SẢN PHẨM AN NINH MẠNG

QUY CHẾ BẢO MẬT THÔNG TIN

SẢN PHẨM TƯỜNG LỬA SHINOBI DEFENSE

Nguyên tắc, tổ chức, phân loại thông tin, kiểm soát truy cập, quản lý lỗ hổng và ứng cứu sự cố

Phiên bản tài liệu 1.0 · Mã tài liệu QCBM-01 · Ngày ban hành 23/8/2026

Đơn vị ban hành	Công ty TNHH Bảo Mật An Minh (mã số doanh nghiệp 0319456414)
Địa chỉ	157C Cô Bắc, Phường Cầu Ông Lãnh, Thành phố Hồ Chí Minh
Người phê duyệt	Lương Đăng Dũng, Giám đốc
Ban hành kèm theo	Phương án kinh doanh sản phẩm tường lửa Shinobi Defense, mã PAKD-FW-01

Thành phố Hồ Chí Minh, tháng 8 năm 2026

MỤC LỤC

QUY CHẾ BẢO MẬT THÔNG TIN

Công ty TNHH Bảo Mật An Minh

1. Bảng kiểm soát tài liệu
2. Mục đích
3. Căn cứ
4. Phạm vi
5. Nguyên tắc bảo mật
6. Tổ chức và trách nhiệm
7. Hệ thống quy chế thành phần
8. Phân loại thông tin và thời hạn lưu trữ
9. Kiểm soát truy cập
10. An toàn vật lý
11. Mã hoá và quản lý khoá
12. An toàn trong phát triển và chuỗi cung ứng phần mềm
13. Tiếp nhận, xử lý và công bố lỗ hổng
14. Quản lý lỗ hổng và bản vá
15. Ứng cứu sự cố
16. Sao lưu, khôi phục và liên tục hoạt động
17. Nhân sự và đào tạo
18. Quản lý bên thứ ba
19. Xử lý yêu cầu của cơ quan nhà nước
20. Kiểm tra và duy trì hiệu lực
21. Hiệu lực

QUY CHẾ BẢO MẬT THÔNG TIN

Công ty TNHH Bảo Mật An Minh

Ban hành kèm theo Phương án kinh doanh sản phẩm tường lửa Shinobi Defense, mã PAKD-FW-01.

1. Bảng kiểm soát tài liệu

Trường	Nội dung
Tên tài liệu	Quy chế bảo mật thông tin
Mã tài liệu	QCBM-01
Phiên bản tài liệu	1.0
Ngày ban hành	23/8/2026
Phạm vi lưu hành	Cung cấp cho khách hàng, đối tác, cơ quan quản lý nhà nước và đăng tải trên trang thông tin điện tử của doanh nghiệp. Bản này nêu nguyên tắc và cam kết, lược các chi tiết vận hành có thể bị lợi dụng để tấn công hệ thống
Đơn vị ban hành	Công ty TNHH Bảo Mật An Minh (mã số doanh nghiệp 0319456414)
Người phê duyệt	Lương Đăng Dũng, Giám đốc (Người đại diện theo pháp luật)
Đối tượng áp dụng	Toàn bộ nhân sự, cộng tác viên, đối tác có quyền truy cập hệ thống hoặc thông tin của doanh nghiệp
Chu kỳ rà soát	Một năm một lần, hoặc ngay khi có thay đổi lớn về công nghệ, tổ chức hoặc quy định pháp luật
Tài liệu liên quan	PAKD-FW-01, CSCL-FW-01, CSKH-01, QTKN-01

2. Mục đích

Quy chế xác lập khung bảo vệ tính bí mật, tính toàn vẹn, tính sẵn sàng và tính chống chối bỏ đối với thông tin mà doanh nghiệp tạo ra, tiếp nhận, xử lý hoặc lưu giữ, bao gồm mã nguồn sản phẩm, khoá ký số, thông tin hệ thống của khách hàng, hồ sơ hợp đồng và hồ sơ sự cố.

Quy chế là cơ sở để doanh nghiệp bảo đảm rằng một sản phẩm an ninh mạng được sản xuất trong môi trường được kiểm soát, và rằng chuỗi cung ứng phần mềm từ mã nguồn tới bản chạy trên máy khách hàng không bị can thiệp.

