ĐẠI HỌC Y DƯỢC TPHCM
BỆNH VIỆN ĐẠI HỌC Y DƯỢC

Số: 48../ BVĐHYD-CNTT
v/v mời chào giá

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Thành phố Hồ Chí Minh, ngày 6 tháng 1 năm 2021

Kính gửi: Quý nhà cung cấp

Bệnh viện Đại học Y Dược TP. Hồ Chí Minh kính mời các Quý đơn vị có quan tâm, có khả năng cung cấp bản quyền phần mềm quản lý tài khoản đặc quyền báo giá theo phụ lục đính kèm.

Kính đề nghị Quý nhà cung cấp gửi file word/excel và bản scan báo giá có đóng dấu theo mẫu đính kèm đến email moichaogia@umc.edu.vn và email congnghethongtin@umc.edu.vn. Gửi bản giấy có đóng dấu về Phòng Công nghệ thông tin, Bệnh viện Đại học Y Dược TPHCM, địa chỉ: 215 Hồng Bàng phường 11 quận 5, TP. Hồ Chí Minh.

- Hồ sơ gửi kèm theo báo giá bao gồm các tài liệu kỹ thuật của hàng hóa: Catalogue sản phẩm và các tài liệu kỹ thuật liên quan khác.
- Thời gian nhận báo giá: đến hết ngày 14./.1./2021.
- Điện thoại liên hệ: 028.39525391.

Trân trọng./.

Nơi nhận:
- Như trên;
- Đơn vị Quản lý đấu thầu (để đăng tin);
- Lưu: VT, CNTT (K18-248-ntmthi) (03)

KT. GIÁM ĐỐC

BỘ Y TẾ
BỆNH VIỆN ĐẠI HỌC Y DƯỢC TP. HỒ CHÍ MINH

Trương Quang Bình
Phó Giám đốc

PHỤ LỤC. DANH MỤC HÀNG HÓA MỜI CHÀO GIÁ

(Kèm theo thư mời chào giá số 48../TMCG-BVĐHYD ngày 6. tháng 1. năm 2021)

Tên hàng hóa: Phần mềm quản lý tài khoản đặc quyền
Đơn vị tính: Bản quyền
Số lượng: 01.

TT	Nội dung yêu cầu		Ghi chú
I	**Yêu cầu về kỹ thuật đáp ứng các yêu cầu về tính năng như sau:**		
1	**Tự động tìm tài khoản, bảo vệ và quản lý mật khẩu**		
1.1	Tìm tự động các tài khoản đặc quyền	Cho phép thực hiện tìm thấy tất cả các tài khoản đặc quyền quan trọng cũng như các tài khoản và thông tin đăng nhập trên toàn hệ thống mạng.	
1.2	Kho mật khẩu tập trung	Cho phép lưu trữ tất cả các mật khẩu của tổ chức, các tài khoản đặc quyền, các tài khoản đã chia sẻ,... một cách tập trung và an toàn	
1.3	Khóa kỹ thuật số, tài liệu và tài khoản web	Cho phép quản lý các chứng chỉ kỹ thuật số, khóa cấp phép, tài liệu và hình ảnh.	
2	**Cấp phép truy cập, kiểm soát & quản trị đặc quyền**		
2.1	Quyền sở hữu mật khẩu và chia sẻ chi tiết	Cho phép thiết lập quyền sở hữu mật khẩu cho các mật khẩu được lưu tập trung. Cung cấp khả năng chia sẻ mật khẩu mang tính chọn lọc dựa trên các yêu cầu	
2.2	Tích hợp máy chủ Active Directory / LDAP	Cho phép nhập Tài khoản cá nhân/Tài khoản nhóm (User/User Group) từ AD hoặc LDAP và cũng tận dụng cơ chế xác thực trên đó. Hỗ trợ các loại như: Novell eDirectory, Oracle OID, OpenLDAP và bất kỳ máy chủ LDAP nào khác	
2.3	Xác thực thông qua máy chủ RADIUS	Cho phép tích hợp với máy chủ RADIUS và tận dụng xác thực RADIUS để bỏ qua xác thực cục bộ do hệ thống quản trị mật khẩu cung cấp	
2.4	Xác thực thông qua Smart Card / PKI	Cung cấp tính năng Xác thực thẻ thông minh, giúp xác thực mạnh hơn để truy cập vào hệ thống quản trị mật khẩu đặc quyền	
2.5	Kiểm soát mật khẩu truy cập có quy trình	Cho phép kiểm soát các yêu cầu cấp/khôi phục mật khẩu và cấp quyền thông qua quy trình phê duyệt. Đồng thời cho phép giới hạn thời gian truy cập.	
3	**Đồng bộ hóa mật khẩu từ xa**		
3.1	Tự động đặt lại các mật khẩu	Cho phép đặt lại các mật khẩu từ xa bằng cách truy cập qua giao diện Web khi được yêu cầu hoặc tự động thông qua các yêu cầu được lên lịch sẵn	

