sau: Dò quét và kiểm kê tất cả dữ liệu hệ thống; Dò quét và định danh/phân loại các kiểu dữ liệu đã và đang có trên hệ thống lưu trữ; Dò quét và đăng ký/đánh dấu dữ liệu cần phòng chống thất thoát; Dò quét, định danh các dữ liệu quan trọng/nhạy cảm và thực hiện các thao tác như sao chép, di chuyển nếu dữ liệu nhạy cảm được lưu trữ ở nơi không an toàn.
TEC.32	Tự động tạo dấu hiệu nhận biết dữ liệu	Giải pháp có khả năng tự động tạo dấu hiệu nhận biết đối với dữ liệu cần phòng chống thất thoát dựa theo nội dung của file dữ liệu, vị trí lưu trữ của dữ liệu.
TEC.33	Tùy biến tìm kiếm dữ liệu	- Giải pháp có sẵn tính năng cho phép tìm kiếm và xem tất cả các dữ liệu đã được dò quét thông qua giao diện web trực quan. - Cho phép lựa chọn đăng ký các folder dữ liệu quan trọng sẽ được bảo vệ bởi DLP discover hoặc có thể thiết lập chính sách, cảnh báo hoặc thực thi copy/move dữ liệu sang vị trí an toàn.

f. Yêu cầu kỹ thuật cho giải pháp phòng chống thất thoát dữ liệu cho Cloud

STT	Hạng mục	Yêu cầu
TEC.34	Phòng chống thất thoát dữ liệu cho O365	- Tích hợp với hạ tầng Cloud của khách hàng (O365) giúp giám sát, phát hiện và ngăn chặn các hành vi truyền gửi / chia sẻ dữ liệu từ môi trường cloud ra bên ngoài qua kênh Email (Exchange Online). - Giám sát hành vi người dùng, phát hiện các trường hợp thỏa hiệp: giám sát liên tục mọi hành vi của người dùng tương tác trên hạ tầng Cloud, sử dụng công nghệ machine learning để định danh, phát hiện các trường hợp: Insider Threats (Người dùng xấu thực hiện các hành vi bất thường), compromised account (các tài khoản bị thỏa hiệp, đánh cắp), và các hành vi bất thường của người dùng đặc quyền trên hạ tầng cloud. - Giám sát, kiểm soát việc lưu trữ dữ liệu trên Cloud: thực hiện giám sát, phát hiện và thực thi xử lý đối với các trường hợp người dùng vô tình/ cố tình tạo ra, upload các dữ liệu quan trọng của tổ chức lên môi trường lưu trữ cloud (One Drive, Sharepoint) vi phạm chính sách của PVcomBank. - Giám sát, kiểm soát việc chia sẻ và tương tác dữ liệu qua môi trường Cloud: + Phát hiện và loại bỏ (revoke) các quyền truy cập vào link tài liệu (được chia sẻ/forward ra bên ngoài theo link). + Phát hiện và ngăn chặn chia sẻ dữ liệu với tài khoản email cá nhân. + Loại bỏ các quyền truy cập của người dùng bên ngoài đối với các dữ liệu quan trọng đang được lưu trữ trên Cloud storage.
TEC.35	Rà quét và hậu kiểm đối với môi trường AWS S3	- Đánh giá và giám sát cho dịch vụ AWS S3 gần như theo thời gian thực (near realtime) khi có các file/dữ liệu được cập nhật/bổ sung trong AWS S3. Phát hiện các trường hợp dữ liệu quan trọng được lưu trữ trên AWS S3 vi phạm chính sách của tổ chức, đồng thời thực hiện các hành vi xử lý (quarantine/ remediation) theo chính sách tổ chức thiết lập.

g. Yêu cầu kỹ thuật cho giải pháp phân loại và gán nhãn dữ liệu

STT	Hạng mục	Yêu cầu
TEC.36	Khả năng phân loại và gán nhãn	- Giải pháp phải cho phép người dùng thực hiện phân loại và gán nhãn dữ liệu trên giao diện các ứng dụng bao gồm tối thiểu MS Office để thực hiện phân loại và gán nhãn dữ liệu. - Giải pháp cho phép phân loại và gán nhãn cho thư mục (folder), tệp (file), thư điện tử (email). - Giải pháp cho phép cài đặt tham số để phân loại và gán nhãn dữ liệu theo các nhóm theo yêu cầu của PVcomBank trong từng thời kỳ, tối thiểu 03 nhóm (Mật, Nội bộ, Công khai) để áp dụng các chính sách phòng chống thất thoát dữ liệu phù hợp.
TEC.37	Chính sách kiểm soát việc gán nhãn dữ liệu	- Giải pháp có thể thực hiện chính sách bắt buộc người dùng phải thực hiện phân loại và gán nhãn cho file trước khi lưu (save) và cho email/message trước khi gửi đi. - Giải pháp cho phép phát hiện và cảnh báo, ngăn chặn trong các trường hợp người dùng phân loại sai/phân loại chưa đúng với nội dung của tài liệu như: nâng cấp (upgrade)/hạ cấp (downgrade) cấp độ quan trọng (nhãn) của tài liệu đã được gán nhãn; phân loại và gán nhãn dữ liệu ở cấp độ thấp hơn mức yêu cầu đối với dữ liệu mới khởi tạo. Yêu cầu bắt buộc người dùng phải lựa chọn nhãn và phân loại phù hợp với nội dung của dữ liệu (không được phân loại thấp hơn mức tối thiểu quy định và không được phân loại thấp hơn nội dung của tài liệu được nhận diện).
TEC.38	Hỗ trợ chính sách mặc định	Giải pháp hỗ trợ các chính sách nhãn mặc định (default label), nhãn khuyến cáo (suggestion label)… giúp đơn giản hóa việc gán nhãn cho người dùng.
TEC.39	Cung cấp các hình thức phân loại và gán nhãn khác nhau	- Giải pháp cho phép thực thi tác vụ phân loại dữ liệu và gán nhãn thông qua câu lệnh hoặc tập các câu lệnh giúp tự động hóa việc phân loại và gán nhãn trên lượng lớn file/dữ liệu. - Giải pháp cho phép gán nhãn dữ liệu tương ứng với kết quả phân loại dữ liệu trên cơ sở tự động nhận diện dữ liệu hoặc theo kết quả phân loại dữ liệu thủ công của người dùng. Dữ liệu được gán nhãn trên chính file tài liệu (header/footer/watermark) hoặc trong metadata của dữ liệu. - Giải pháp cho phép tự động phân loại và gán nhãn dữ liệu theo quy tắc tùy chỉnh hoặc phân loại và gán nhãn dữ liệu theo lựa chọn của người dùng.