3. Căn cứ

Văn bản, tiêu chuẩn	Vai trò
Luật An ninh mạng số 116/2025/QH15	Nghĩa vụ bảo đảm an ninh mạng của doanh nghiệp kinh doanh sản phẩm an ninh mạng
Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 và Nghị định 356/2025/NĐ-CP	Nghĩa vụ bảo vệ dữ liệu cá nhân trong hoạt động của doanh nghiệp
Luật Dữ liệu số 60/2024/QH15	Quản trị dữ liệu số, lưu trữ dữ liệu trong nước
ISO/IEC 27001:2022	Khung hệ thống quản lý an toàn thông tin được doanh nghiệp tự nguyện áp dụng
ISO/IEC 29147 và ISO/IEC 30111	Thực hành quốc tế về tiếp nhận, xử lý và công bố lỗ hổng
ISO 22301	Thực hành quốc tế về quản lý liên tục hoạt động

4. Phạm vi

Nhóm	Nội dung thuộc phạm vi
Hệ thống	Máy trạm phát triển, hệ thống quản lý mã nguồn, hạ tầng kiểm thử, hạ tầng phát hành và cấp phép, thiết bị lưu trữ sao lưu
Thông tin	Mã nguồn, tài liệu thiết kế, khoá ký số và khoá riêng, thông tin cấu hình hệ thống khách hàng, kết quả kiểm thử, hồ sơ sự cố, hồ sơ hợp đồng, dữ liệu cá nhân phát sinh trong quá trình hỗ trợ
Con người	Nhân sự chính thức, cộng tác viên, thực tập sinh, đại lý và đối tác tích hợp hệ thống có quyền truy cập
Quy trình	Phát triển, kiểm thử, phát hành, triển khai, hỗ trợ, quản lý thay đổi, ứng cứu sự cố, sao lưu và tiêu huỷ dữ liệu

5. Nguyên tắc bảo mật

Nguyên tắc	Áp dụng cụ thể
Đặc quyền tối thiểu	Mỗi tài khoản chỉ được cấp đúng quyền cần cho công việc. Tiến trình sản phẩm chạy dưới tài khoản không phải quản trị hệ thống, chỉ nhận đúng các quyền hệ thống tối thiểu
Phòng thủ nhiều lớp	Bảo vệ độc lập ở các lớp mạng, kênh truyền, ứng dụng, thời gian chạy, dữ liệu, truy cập và giám sát. Một lớp bị vô hiệu không làm sụp toàn bộ
An toàn khi lỗi	Khi cấu hình không hợp lệ hoặc thành phần kiểm tra gặp lỗi, hệ thống chuyển sang trạng thái chặn hoặc tắt chức năng, không chuyển sang trạng thái cho qua
An toàn theo mặc định	Giá trị mặc định là giá trị an toàn cho môi trường vận hành thật. Không dùng khoá, mã bí mật hoặc cấu hình rút gọn dành cho phát triển làm giá trị mặc định
Phân tách trách nhiệm	Người viết mã, người phê duyệt phát hành và người giữ khoá ký là các vai trò khác nhau

Nguyên tắc	Áp dụng cụ thể
Lưu vết đầy đủ	Mọi thao tác quản trị và mọi thay đổi cấu hình được ghi nhật ký kiểm toán có chuỗi toàn vẹn, phát hiện được hành vi sửa hoặc xoá bản ghi
Cần biết mới được biết	Thông tin hệ thống của khách hàng chỉ chia sẻ trong phạm vi nhân sự trực tiếp tham gia dự án

6. Tổ chức và trách nhiệm

Vai trò	Trách nhiệm
Giám đốc	Phê duyệt quy chế, cấp nguồn lực, quyết định xử lý sự cố mức nghiêm trọng, quản lý khoá ký gốc
Bộ phận Bảo đảm chất lượng và An ninh thông tin	Ban hành hướng dẫn thực hiện, giám sát tuân thủ, quản lý rủi ro và lỗ hổng, điều phối ứng cứu sự cố, đầu mối tiếp nhận báo cáo lỗ hổng từ bên ngoài. Hoạt động độc lập với khối phát triển
Trưởng các khối	Bảo đảm nhân sự thuộc khối tuân thủ quy chế, rà soát quyền truy cập của nhân sự trong khối
Toàn bộ nhân sự	Tuân thủ quy chế, báo cáo ngay khi phát hiện dấu hiệu bất thường hoặc nghi ngờ lộ lọt thông tin