TT	Nội dung yêu cầu		Ghi chú
3.2	Thực thi các chính sách về mật khẩu	Cho phép thiết lập các chính sách về mật khẩu, bảo đảm sử dụng mật khẩu mạnh và đặt lại theo định kì	
3.3	Hỗ trợ đa dạng các hệ điều hành, các thiết bị Công nghệ thông tin	Hỗ trợ đa dạng các hệ thống, cơ sở dữ liệu, các thiết bị mạng cho việc kiểm soát truy cập và tự động đặt lại mật khẩu	
3.4	Quản lý mật khẩu theo dạng Application-to-Application	Cho phép các ứng dụng bên ngoài kết nối bảo mật đến cổng API để sử dụng các mật khẩu đặc quyền	
3.5	Quản lý các tài khoản dịch vụ Microsoft Windows	Cho phép tự động xác định và đặt lại mật khẩu của các tài khoản dịch vụ Microsoft Windows được liên kết với các tài khoản domain	
3.6	Thực thi các đoạn lệnh script sau khi đặt lại mật khẩu	Cho phép thực thi các đoạn lệnh sau khi hành động đặt lại mật khẩu được thực hiện	
3.7	Đặt lại mật khẩu từ xa ở chế độ agent-less	Cho phép đặt lại mật khẩu ở một trong hai chế độ sau: agent hoặc agent-less. Để đặt lại mật khẩu ở chế độ agent-less, Hệ thống quản trị mật khẩu kết nối trực tiếp với hệ thống đích và thay đổi mật khẩu.	
4	**Quản lý phiên làm việc đặc quyền**		
4.1	Đăng nhập từ xa trực tiếp	Cho phép người dùng có thể khởi chạy các phiên SSH, Telnet, giả lập Windows RDP với mức độ bảo mật cao, đáng tin cậy từ trình duyệt mà không cần phải kết nối trực tiếp đến thiết bị hoặc bất kì phần mềm agent nào	
4.2	Ghi lại hoạt động của các phiên đặc quyền	Cho phép ghi lại video các phiên đặc quyền được khởi chạy từ hệ thống quản trị mật khẩu đặc quyền, được lưu trữ và xem lại phục vụ cho việc kiểm tra, truy vết tác động vào hệ thống.	
4.3	Tự động đăng nhập đến các hệ thống khác, các website	Cho phép tự động đăng nhập đến các hệ thống, các trang web và các ứng dụng trực tiếp từ giao diện web của hệ thống quản trị mật khẩu đặc quyền mà không cần phải sao chép hay dán mật khẩu	
5	**Bảo mật và sẵn sàng cho doanh nghiệp**		
5.1	Cơ chế vault	Hỗ trợ cơ chế bảo mật mạnh mẽ, mã hóa AES-256, mã hóa kép, cách ly khóa mã hóa và các phương pháp tốt tiêu chuẩn khác đảm bảo tính bảo mật dữ liệu vững chắc.	
5.2	Truyền dữ liệu an toàn	Cho phép bảo vệ dữ liệu khi chuyển tiếp, Hệ thống quản trị mật khẩu đặc quyền yêu cầu tất	