4. Yêu cầu về hiệu năng

STT	Hạng mục	Yêu cầu
TEC.40	Yêu cầu về hiệu năng hiện tại	Nhà thầu phải đề xuất sizing hạ tầng, thiết bị cần thiết để đảm bảo triển khai DLP giám sát cho toàn bộ người dùng đồng thời, khối lượng dữ liệu xử lý tại giai đoạn thử nghiệm, cụ thể: - Giải pháp phòng chống thất thoát dữ liệu cho Network: cho 1000 user - Giải pháp phòng chống thất thoát dữ liệu cho Endpoint: cho 1000 user - Mã hóa máy trạm: 100 thiết bị - Giải pháp Gán nhãn: cho 1000 user - Giải pháp Discover: cho 250 máy chủ - Giải pháp phòng chống thất thoát dữ liệu cho Cloud bao gồm tối thiểu: + Giải pháp phòng chống thất thoát dữ liệu cho Office 365: cho 1000 user. + Giải pháp phòng chống thất thoát dữ liệu cho AWS S3: AWS S3 với dung lượng 5TB, 40 nguồn dịch vụ.
TEC.41	Yêu cầu về hiệu năng mở rộng	Nhà thầu phải đề xuất giải pháp, sizing đáp ứng nhu cầu tăng trưởng của PVcomBank trong 05 năm tới mà không phải thay đổi thiết kế hay phải thay thế thiết bị/giải pháp hiện tại. Cụ thể: - Giải pháp đáp ứng được hiệu năng trong trường hợp mở rộng license trong tương lai: + Đáp ứng cho 5500 user hiện tại, tốc độ tăng trưởng số lượng người dùng hàng năm tối thiểu: 10%. + Băng thông truy cập internet hiện tại 528Mbps, tốc độ phát triển dữ liệu trung bình hàng năm tối thiểu: 20%. - Dễ dàng mở rộng năng lực của giải pháp theo bề ngang: Bổ sung dễ dàng các thiết bị/thành phần vào các cụm HA/Cluster mà không cần phải thay thế thiết bị/thành phần đang có.

5. Yêu cầu về hạ tầng và vận hành

STT	Hạng mục	Yêu cầu
TEC.42	Yêu cầu về tính	- Hệ điều hành máy trạm:

STT	Hạng mục	Yêu cầu
	năng tương thích với máy trạm của người sử dụng	+ Windows 10, Windows 11 Enterprise and Professional (32/64 bit). + Apple Mac OS X (11.0 hoặc cao hơn). - Trình duyệt cho máy trạm: Edge, FireFox, Google Chrome từ phiên bản đang sử dụng phổ biến tại thời điểm mở thầu trở lên.
TEC.43	Tính năng tương thích với máy chủ	Hệ điều hành máy chủ bao gồm tối thiểu: - Windows Server 2012 R2 - Windows Server 2016 - Windows Server 2019 - Windows Server 2022
TEC.44	Yêu cầu về tính sẵn sàng	Giải pháp phải có kiến trúc sẵn sàng cao HA (Active-Active/Active-Standby) hoặc theo cụm Cluster nhiều node cho các thành phần như sau, đảm bảo khi một node lỗi, các tính năng của giải pháp vẫn hoạt động liên tục và đáp ứng yêu cầu về năng lực: - Đảm bảo tính sẵn sàng (HA) cho các thành phần DLP mức mạng (web, email). - Đảm bảo tính sẵn sàng (HA) cho thành phần quản trị.
TEC.45	Yêu cầu về cấu hình hệ thống	Giải pháp phải đưa ra cấu hình hệ thống đáp ứng yêu cầu về hiệu năng ở TEC 40 và TEC 41 (bao gồm cho hiện tại và sẵn sàng cho mở rộng).

6. Yêu cầu an toàn thông tin

STT	Hạng mục	Yêu cầu
TEC.46	Yêu cầu về xác thực và phân quyền người dùng	Yêu cầu về xác thực và phân quyền người dùng: - Tích hợp với hệ thống quản lý đăng nhập hiện tại của PVcomBank bao gồm: + IBM CIAM cho tài khoản khách hàng. + Entra ID với giao thức SAML 2.0 hoặc OIDC với tài khoản quản trị và nghiệp vụ. - Trường hợp giải pháp có tài khoản local thì phải có khả năng kiểm tra độ phức tạp của mật khẩu theo đúng chính sách An ninh thông tin. Tên tài khoản và mật khẩu phải phù hợp các quy định hiện hành của PVcomBank: + Độ dài mật khẩu: từ 08 (tám) ký tự trở lên. + Cấu tạo từ các ký tự số, chữ hoa, chữ thường và các ký tự đặc biệt. - Hệ thống cho phép cài đặt chính sách mật khẩu người dùng local như sau: + Yêu cầu thay đổi mật khẩu lần đầu đăng nhập. + Yêu cầu thay đổi mật khẩu sau khoảng thời gian được cài đặt bằng tham số và có thông báo người sử dụng thay đổi mật khẩu sắp hết hạn sử dụng. + Hủy hiệu lực của mật khẩu hết hạn sử dụng. - Quyền/các nhóm quyền của người dùng trên ứng dụng phải được xác định rõ ràng. Quyền/nhóm quyền chỉ rõ người dùng được truy cập đến các chức năng và tài nguyên cụ thể. - Đối với ứng dụng Web, ứng dụng Client - Server, chức năng xác thực phải được thực hiện ở phía máy chủ. - Tên truy cập người dùng (User - IDs) phải là duy nhất, tránh sự trùng lặp tên truy cập.
TEC.47	Quản lý phiên làm việc	Quản lý phiên làm việc (Session Management): - Session phải được hủy bỏ ngay sau khi người dùng sử dụng chức năng logout để đăng xuất ra khỏi ứng dụng. - Session phải được tự động ngắt (time-out) sau một khoảng thời gian không sử dụng (inactivity). Khoảng thời gian này có thể thiết lập được theo tham số.