7. Hệ thống quy chế thành phần

Nhóm	Quy chế	Nội dung chính
Chính sách nền	Chính sách an toàn thông tin	Mục tiêu bảo mật, cam kết nguồn lực của lãnh đạo, chu kỳ rà soát
Chính sách nền	Quy định sử dụng hợp lệ tài nguyên	Phạm vi được phép sử dụng thiết bị, tài khoản và dữ liệu của doanh nghiệp
Kiểm soát truy cập	Quy chế kiểm soát truy cập	Nguyên tắc đặc quyền tối thiểu, cấp phát và thu hồi quyền, rà soát quyền định kỳ
Kiểm soát truy cập	Quy chế mật khẩu và xác thực	Yêu cầu độ mạnh, xác thực hai lớp, cấm dùng chung tài khoản
Dữ liệu	Quy chế phân loại thông tin	Bốn mức phân loại và yêu cầu bảo vệ tương ứng
Dữ liệu	Quy chế mã hoá	Thuật toán được phép, quản lý vòng đời khoá, yêu cầu mã hoá khi lưu và khi truyền
Dữ liệu	Quy chế lưu trữ và tiêu huỷ dữ liệu	Thời hạn lưu từng loại dữ liệu, phương pháp xoá an toàn, thẩm quyền phê duyệt tiêu huỷ
Vận hành	Quy chế quản lý tài sản	Kiểm kê thiết bị, hệ thống và tài khoản, gán chủ sở hữu cho từng tài sản

Nhóm	Quy chế	Nội dung chính
Vận hành	Quy chế quản lý thay đổi	Yêu cầu thay đổi, đánh giá tác động, phê duyệt, phương án quay lui, thay đổi khẩn cấp
Vận hành	Quy chế quản lý lỗ hổng và bản vá	Nguồn thông tin lỗ hổng, phân loại mức nghiêm trọng, thời hạn khắc phục
Ứng cứu	Quy chế ứng cứu sự cố	Phân loại mức sự cố, thời gian phản hồi, quy trình leo thang, hồ sơ sau sự cố
Liên tục hoạt động	Quy chế sao lưu và liên tục hoạt động	Chu kỳ sao lưu, mục tiêu thời gian khôi phục, kịch bản mất hạ tầng phát hành
Quản trị rủi ro	Quy chế đánh giá và xử lý rủi ro	Danh mục tài sản, mô hình mối đe doạ, sổ đăng ký rủi ro, kế hoạch xử lý, chấp nhận rủi ro tồn dư

8. Phân loại thông tin và thời hạn lưu trữ

Mức phân loại	Ví dụ	Yêu cầu bảo vệ	Thời hạn lưu
Bí mật	Khoá ký số, khoá riêng chứng thư, thông tin xác thực hệ thống	Chỉ người được chỉ định truy cập, lưu mã hoá, không truyền qua kênh không mã hoá	Theo vòng đời khoá, tiêu huỷ an toàn ngay khi thay khoá
Nhạy cảm	Thông tin cấu hình hệ thống khách hàng, kết quả kiểm thử xâm nhập, hồ sơ sự cố	Chỉ nhân sự tham gia dự án truy cập, lưu mã hoá, có nhật ký truy cập	3 năm kể từ khi kết thúc dự án hoặc đóng sự cố
Nội bộ	Tài liệu thiết kế, mã nguồn, quy trình nội bộ	Chỉ nhân sự doanh nghiệp truy cập, kiểm soát theo vai trò	Theo vòng đời sản phẩm
Công khai	Tài liệu giới thiệu sản phẩm, hướng dẫn cài đặt, các tài liệu doanh nghiệp đăng tải công khai	Không hạn chế truy cập, kiểm soát tính chính xác trước khi đăng tải	Không giới hạn

Bản sao cấu hình và nhật ký do khách hàng cung cấp để phân tích sự cố không áp dụng thời hạn 3 năm nêu trên. Các bản sao này được xoá ngay sau khi kết thúc phân tích, theo thời hạn cam kết tại tài liệu mã CSKH-01. Thời hạn 3 năm chỉ áp dụng cho hồ sơ sự cố do doanh nghiệp lập, gồm diễn biến, kết luận và biện pháp khắc phục, không kèm dữ liệu gốc của khách hàng.