TT	Nội dung yêu cầu		Ghi chú
		cả các quá trình truyền từ và trong ứng dụng chỉ được thực hiện thông qua các giao thức an toàn.	
5.3	Chứng thực 2 lớp	Cho phép thực thi chứng thực 2 lớp cho việc đăng nhập vào hệ thống quản trị mật khẩu đặc quyền. Xác thực thông thường ở giai đoạn 1, cung cấp nhiều lựa chọn cho việc xác thực ở giai đoạn 2	
5.4	Tích hợp hệ thống tạo yêu cầu hỗ trợ (ticket)	Cho phép tích hợp với các hệ thống tạo/quản lý yêu cầu hỗ trợ	
5.5	Chế độ tuân thủ FIPS 140-2	Cho phép hoạt động ở chế độ tuân thủ FIPS 140-2.	
5.6	Quản lý danh tính liên kết	Hỗ trợ tích hợp cho Security Assertion Markup Language (SAML) 2.0 và tích hợp sẵn với Okta cho SSO. Ngoài ra cũng có thể cấu hình hệ thống quản trị mật khẩu đặc quyền để tích hợp với bất kỳ kho nhận dạng nào trong môi trường hệ thống mạng.	
6	**Truy vết, kiểm tra, quản lý thời gian thực, báo cáo & tuân thủ**		
6.1	Kiểm tra tác động vào hệ thống Công nghệ thông tin	Cho phép nắm bắt mọi thao tác của người dùng, thiết lập trách nhiệm giải trình và tính minh bạch cho tất cả các hành động liên quan đến mật khẩu. Thông tin này có thể được trình bày dưới dạng: Log dựa trên văn bản, thông báo email, thông báo log đến các giải pháp SIEM, SNMP trap hệ thống giám sát	
6.2	Truy cập và báo cáo hoạt động	Cung cấp một bộ sưu tập về quyền truy cập của người dùng, hoạt động và các báo cáo tóm tắt khác mà người quản trị có thể sử dụng để tăng cường quản lý các mật khẩu đặc quyền trong tổ chức của mình.	
6.3	Báo cáo tùy chọn	Hệ thống quản trị mật khẩu đặc quyền có thể kết hợp các bộ chi tiết độc lập từ hồ sơ kiểm toán và báo cáo trạng thái chung để thu được thông tin hữu ích. Có thể tận dụng dữ liệu có sẵn để đáp ứng các yêu cầu kiểm toán, nhiệm vụ bảo mật và các nhu cầu tuân thủ khác nhau.	
6.4	Cảnh báo và thông báo thời gian thực	Cho phép gửi cảnh báo thời gian thực cho tất cả các hoạt động được kiểm tra, bao gồm quyền truy cập, sửa đổi, xóa, thay đổi quyền chia sẻ và nhiều sự kiện khác. Ngoài ra ,cũng có thể tạo SNMP trap và thông báo Syslog tới hệ thống quản lý để phát hiện các bất thường một cách nhanh chóng.	

TT	Nội dung yêu cầu		Ghi chú
6.5	Báo cáo tuân thủ đa dạng và đa chiều	Giúp các tổ chức đạt được sự tuân thủ Công nghệ thông tin (NIST, PCI-DSS, FISMA, HIPAA, NERC-CIP, ISO-IEC 27001, SOX) thông qua cơ chế vault mạnh mẽ, xác thực người dùng và cung cấp tài khoản.	
6.6	Tích hợp hệ thống giám sát an ninh mạng SIEM (Security information and event management – SIEM)	Cho phép tích hợp SIEM để cung cấp dữ liệu truy cập đặc quyền cho bất kỳ công cụ quản lý sự kiện nào.	
6.7	Báo cáo truy vấn (query report)	Cho phép tạo báo cáo truy vấn để lấy dữ liệu cụ thể từ cơ sở dữ liệu của hệ thống quản trị mật khẩu, bằng cách viết truy vấn SQL hoặc tùy chỉnh truy vấn SQL trực tiếp từ các báo cáo hiện có trong danh mục	
7	**Phục hồi sau thảm họa, tính khả dụng và tính di động cao**		
7.1	Sao lưu trực tiếp	Cung cấp cả 2 cách sao lưu theo lịch hoặc trực tiếp cho toàn bộ cơ sở dữ liệu cho việc khắc phục sự cố	
7.2	Khôi phục nhanh	Cho phép khôi phục (dữ liệu đã sao lưu) từ cơ sở dữ liệu PostgreSQL hoặc MySQL vào cơ sở dữ liệu ứng dụng bằng cách thực thi tập lệnh có sẵn trong thư mục cài đặt của hệ thống quản trị mật khẩu đặc quyền	
7.3	Kiến trúc khả dụng cao (high availability)	Cho phép thiết lập các cơ chế khả dụng cao cho hệ thống quản trị mật khẩu đặc quyền, đảm bảo tính liên tục trong các hoạt động liên quan đến mật khẩu với dự phòng dữ liệu	
7.4	Truy cập di động	Cung cấp một ứng dụng riêng dành cho các nền tảng iOS, Android và Windows.	
7.5	Truy cập ngoại tuyến an toàn	Để đảm bảo mật khẩu liên tục có sẵn ngay cả khi không có kết nối internet, Hệ thống quản trị mật khẩu đặc quyền cung cấp nhiều tùy chọn để truy cập ngoại tuyến an toàn. Mật khẩu có thể được xuất dưới dạng tệp HTML được mã hóa hoặc bảng tính văn bản thuần túy. Tất cả các hoạt động xuất khẩu đều được nắm bắt kịp thời trong quá trình kiểm toán.	
7.6	Thiết lập kế hoạch dự phòng cho tài khoản cấp cao (super admin), có quyền	Cho phép lập kế hoạch trước với tài khoản quản trị viên cấp cao tùy chọn. Về cơ bản, quản trị viên cấp cao có toàn quyền truy cập vào tất cả các mật khẩu được lưu trữ trong hệ thống quản trị mật khẩu. Nếu người dùng cần mật khẩu	