STT	Hạng mục	Yêu cầu
		- Mỗi khi đăng nhập thành công, một session mới được tạo ra và gắn với người dùng hợp lệ.
TEC.48	Sử dụng mã hóa an toàn	Sử dụng mã hóa an toàn (Cryptography): - Tất cả kết nối truyền dữ liệu đều phải hỗ trợ mã hóa đảm bảo an toàn, dữ liệu nhạy cảm hoặc bí mật (thông tin mật khẩu, số PIN, dữ liệu giao dịch tài chính, mã số thẻ…) phải được mã hóa/che giấu trong quá trình truyền và lưu trữ. Đảm bảo tất cả các truy cập quản trị phải được mã hóa bằng thuật toán mã hóa mạnh, tối thiểu: AES256, TDES/TDEA, RSA 2048, ECC224, DSA/D-H2048/224 hoặc tương đương. - Mật khẩu phải được mã hóa 1 chiều (hashing).
TEC.49	Kiểm soát lỗi và ghi nhật ký hoạt động của giải pháp	Kiểm soát lỗi và ghi nhật ký hoạt động của các thành phần trong giải pháp: - Các sự kiện liên quan đến bảo mật cũng phải được ghi chép lại trong logs bao gồm tối thiểu (đăng nhập không thành công, truy cập đến các tài nguyên không hợp lệ (access denied)). - Các events trong log phải chứa đầy đủ thông tin cần thiết để phục vụ truy vết về sau bao gồm tối thiểu: địa chỉ IP (nguồn/đích), users, tài nguyên truy cập, kết quả hành vi (success, failure). - Chức năng xem logs của ứng dụng chỉ thực hiện hiển thị nội dung events, không được thực thi các nội dung chứa trong events. - Dữ liệu nhật ký của ứng dụng (logs ứng dụng) phải được bảo vệ, chống truy cập và sửa đổi trái phép bởi người dùng thông thường (chỉ có người quản trị mới có quyền tiếp cận dữ liệu logs của ứng dụng tuy nhiên không thể sửa đổi thông tin). - Ứng dụng có khả năng tích hợp với một hệ thống lưu logs tập trung của bên thứ ba bao gồm tối thiểu như ELK, Splunk, SIEM.
TEC.50	Bảo mật đường truyền	Bảo mật đường truyền: - Sử dụng https (mã hóa đường truyền) cho tất cả các thông tin gửi nhận giữa client và server, giữa client và APIs. Sử dụng giao thức TLS v1.2 trở lên.
TEC.51	Bảo mật cấu hình	Bảo mật cấu hình: - User để kết nối các thành phần ứng dụng, ví dụ giữa database và application chỉ được thiết lập các quyền hạn chế đủ để thực hiện chức năng cần thiết, không sử dụng user quyền cao nhất.

7. Yêu cầu tích hợp

STT	Hạng mục	Yêu cầu
TEC.52	Khả năng tích hợp với các hệ thống network tại PVcomBank	Giải pháp DLP Network phải tích hợp được với các giải pháp network hiện tại bao gồm: - Giải pháp có thể tích hợp với hệ thống Web Proxy của PVcomBank để phòng chống thất thoát dữ liệu cho luồng truy cập web tại cổng kết nối Internet của PVcomBank, hỗ trợ giám sát và chống thất thoát đồng thời cho giao thức HTTP và HTTPs. - Giải pháp có thể tích hợp với hệ thống Email Gateway của PVcomBank để phòng chống thất thoát dữ liệu cho luồng truyền gửi email tại cổng kết nối Internet của PVcomBank.
TEC.53	Khả năng tích hợp với các hệ thống giám sát	- Tích hợp với các giải pháp tổ chức hiện có như SIEM (IBM Qradar), NOC (ManageEngine).

8. Các yêu cầu về triển khai

a. Yêu cầu khảo sát và phân loại dữ liệu

STT	Hạng mục	Yêu cầu
TEC.54	Khảo sát thực trạng bao gồm các quy trình, quy định bảo mật dữ liệu trong việc kiểm soát phòng chống thất thoát dữ liệu tại PVcomBank	- Tìm hiểu và phân tích hiện trạng về việc kiểm soát phòng chống thất thoát dữ liệu tại PVcomBank trên các khía cạnh con người, công nghệ và quy trình; - Thực hiện đánh giá khả năng đáp ứng của PVcomBank & so sánh với các thông tư, quy định hiện tại trên thị trường Việt Nam, bao gồm nhưng không giới hạn các quy định tại Việt Nam và các thông lệ quốc tế sau: + Thông tư 09/2020/TT-NHNN quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng hoặc văn bản sửa đổi, bổ sung, thay thế trong từng thời kỳ (nếu có); + Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân hoặc văn bản sửa đổi, bổ sung, thay thế trong từng thời kỳ (nếu có); + Luật dữ liệu hoặc văn bản sửa đổi, bổ sung, thay thế trong từng thời kỳ (nếu có);

STT	Hạng mục	Yêu cầu
		+ Nghị định 53/2022/NĐ-CP quy định chi tiết một số điều của Luật An ninh mạng hoặc văn bản sửa đổi, bổ sung, thay thế trong từng thời kỳ (nếu có); + Nghị định 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ hoặc văn bản sửa đổi, bổ sung, thay thế trong từng thời kỳ (nếu có); + Nghị định 117/2018/NĐ-CP quy định về việc giữ bí mật, cung cấp thông tin khách hàng của tổ chức tín dụng, chi nhánh ngân hàng nước ngoài hoặc văn bản sửa đổi, bổ sung, thay thế trong từng thời kỳ (nếu có); + ISO27001 & 27002 hoặc văn bản sửa đổi, bổ sung, thay thế trong từng thời kỳ (nếu có). - Đánh giá GAP và đưa ra khuyến nghị, phân tích các mối đe dọa, lỗ hổng, và điểm yếu dựa trên kết quả khảo sát hiện trạng năng lực đáp ứng của PVcomBank về phòng chống thất thoát dữ liệu.
TEC.55	Đề xuất lộ trình triển khai hoạt động chống thất thoát dữ liệu	- Xác định các mục tiêu bảo mật dữ liệu, yêu cầu của giải pháp DLP; - Xây dựng quy trình nhận diện dữ liệu: bao gồm tối thiểu các bước sau: + Xác định Mục tiêu: đáp ứng các yêu cầu tuân thủ và bảo mật dữ liệu; + Xác định phạm vi: Định nghĩa phạm vi của các thủ tục nhận diện dữ liệu, bao gồm các loại dữ liệu, các hệ thống và các phòng ban liên quan; + Xác định các nhóm dữ liệu: Phân loại dữ liệu thành các nhóm dựa trên các tiêu chí như mức độ nhạy cảm, giá trị kinh doanh, và mức độ sử dụng; + Đánh Giá Rủi Ro: Đánh giá rủi ro liên quan đến từng loại dữ liệu để xác định các biện pháp bảo vệ cần thiết; + Xác định phương pháp tiếp cận, các phương thức và kỹ thuật sẽ được sử dụng để nhận diện dữ liệu như công cụ quét tự động, kỹ thuật nhận diện thủ công;