Thời hạn lưu nhật ký hệ thống nội bộ: nhật ký truy cập và nhật ký sự kiện an ninh lưu 90 ngày ở chế độ trực tuyến và 365 ngày ở chế độ lưu trữ nén có mã hoá. Nhật ký kiểm toán lưu 365 ngày. Chứng cứ sự cố lưu 3 năm kể từ ngày đóng sự cố. Dữ liệu ở mức bí mật và nhạy cảm khi hết thời hạn được xoá bằng phương pháp ghi đè nhiều lần, có biên bản.

9. Kiểm soát truy cập

- Cấp quyền theo vai trò công việc, phê duyệt bởi trưởng khối và Bộ phận Bảo đảm chất lượng và An ninh thông tin.
- Truy cập máy chủ chỉ bằng khoá, không dùng mật khẩu. Giao diện quản trị dùng xác thực hai lớp.
- Giao diện quản trị của mọi máy chủ chỉ nghe trên máy cục bộ, truy cập từ xa phải qua kênh quản trị riêng.
- Cấm dùng chung tài khoản. Mỗi thao tác phải quy được về một người cụ thể.
- Rà soát toàn bộ quyền truy cập định kỳ, thu hồi quyền không còn cần thiết.
- Thu hồi quyền trong ngày làm việc khi nhân sự thay đổi vị trí hoặc nghỉ việc, có biên bản bàn giao.

10. An toàn vật lý

- Khu vực đặt máy trạm phát triển, máy ký số và thiết bị lưu trữ sao lưu có kiểm soát ra vào, tách biệt với khu vực tiếp khách.
- Thiết bị lưu trữ chứa thông tin mức bí mật và nhạy cảm được mã hoá toàn bộ ổ đĩa.
- Thiết bị mang ra ngoài trụ sở phải được phê duyệt, mã hoá và không lưu khoá ký số.
- Thiết bị hết vòng đời được xoá dữ liệu an toàn trước khi thanh lý, có biên bản.

11. Mã hoá và quản lý khoá

- Bắt buộc mã hoá kênh truyền cho mọi kết nối quản trị và mọi kết nối truyền dữ liệu nhạy cảm.
- Mã hoá dữ liệu khi lưu đối với tệp chứa thông tin nhạy cảm. Mật khẩu được băm bằng thuật toán chống tấn công dò tìm.
- Khoá ký gốc dùng cho chuỗi tin cậy phát hành được lưu trên máy ký chuyên dụng, không đặt trên máy chủ dịch vụ, không sao chép lên máy khách hàng.
- Khoá được thay theo chu kỳ. Khoá cũ bị tiêu huỷ an toàn ngay sau khi xác nhận khoá mới hoạt động.
- Doanh nghiệp ưu tiên các thuật toán mật mã thuộc nhóm được phê duyệt theo chuẩn quốc tế đang áp dụng cho sản phẩm.

12. An toàn trong phát triển và chuỗi cung ứng phần mềm

- Mọi thay đổi mã nguồn phải qua xét duyệt bởi người khác trước khi hợp nhất.
- Kiểm thử tự động, kiểm thử xâm nhập và kiểm thử hiệu năng phải đạt trước khi qua cổng chất lượng.
- Bản phát hành được ký số và phân phối qua kho cập nhật có chuỗi tin cậy. Máy khách hàng xác thực chữ ký trước khi áp dụng.
- Không đưa thông tin xác thực, khoá hoặc dữ liệu thật của khách hàng vào mã nguồn, vào dữ liệu kiểm thử hoặc vào tài liệu.

- Doanh nghiệp lập và duy trì **danh mục thành phần phần mềm** theo định dạng máy đọc được, gồm các thư viện bên thứ ba và phiên bản tương ứng, phục vụ việc rà soát lỗ hổng và cung cấp cho khách hàng khi có yêu cầu.
- Thư viện bên thứ ba được rà soát về giấy phép và lỗ hổng trước khi đưa vào sản phẩm, theo dõi liên tục sau đó. Phụ thuộc được ghim theo phiên bản, không tự động nâng cấp trong bản phát hành.
- Việc dựng bản phát hành thực hiện trên hạ tầng do doanh nghiệp kiểm soát, không dựng trên máy cá nhân không được quản lý.