TT	Nội dung yêu cầu		Ghi chú
	truy cập vào tất cả hệ thống	gấp, hãy sử dụng thông tin đăng nhập quản trị viên cấp cao để nhanh chóng đăng nhập và lấy lại mật khẩu cần thiết.	
7.7	Từ chối việc tạo tài khoản cấp cao (super-admin) nhiều hơn một	Hạn chế tạo thêm các tài khoản quản trị viên cấp cao khác sau khi tài khoản đầu tiên đã được tạo để ngăn chặn việc lưu thông nhiều tài khoản một cách nguy hiểm.	
7.8	Nhập mật khẩu từ KeePass	Có thể nhập chi tiết tài nguyên (tài nguyên CNTT, tài khoản và mật khẩu) trực tiếp từ KeePass (cả 1.x và 2.x) bằng trình hướng dẫn nhập. Tệp nhập phải là tệp cơ sở dữ liệu KeePass, .kdb hoặc .kdbx.	
7.9	Tiện ích mở rộng trên trình duyệt	Cho phép đồng bộ hóa mật khẩu trên các trình duyệt một cách an toàn thông qua các tiện ích mở rộng trình duyệt gốc để giúp các hoạt động quản lý mật khẩu và tự động đăng nhập diễn ra liền mạch.	
8	**Quản lý chứng chỉ SSL & khóa SSH**		
8.1	Tự động phát hiện SSH / SSL	Khám phá tất cả các khóa và chứng chỉ SSH được triển khai trong hệ thống mạng. Hợp nhất tất cả các thực thể đã phát hiện và bảo mật chúng trong kho lưu trữ.	
8.2	Tạo cặp khóa SSH và phân lập người dùng	Tạo các cặp khóa công khai và riêng tư mới và liên kết các khóa riêng tư với người dùng của họ. Xoay chìa khóa định kỳ để tránh sử dụng sai.	
8.3	Xoay định kỳ các khóa SSH	Xoay các cặp khóa SSH theo định kỳ.	
8.4	Quản lý vòng đời chứng chỉ (mua lại, triển khai và tự động gia hạn từ CA của bên thứ ba)	Giúp đơn giản hóa quy trình quản lý chứng chỉ bằng cách tự động hóa việc mua lại, phát hành, triển khai, cấp lại, gia hạn và thu hồi chứng chỉ. Hỗ trợ quản lý vòng đời chứng chỉ từ đầu đến cuối cho các trang web công khai bằng cách tích hợp với Tổ chức Certificate Authority (CA)	
8.5	Tạo chứng chỉ self-service	Cho phép quản trị viên tạo chứng chỉ tự ký của riêng bằng cách sử dụng Java keytool. Các chứng chỉ này được tự động nhập vào kho lưu trữ của hệ thống quản trị mật khẩu khi tạo thành công.	
8.6	Quản lý quy trình CSR	Quản lý quy trình CSR	
8.7	Triển khai và xác thực chứng chỉ SSL	Hỗ trợ quản lý vòng đời từ đầu đến cuối của các chứng chỉ thu được từ các tổ chức phát hành chứng chỉ đáng tin cậy (CA) bằng cách cho phép người dùng thu thập, hợp nhất, triển khai,	

TT	Nội dung yêu cầu		Ghi chú
		gia hạn và theo dõi các chứng chỉ do CA thương mại cấp từ một giao diện duy nhất.	
8.8	Theo dõi tính hợp lệ và triển khai chứng chỉ SSL	Tự động triển khai các chứng chỉ từ kho lưu trữ trên các hệ thống đích chính xác. Có thể sử dụng để triển khai các chứng chỉ trên các hệ thống khác nhau một cách riêng lẻ hoặc hàng loạt.	
8.9	Chia sẻ chứng chỉ SSL	Cho phép chia sẻ chứng chỉ hoặc nhóm chứng chỉ của mình với người dùng và nhóm người dùng.	
8.10	Quét lỗ hổng SSL	Quét các chứng chỉ SSL trong kho lưu trữ của và gắn cờ các chứng chỉ dễ gặp bất kỳ lỗ hổng nào.	
8.11	Cảnh báo hết hạn chứng chỉ SSL	Cho phép kích hoạt thông báo cho nhiều hoạt động khác nhau như hết hạn khóa SSL, xoay khóa SSH không thành công, quản lý chứng chỉ, hết hạn khóa.	
II	**Yêu cầu khác**		
1	Phiên bản phần mềm	- Bản quyền cho ít nhất 5 quản trị viên - Quản lý ít nhất 25 tài khoản (keys) sử dụng vĩnh viễn	
2	Thời gian sử dụng	- Bản quyền sử dụng, nâng cấp và cập nhật vĩnh viễn. - Bản quyền hỗ trợ kỹ thuật từ Hãng trong 02 năm.	