STT	Hạng mục	Yêu cầu
		+ Thiết Kế Quy Trình Nhận Diện Dữ Liệu: Xây dựng quy định đặt tên và định danh dữ liệu để dễ dàng nhận diện và truy xuất. - Xây dựng Bộ quy định, quy trình nội bộ về phòng chống thất thoát dữ liệu tại Ngân hàng, gồm (*): + Ma trận chính sách DLP; + Quy định về phân loại dữ liệu; + Quy định về bảo vệ/phòng chống thất thoát dữ liệu; + Quy trình về phân loại và gán nhãn dữ liệu; + Quy trình về cung cấp thông tin, dữ liệu ra bên ngoài Ngân hàng; + Quy trình quản lý sự cố DLP. Trong đó lưu ý các yếu tố: + Phân Phối Tài Liệu: Đảm bảo tất cả các bên liên quan đều có quyền truy cập và hiểu các quy định, quy trình này; + Theo Dõi Thay Đổi: Theo dõi các thay đổi về dữ liệu, hệ thống và quy định để cập nhật quy trình nhận diện dữ liệu kịp thời; + Quản Lý Phiên Bản: Duy trì quản lý phiên bản của tài liệu và quy trình để đảm bảo sự nhất quán và cập nhật. *(*) Lưu ý: Đối với mỗi quy định/quy trình cần liệt kê đầu mục các nội dung bao gồm trong hồ sơ đề xuất kỹ thuật khi tham gia chào hàng.*
TEC.56	Nhận diện và phân loại dữ liệu	Triển khai nhận diện và phân loại dữ liệu cần thực hiện tối thiểu theo các bước sau: - Lập Kế Hoạch Chi Tiết + Phạm vi bao gồm 05 khối với 20 loại dữ liệu bao gồm: Khối QTNNL, Khối TCKT, Khối CNTT, Khối QTRR, Khối KHCN, (Danh sách 20 loại dữ liệu tại mục 1.III); + Thiết lập đội dữ liệu liên phòng bao gồm đại diện từ mỗi khối; + Thiết lập công cụ hỗ trợ và chuẩn bị biểu mẫu thủ công;

STT	Hạng mục	Yêu cầu
		+ Phương thức thực hiện: Tổ chức các cuộc họp với đại diện của các khối, phòng ban, và chi nhánh về phương thức thực hiện, cách thức trao đổi giữa các bên. - Kiểm Kê Dữ Liệu: + Thực hiện kiểm kê dữ liệu hiện có trong mỗi khối; + Sử dụng các công cụ tự động để quét cùng các cách thức thủ công để lập danh sách dữ liệu, bao gồm dữ liệu cấu trúc và phi cấu trúc; + Đối chiếu và hiệu chỉnh kết quả giữa thủ công và tự động. - Phân Loại và Đánh Giá Dữ Liệu: + Áp dụng các tiêu chí để phân loại dữ liệu trong từng khối; + Sử dụng công cụ phần mềm để hỗ trợ việc phân loại tự động nếu có thể. - Tổng hợp, lập danh mục dữ liệu và báo cáo: + Lập danh mục dữ liệu; + Lập danh sách dữ liệu nhạy cảm và biện pháp bảo vệ tương ứng; + Lập báo cáo kiểm kê, phân loại dữ liệu, nhận diện rủi ro, và khuyến nghị các hoạt động bảo vệ dữ liệu.

b. Yêu cầu chi tiết về triển khai

STT	Hạng mục	Yêu cầu
TEC.57	Phương pháp triển khai	- Nhà thầu có trách nhiệm đảm bảo tính sẵn sàng của toàn bộ giải pháp trước khi tiến hành triển khai chính thức, bao gồm cả việc giải pháp phải được cập nhật lên phiên bản ổn định, an toàn bảo mật nhất theo khuyến nghị của hãng cung cấp. - Nhà thầu đề xuất và mô tả phương pháp, kế hoạch và kịch bản triển khai chính thức trong đó nêu rõ các phương án dự phòng cần thiết để đảm bảo hoạt động của PVcomBank không bị gián đoạn vì bất kỳ lý do gì. Kịch bản triển khai chính thức phải được PVcomBank xác nhận trước khi thực hiện. - Nhà thầu phải đảm bảo không còn bất cứ lỗi nghiêm trọng nào ảnh hưởng đến hoạt động của PVcomBank được ghi nhận trên