13. Tiếp nhận, xử lý và công bố lỗ hổng

Doanh nghiệp áp dụng thực hành công bố lỗ hổng có phối hợp theo ISO/IEC 29147 và ISO/IEC 30111.

Nội dung	Cam kết
Kênh tiếp nhận	Thư điện tử security@anminhsecurity.com, công bố trên trang thông tin điện tử anminhsecurity.com. Chấp nhận báo cáo ẩn danh
Xác nhận tiếp nhận	Trong 3 ngày làm việc kể từ khi nhận báo cáo
Kết quả xác minh ban đầu	Trong 10 ngày làm việc, thông báo cho người báo cáo là chấp nhận, cần thêm thông tin hay không tái hiện được
Khắc phục	Theo mức nghiêm trọng nêu tại mục 14
Thời điểm công bố	Phối hợp với người báo cáo, thông thường sau khi bản vá sẵn sàng, mốc tham chiếu 90 ngày kể từ ngày tiếp nhận. Rút ngắn khi lỗ hổng đang bị khai thác
Nội dung công bố	Bản tin an ninh nêu phiên bản bị ảnh hưởng, mức nghiêm trọng, biện pháp khắc phục và biện pháp giảm thiểu tạm thời. Ghi nhận công lao người báo cáo nếu họ đồng ý
Cam kết với người báo cáo	Doanh nghiệp không thực hiện hành vi pháp lý bất lợi đối với người báo cáo có trách nhiệm, với điều kiện người đó không khai thác vượt phạm vi cần thiết để chứng minh, không truy cập dữ liệu của bên thứ ba và không công bố trước khi thống nhất
Trường hợp lỗ hổng đang bị khai thác	Thông báo sớm cho khách hàng bị ảnh hưởng và cho cơ quan nhà nước có thẩm quyền theo quy định pháp luật, kèm biện pháp giảm thiểu áp dụng ngay

14. Quản lý lỗ hổng và bản vá

Mức nghiêm trọng	Tiếp nhận	Xác minh	Khắc phục
Nghiêm trọng	Trong 2 giờ	Trong 4 giờ	Trong 48 giờ kể từ khi phát hiện
Cao	Trong 24 giờ	Trong 48 giờ	Trong 7 ngày
Trung bình	Trong 48 giờ	Trong 5 ngày	Trong 30 ngày

Mức nghiêm trọng	Tiếp nhận	Xác minh	Khắc phục
Thấp	Trong 5 ngày	Theo kế hoạch	Trong 60 ngày

Doanh nghiệp theo dõi liên tục thông tin lỗ hổng của các thành phần bên thứ ba có trong danh mục thành phần phần mềm và xử lý theo cùng thang thời hạn nêu trên.

15. Ứng cứu sự cố

Mức	Mô tả	Thời gian phản hồi
P1	Có dấu hiệu khai thác đang diễn ra, lộ lọt dữ liệu, hoặc mất hoàn toàn khả năng bảo vệ	15 phút
P2	Suy giảm đáng kể năng lực bảo vệ, vượt qua một phần cơ chế phát hiện, lộ thông tin xác thực quản trị	1 giờ
P3	Ảnh hưởng giới hạn, hỏng một thành phần còn dự phòng, tỷ lệ cảnh báo sai tăng cao	4 giờ
P4	Ảnh hưởng nhỏ, không có rủi ro an ninh trực tiếp	24 giờ

Sự cố mức P1 và P2 báo cáo Giám đốc ngay khi phân loại. Sự cố liên quan đến thông tin của khách hàng được thông báo cho khách hàng theo tài liệu mã CSKH-01. Sự cố thuộc trường hợp phải báo cáo cơ quan quản lý nhà nước được báo cáo theo đúng thời hạn pháp luật quy định. Mỗi sự cố đều lập hồ sơ gồm diễn biến, nguyên nhân gốc, biện pháp khắc phục và biện pháp phòng ngừa tái diễn.