STT	Hạng mục	Yêu cầu
		hệ thống ở trạng thái mở hay đang xử lý và được PVcomBank chấp thuận trước khi tiến hành triển khai thử nghiệm. - Nhà thầu phải giải trình, thông báo kế hoạch khắc phục nếu có lỗi được ghi nhận trong quá trình triển khai và chỉ được phép tiếp tục triển khai nếu có sự đồng ý từ PVcomBank. - Nhà thầu có trách nhiệm bố trí nhân lực (bao gồm cả nhân lực onsite và offsite) đầy đủ và phù hợp để xử lý kịp thời lỗi phát sinh trong quá trình triển khai chính thức.
TEC.58	Kế hoạch kiểm thử	- Nhà thầu đề xuất và mô tả chiến lược, kế hoạch kiểm thử giải pháp một cách toàn diện bao gồm: + Kiểm thử tích hợp giải pháp (SIT); + Kiểm thử người dùng chấp nhận giải pháp (UAT); + Kiểm thử hiệu năng giải pháp (PT); + Kiểm thử bảo mật (ST). - Nhà thầu có trách nhiệm xây dựng tất cả các kịch bản kiểm thử và hoàn thiện kịch bản kiểm thử dựa trên ý kiến đóng góp của PVcomBank và phải được PVcomBank chấp nhận trước khi chính thức tiến hành kiểm thử. - Nhà thầu phải cung cấp công cụ phục vụ cho mục đích kiểm thử. - Nhà thầu chịu trách nhiệm quản lý, báo cáo kết quả kiểm thử đối với tất cả các loại hình kiểm thử, xử lý sửa lỗi trong tất cả các môi trường kiểm thử và giải quyết vấn đề xảy ra trong giai đoạn kiểm thử theo như cam kết dịch vụ. - Nhà thầu phải cung cấp các biểu mẫu bao gồm tối thiểu như tình huống kiểm thử, trường hợp kiểm thử, kịch bản kiểm thử đã được sử dụng trong những dự án gần đây. - Nhà thầu có trách nhiệm huy động đầy đủ nguồn lực để xử lý dứt điểm tất cả các lỗi phát sinh trong quá trình thực hiện kiểm thử một cách nhanh nhất để đảm bảo kế hoạch dự án mà hai bên đã thống nhất.
TEC.59	Truyền thông và Tổ chức đào tạo	1. Thực hiện truyền thông bao gồm - Lập kế hoạch truyền thông: + Xác định đối tượng: Xác định các bên liên quan cần được thông báo (nhóm dự án, nhân sự các đơn vị); + Xác định thông tin cần truyền tải: Biên soạn tài liệu truyền thông về nhận thức bảo vệ tài sản thông tin, chống thất thoát

STT	Hạng mục	Yêu cầu
		dữ liệu; các thông tin về tiến độ dự án, thay đổi phạm vi, rủi ro trong quá trình thực hiện dự án, truyền thông nhận thức; + Kênh truyền thông: Lựa chọn đa dạng các kênh phù hợp để truyền tải thông tin (email, họp mặt, báo cáo, nền tảng trực tuyến, v.v.); + Tần suất truyền thông: Quyết định tần suất truyền thông (hàng ngày, hàng tuần, hàng tháng). - Thực hiện truyền thông: + Họp dự án: Tổ chức các cuộc họp định kỳ để cập nhật tình hình dự án và thảo luận về các vấn đề cần giải quyết; + Báo cáo tiến độ: Cung cấp báo cáo tiến độ định kỳ để cập nhật trạng thái dự án cho các bên liên quan; + Thông báo thay đổi: Thông báo kịp thời về các thay đổi quan trọng trong dự án, bao gồm thay đổi về phạm vi, lịch trình. - Quản lý phản hồi: + Thu thập phản hồi: Thu thập phản hồi từ các bên liên quan qua các kênh khác nhau (cuộc họp, khảo sát, email); + Phản hồi lại: Đáp ứng phản hồi và giải quyết các vấn đề kịp thời. 2. Yêu cầu về đào tạo - Xác định nhu cầu đào tạo: + Đánh giá kỹ năng hiện tại: Đánh giá kỹ năng và kiến thức hiện tại của đội ngũ dự án; + Xác định khoảng cách kỹ năng: Xác định các kỹ năng và kiến thức còn thiếu so với yêu cầu của dự án; + Dự định 08 buổi đào tạo tại PVcomBank trong đó: 05 buổi đào tạo nhận thức cho toàn bộ cán bộ nhân viên của 05 khối, 02 buổi đào tạo cho đầu mối các khối về việc thực hiện nhận diện, phân loại dữ liệu, 01 buổi đào tạo cho nhân viên quản trị và vận hành hệ thống. - Lập kế hoạch đào tạo: + Mục tiêu đào tạo: Xác định mục tiêu cụ thể của chương trình đào tạo; + Nội dung đào tạo: Xác định các chủ đề và nội dung cần đào tạo (kỹ thuật, quy trình, công cụ); + Phương pháp đào tạo: Chọn phương pháp đào tạo phù hợp (hội thảo, lớp học, đào tạo trực tuyến, hướng dẫn trực tiếp);

STT	Hạng mục	Yêu cầu
		+ Lịch trình đào tạo: Lên lịch trình chi tiết cho các buổi đào tạo. - Thực hiện đào tạo: + Triển khai các buổi đào tạo: Thực hiện các buổi đào tạo theo kế hoạch; + Tài liệu đào tạo: Cung cấp tài liệu hỗ trợ (hướng dẫn, slide, tài liệu tham khảo) như: tài liệu nâng cao về nhận thức chuyên sâu cho quản trị viên và nhân viên liên quan đến DLP, đặt nền tảng để triển khai lâu dài về nhận thức về quyền riêng tư và bảo vệ dữ liệu cho PVcomBank; đào tạo quy định, quy trình và ứng dụng cụ thể của DLP cho tất cả người dùng hệ thống DLP; đào tạo thực hiện nhận diện dữ liệu, phân loại dữ liệu. - Đánh giá hiệu quả đào tạo: + Kiểm tra sau đào tạo: Thực hiện kiểm tra để đánh giá mức độ tiếp thu kiến thức và kỹ năng; + Thu thập phản hồi: Lấy phản hồi từ người tham gia đào tạo để cải thiện chương trình đào tạo; + Điều chỉnh và cải tiến: Dựa vào phản hồi và kết quả kiểm tra, điều chỉnh chương trình đào tạo nếu cần thiết. - Tích hợp truyền thông và đào tạo: + Lập kế hoạch phối hợp: Đảm bảo kế hoạch truyền thông và đào tạo được tích hợp và phối hợp chặt chẽ; + Sử dụng nền tảng chung: Sử dụng các nền tảng công nghệ chung để hỗ trợ cả truyền thông và đào tạo (ví dụ: nền tảng quản lý học tập, công cụ họp trực tuyến); + Cập nhật thường xuyên: Cập nhật liên tục về tiến độ và thay đổi trong kế hoạch đào tạo thông qua các kênh truyền thông đã chọn.
TEC.60	Lộ trình triển khai giải pháp chống thất thoát dữ liệu	- Báo cáo khảo sát thực trạng môi trường hệ thống công nghệ thông tin trong kiểm soát phòng chống thất thoát dữ liệu (DLP) tại PVcomBank; - Báo cáo đề xuất lộ trình triển khai và sáng kiến chiến lược hành động; - Báo cáo tiến độ dự án định kỳ/đột xuất; - Mô hình hoạt động DLP: bao gồm các vai trò và trách nhiệm được xác định, phù hợp với mức độ trưởng thành của DLP;