16. Sao lưu, khôi phục và liên tục hoạt động

- Sao lưu định kỳ mã nguồn, cấu hình hệ thống nội bộ và hồ sơ, lưu ở vị trí tách biệt với hệ thống gốc.
- Bản sao lưu chứa thông tin nhạy cảm được mã hoá.
- Kiểm tra khả năng khôi phục định kỳ, không coi việc sao lưu thành công là bằng chứng khôi phục được.
- Doanh nghiệp duy trì kịch bản ứng phó cho trường hợp mất hạ tầng phát hành hoặc hạ tầng cấp phép, bảo đảm khách hàng đang sử dụng không bị gián đoạn: sản phẩm vận hành độc lập tại hạ tầng khách hàng, không phụ thuộc kết nối tới doanh nghiệp để tiếp tục chạy.
- Với khách hàng thuộc lĩnh vực trọng yếu, doanh nghiệp sẵn sàng thoả thuận phương án ký quỹ mã nguồn tại bên thứ ba trung lập, để khách hàng tiếp tục vận hành và bảo trì sản phẩm trong trường hợp doanh nghiệp chấm dứt hoạt động.

17. Nhân sự và đào tạo

- Toàn bộ nhân sự ký thoả thuận bảo mật khi tiếp nhận công việc. Nghĩa vụ bảo mật tiếp tục có hiệu lực sau khi chấm dứt hợp đồng lao động.
- Đào tạo nhận thức an toàn thông tin khi tiếp nhận công việc và đào tạo lại định kỳ hằng năm.

- Nhân sự tham gia triển khai tại khách hàng được phổ biến quy định bảo vệ dữ liệu cá nhân và quy tắc ứng xử tại hiện trường trước mỗi dự án.
- Vi phạm quy chế được xử lý theo nội quy lao động và quy định pháp luật, tuỳ mức độ.

18. Quản lý bên thứ ba

- Đại lý và đối tác tích hợp hệ thống phải ký hợp đồng có điều khoản bảo mật, được đào tạo và chứng nhận trước khi phân phối sản phẩm.
- Nhà cung cấp dịch vụ hạ tầng được đánh giá về năng lực bảo mật trước khi sử dụng và rà soát định kỳ.
- Thông tin của khách hàng chỉ được chia sẻ với bên thứ ba khi có sự đồng ý bằng văn bản của khách hàng, trong phạm vi tối thiểu cần thiết.

19. Xử lý yêu cầu của cơ quan nhà nước

- Doanh nghiệp chấp hành yêu cầu hợp pháp của cơ quan nhà nước có thẩm quyền theo quy định pháp luật Việt Nam.
- Yêu cầu phải bằng văn bản, nêu rõ căn cứ pháp lý, phạm vi và thẩm quyền. Doanh nghiệp cung cấp đúng phạm vi được yêu cầu, không mở rộng.
- Mỗi lần cung cấp đều được ghi hồ sơ, lưu theo thời hạn quy định.
- Khi pháp luật không cấm, doanh nghiệp thông báo cho khách hàng có liên quan.
- Doanh nghiệp không cài đặt cơ chế truy cập ngầm vào sản phẩm dưới bất kỳ hình thức nào.

20. Kiểm tra và duy trì hiệu lực

- Rà soát toàn bộ hệ thống quy chế tối thiểu một năm một lần, hoặc ngay khi có thay đổi lớn.
- Đánh giá rủi ro định kỳ, cập nhật sổ đăng ký rủi ro và kế hoạch xử lý.
- Diễn tập ứng cứu sự cố định kỳ theo kịch bản, ghi nhận kết quả và điểm cần cải thiện.
- Rà soát quyền truy cập, nhật ký kiểm toán và tình trạng bản vá theo chu kỳ.
- Định kỳ mời đánh giá độc lập từ bên ngoài đối với sản phẩm và hạ tầng phát hành, kết quả là đầu vào bắt buộc cho kỳ rà soát quy chế.
- Doanh nghiệp chấp hành việc thanh tra, kiểm tra của cơ quan nhà nước có thẩm quyền và cung cấp hồ sơ theo yêu cầu hợp pháp.

21. Hiệu lực

Quy chế có hiệu lực kể từ ngày ban hành và thay thế các quy định nội bộ trước đó có nội dung trái với quy chế này. Mọi ý kiến liên quan gửi về Công ty TNHH Bảo Mật An Minh, 157C Cô Bắc, Phường Cầu Ông Lãnh, Thành phố Hồ Chí Minh, hoặc thư điện tử contact@anminhsecurity.com. Báo cáo lỗ hổng bảo mật gửi về security@anminhsecurity.com.