STT	Hạng mục	Yêu cầu
		- Chính sách và thủ tục DLP; - Khung phân loại dữ liệu; - Danh sách năng lực kỹ thuật: Danh sách các yêu cầu về năng lực kỹ thuật cùng các yêu cầu bảo mật; - Bảng điểm đánh giá công cụ DLP; - Báo cáo tiêu chí lựa chọn nhà cung cấp giải pháp công nghệ; - Tiêu chí đánh giá quá trình triển khai giải pháp đảm bảo Tuân thủ các yêu cầu kỹ thuật, đúng tiến độ; - Báo cáo giám sát chất lượng và tiến độ triển khai định kỳ.
TEC.61	Tài liệu chuyển giao	Bao gồm nhưng không giới hạn: - Kế hoạch truyền thông - Tài liệu đào tạo và nâng cao nhận thức về DLP (Mức cơ bản): Tài liệu nâng cao nhận thức về bảo vệ dữ liệu cho toàn bộ Tổ chức. - Tài liệu đào tạo & nâng cao nhận thức về DLP (Mức chuyên sâu): Tài liệu nâng cao nhận thức về bảo vệ dữ liệu cho quản trị viên DLP và những nhân viên có liên quan nhiều đến kỹ thuật giải pháp DLP. - Toàn bộ các tài liệu bảng biểu, bảng hỏi, phương pháp/cách thức đánh giá liên quan đến báo cáo phân tích về mặt kỹ thuật của nhà cung cấp để ra được kết quả đánh giá thực trạng.

c. Yêu cầu về Bản quyền, bảo hành, bảo trì và hỗ trợ kỹ thuật

STT	Hạng mục	Yêu cầu
TEC.62	Yêu cầu về bản quyền	- Tất cả các phần mềm của bên thứ 3 được nhà thầu sử dụng cho giải pháp DLP phải có bản quyền hợp lệ. Nhà thầu phải cung cấp danh sách các phần mềm của bên thứ 3 được sử dụng trong giải pháp và giấy phép sử dụng các phần mềm đó. - Giải pháp cần cung cấp bản quyền (License) như sau: + Giải pháp phòng chống thất thoát dữ liệu cho Network: License bản quyền vĩnh viễn. + Giải pháp phòng chống thất thoát dữ liệu cho Endpoint: License bản quyền vĩnh viễn. + Mã hoá máy trạm: License bản quyền vĩnh viễn. + Giải pháp Gán nhãn: License bản quyền tối thiểu 12 tháng kể từ ngày nghiệm thu tổng thể và đưa vào sử dụng.

STT	Hạng mục	Yêu cầu
		+ Giải pháp Discover: License bản quyền tối thiểu 12 tháng kể từ ngày nghiệm thu tổng thể và đưa vào sử dụng. + Giải pháp phòng chống thất thoát dữ liệu cho Cloud: License bản quyền tối thiểu 12 tháng kể từ ngày nghiệm thu tổng thể và đưa vào sử dụng. - Yêu cầu cung cấp cơ sở tính giá và chi phí bảo trì sau triển khai trong vòng (04) năm sau thời gian bảo hành.
TEC.63	Bảo trì giải pháp DLP	Nhà thầu cam kết cung cấp dịch vụ bảo trì phần cứng/phần mềm của giải pháp DLP khi PVcomBank có yêu cầu như sau. Thời gian cung cấp dịch vụ: Tối thiểu 12 tháng kể từ ngày nghiệm thu tổng thể và đưa vào sử dụng. Phạm vi cung cấp: - Cung cấp dịch vụ hỗ trợ kỹ thuật; - Cung cấp truy cập bất kỳ lúc nào cần hỗ trợ kỹ thuật; - Cung cấp cập nhật và sửa chữa sản phẩm (Phần mềm, hệ thống, bản quyền/nếu có); - Cung cấp các cảnh báo bảo mật, cập nhật và vá lỗi khẩn cấp cũng như các công cụ/tiện ích cập nhật (nếu có). Thời gian đáp ứng: - Thời gian yêu cầu hỗ trợ: 24 giờ trong ngày, 7 ngày trong tuần; - Thời gian đáp ứng ban đầu: đối với loại lỗi 1&2 trong vòng 4 giờ làm việc; - Thời gian sửa lỗi xong: đối với lỗi loại 1 – trong vòng 24 giờ, đối với lỗi loại 2: trong vòng 48 giờ, đối với lỗi loại 3: sửa chữa trong vòng phiên bản nâng cấp tiếp theo; - Cung cấp ít nhất một kỹ sư hỗ trợ tại chỗ trong vòng 3 tháng sau ngày giải pháp đi vào hoạt động. Nhân viên hỗ trợ kỹ thuật phải giải quyết cho tất cả những thành phần hệ thống và nghiệp vụ của giải pháp cung cấp, bao gồm nhưng không giới hạn bởi cơ sở dữ liệu, ứng dụng, add-on, v.v. Mức độ nghiêm trọng được định nghĩa dưới đây: - Loại 1: là một trường hợp khẩn cấp trên hệ thống đang chạy khi hệ thống hoàn toàn không hoạt động hoặc gặp sự cố thảm khốc và không có giải pháp thay thế. - Loại 2: là một trường hợp bất lợi (không có giải pháp thay thế) khi (a) hiệu năng hệ thống suy giảm, (b) hệ thống vẫn sử dụng

STT	Hạng mục	Yêu cầu
		được nhưng giảm thiểu khả năng một cách trầm trọng; hoặc (c) một hay nhiều chức năng hoặc lệnh then chốt không còn tác dụng. - Loại 3: là trường hợp hệ thống vẫn sử dụng được, nhưng không cung cấp chức năng một cách thuận tiện.

III. Danh sách nhóm dữ liệu trong phạm vi triển khai

Mục 1: *(Theo nội dung yêu cầu tại Tec.56 của mục 1.II.8.a)*

	Nhóm dữ liệu	Mô tả
1	Dữ liệu cá nhân định danh được khách hàng, đối tác/bên thứ ba	Dữ liệu cá nhân theo định nghĩa tại Khoản 3, Khoản 4 Điều 2 Nghị định 13/2023/NĐ-CP Bảo vệ dữ liệu cá nhân.
2	Dữ liệu khách hàng	Nhóm dữ liệu các thông tin thu thập và phát sinh trong quá trình cung cấp sản phẩm dịch vụ cho khách hàng PVcomBank. Một số dữ liệu bao gồm thông tin tài khoản, sao kê, tiền gửi, tài sản gửi của khách hàng, hợp đồng, thông tin giao dịch của khách hàng, thông tin thẩm định khách hàng, thông tin nợ và xử lý nợ của khách hàng, thông tin khiếu nại tố cáo và giải quyết khiếu nại tố cáo của khách hàng, v.v.
3	Dữ liệu hoạt động kinh doanh	Nhóm dữ liệu liên quan đến các báo cáo tổng hợp và chi tiết liên quan đến tình hình hoạt động, kết quả hoạt động kinh doanh của các đơn vị và toàn hệ thống PVcomBank. Một số dữ liệu bao gồm báo cáo kết quả kinh doanh, báo cáo hoạt động, báo cáo quản trị nội bộ các đơn vị PVcomBank, báo cáo doanh thu, doanh số kinh doanh các sản phẩm dịch vụ của Ngân hàng, báo cáo đánh giá KPIs, v.v.
4	Thông tin về sản phẩm dịch vụ cung cấp cho khách hàng	Thông tin sản phẩm dịch vụ cung cấp cho khách hàng kể từ giai đoạn sáng kiến, phát triển/cập nhật/hoàn thiện, phê duyệt, công bố và cung cấp tới khách hàng.

	Nhóm dữ liệu	Mô tả
5	Dữ liệu vận hành	Các dữ liệu phát sinh trong quá trình tác nghiệp, vận hành hàng ngày các hoạt động nghiệp vụ của Ngân hàng, như tài liệu theo dõi, giám sát, phân tích, đánh giá tình hình kinh doanh, tình hình hoạt động, chất lượng dịch vụ của từng đơn vị hoặc từng nghiệp vụ của Ngân hàng, các báo cáo nội bộ hoặc phát sinh theo yêu cầu của Ban lãnh đạo Khối hoặc Ban lãnh đạo Ngân hàng, dữ liệu làm việc hoặc hỗ trợ công việc, dữ liệu hành chính, v.v.
6	Chiến lược và quy hoạch/kế hoạch/lộ trình hoạt động, phát triển	Nhóm dữ liệu liên quan đến các định hướng chiến lược, dự án chiến lược, khách hàng chiến lược và các thông tin chiến lược do Hội đồng quản trị và Ban điều hành chỉ đạo cũng như giám sát thực hiện. Một số dữ liệu bao gồm hồ sơ, tài liệu về chiến lược, đề án, quy hoạch, kế hoạch phát triển Ngân hàng ngắn/trung/dài hạn, kế hoạch phát triển Ngân hàng, kế hoạch hoạt động, kế hoạch ngân sách, kế hoạch kinh doanh của các đơn vị, và các dữ liệu báo cáo giám sát tình hình thực hiện chiến lược, kế hoạch.
7	Dữ liệu kế toán tài chính	Nhóm dữ liệu liên quan đến các hồ sơ sổ sách, số liệu, dữ liệu phát sinh trong các hoạt động ghi nhận doanh thu, chi phí, giám sát, báo cáo kết quả kế toán tài chính của Ngân hàng. Một số dữ liệu bao gồm các báo cáo tài chính, hồ sơ thanh toán, theo dõi ngân sách và chi tiêu, dữ liệu hạch toán, phân bổ chi phí nội bộ, dữ liệu theo dõi các chỉ số tài chính, dữ liệu chấm số liệu tài chính, v.v.
8	Chính sách quy định nội bộ	Bộ các tài liệu quy chế, quy trình, quy định, chính sách, hướng dẫn nghiệp vụ; tài liệu đặc tả, vận hành sản phẩm dịch vụ PVcomBank, được soạn thảo, ban hành, truyền thông/ đào tạo và sử dụng hàng ngày bởi các đơn vị cũng như các chi nhánh PVcomBank.
9	Dữ liệu kiểm tra, kiểm soát nội bộ	Nhóm dữ liệu liên quan đến công tác giám sát, kiểm tra, đánh giá tuân thủ các quy định pháp luật; tiêu chuẩn, chính sách, quy định nội bộ của toàn bộ Ngân hàng. Một số dữ liệu bao gồm các báo cáo giám sát, kiểm tra tuân thủ, hồ sơ tài liệu kiểm tra tuân thủ, hồ sơ, tài liệu khắc phục những khuyến nghị qua hoạt động giám sát kiểm tra, các văn bản, tờ trình, thông báo liên quan đến hoạt động kiểm soát nội bộ, v.v.

	Nhóm dữ liệu	Mô tả
10	Kết quả quản lý rủi ro	Nhóm dữ liệu liên quan đến các hoạt động quản lý rủi ro hoạt động và phòng chống rửa tiền, rủi ro tín dụng, rủi ro thị trường, rủi ro hệ thống, rủi ro công nghệ và kinh doanh liên tục của toàn hệ thống Ngân hàng. Một số dữ liệu bao gồm hồ sơ rủi ro, hồ sơ xử lý rủi ro, báo cáo tình hình rủi ro, báo cáo sự kiện rủi ro, báo cáo chuyên đề liên quan đến quản lý rủi ro, báo cáo tuân thủ về quản lý rủi ro, báo cáo quản trị nội bộ về quản lý rủi ro; công văn trao đổi về quản lý rủi ro, v.v.
11	Dữ liệu dự án	Nhóm dữ liệu phát sinh trong quá trình thực hiện các dự án, đề án của Ngân hàng. Một số dữ liệu bao gồm các hồ sơ dự án (tờ trình lập dự án, hồ sơ đấu thầu, hợp đồng với đối tác, báo cáo tiến độ, tài liệu kiểm thử, báo cáo nghiệm thu, v.v.), các dữ liệu thu thập và sử dụng trong quá trình thực hiện dự án, các sản phẩm chuyển giao của dự án.
12	Dữ liệu cá nhân định danh được cán bộ nhân viên	Dữ liệu cá nhân theo định nghĩa tại Khoản 3, 4 Điều 2 Nghị định 13/2023/NĐ-CP Bảo vệ dữ liệu cá nhân.
13	Dữ liệu nhân sự	Nhóm dữ liệu liên quan đến hoạt động tuyển dụng và quản lý nhân sự của PVcomBank. Một số dữ liệu bao gồm thông tin cá nhân của nhân viên PVcomBank, thông tin liên lạc, hồ sơ lý lịch, hồ sơ sức khỏe, thông tin lương thưởng, thông tin bảo hiểm, KPIs, năng suất lao động, đánh giá kết quả làm việc, thông tin luân chuyển bổ nhiệm, hồ sơ đào tạo, kế hoạch nguồn nhân lực, báo cáo quản trị nhân sự của Ngân hàng; v.v.
14	Thông tin hệ thống CNTT	Bao gồm tối thiểu các thông tin sau: - Thông tin hệ thống CNTT trong quá trình phát triển hệ thống thông tin: tài liệu đặc tả, tài liệu thiết kế, tài liệu kiểm thử. - Thông tin hệ thống CNTT trong quá trình quản trị hệ thống thông tin (dành cho admin): cài đặt, cấu hình, mô hình/thiết kế. - Thông tin hệ thống CNTT trong quá trình vận hành hệ thống thông tin (dành cho Admin). - Thông tin bảo mật hệ thống: Đánh giá/ quản lý điểm yếu, sự cố và xử lý sự cố ATTT, báo cáo pentest.

	Nhóm dữ liệu	Mô tả
15	Dữ liệu quy trình chính sách, tài liệu sản phẩm dịch vụ, tài liệu hệ thống	Bộ các tài liệu quy chế, quy trình, quy định, chính sách, hướng dẫn nghiệp vụ; tài liệu đặc tả, vận hành sản phẩm dịch vụ PVcomBank, được soạn thảo, ban hành, truyền thông/ đào tạo và sử dụng hàng ngày bởi các đơn vị cũng như các chi nhánh PVcomBank. Ngoài ra, dữ liệu còn bao gồm các tài liệu đặc tả, hướng dẫn quản trị, vận hành các hệ thống CNTT của Ngân hàng.
16	Dữ liệu trao đổi với các cơ quan chức năng, ban ngành đoàn thể	Nhóm dữ liệu liên quan đến các công văn đến, văn bản phản hồi, báo cáo định kỳ về hoạt động của Ngân hàng theo quy định hoặc đột xuất theo yêu cầu cho các cơ quan chức năng như Ngân hàng Nhà nước, Bộ Quốc phòng, Đảng ủy, v.v. Một số dữ liệu bao gồm báo cáo kinh doanh, báo cáo tài chính, báo cáo rủi ro, báo cáo theo các thông tư gửi cho Ngân hàng Nhà nước, các công văn nhận và báo cáo phản hồi cho các cơ quan, dữ liệu về công tác tuyên huấn và an sinh xã hội, công tác tổ chức xây dựng Đảng và công tác thanh niên, công tác cán bộ, quân đội, dân vận, v.v.
17	Dữ liệu thanh tra, điều tra, tố tụng	Nhóm dữ liệu liên quan đến các hồ sơ, tài liệu liên quan đến hoạt động thanh tra, vụ việc điều tra tố tụng, xử lý tranh chấp của Ngân hàng. Dữ liệu bao gồm hồ sơ thanh tra, và xử lý sau thanh tra hồ sơ điều tra tố tụng, tranh chấp, và xử lý sau điều tra tố tụng, tranh chấp, các công văn trả lời cá nhân và tập thể có đơn tố tụng, v.v.
18	Dữ liệu mua sắm, đầu tư và dự án	Nhóm dữ liệu phát sinh trong quá trình thực hiện các dự án, đề án của Ngân hàng. Một số dữ liệu bao gồm các hồ sơ dự án (tờ trình lập dự án, hồ sơ đấu thầu, hồ sơ chấm thầu, hợp đồng với đối tác, hồ sơ triển khai,, v.v.), các dữ liệu thu thập và sử dụng trong quá trình thực hiện dự án, các sản phẩm chuyển giao của dự án.
19	Dữ liệu đối tác, cổ đông	Nhóm dữ liệu liên quan đến thông tin liên hệ của các đối tác cung cấp sản phẩm dịch vụ cho Ngân hàng, các đối tác PVcomBank liên kết để cung cấp sản phẩm dịch vụ cho khách hàng, các cổ đông, các thông tin liên quan như hợp đồng, thông tin giao dịch, hồ sơ thanh toán, báo cáo định kỳ, v.v.

	Nhóm dữ liệu	Mô tả
20	Dữ liệu camera giám sát	Dữ liệu là các file video, hình ảnh giám sát tại hội sở, chi nhánh, phòng giao dịch, ATM.

IV. Địa điểm triển khai:

Triển khai tại Hội sở và các địa điểm do PVcombank chỉ định trên toàn quốc.

Hội sở PVcomBank, 22 Ngô Quyền, Cửa Nam, Hà Nội

Mục 2. Bản vẽ

E-HSMT này gồm có các bản vẽ trong danh mục sau đây*:* Không có .

Mục 3. Kiểm tra và thử nghiệm

Các kiểm tra và thử nghiệm cần tiến hành gồm có:

- Trong quá trình triển khai cần thử nghiệm tính tương thích đảm bảo tích hợp với các hệ thống hiện có của PVcomBank.
- Phải kiểm thử các tính năng hệ thống đáp ứng các yêu cầu tại Khoản II.2, II.3, Mục 1, Chương V – YÊU CẦI VỀ KỸ THUẬT.
- Kế hoạch kiểm thử phải đảm bảo đáp ứng yêu cầu nêu ra tại điểm b, Khoản II.8, Mục 1, Chương V – YÊU CẦI VỀ KỸ THUẬT.