



BỘ TÀI CHÍNH

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

Số: 2999/QĐ-BTC

Hà Nội, ngày 16 tháng 10 năm 2026

QUYẾT ĐỊNH

**Về việc ban hành Quy chế quản lý, sử dụng và khai thác
Hệ thống camera giám sát an ninh tại các trụ sở cơ quan Bộ Tài chính**

BỘ TRƯỞNG BỘ TÀI CHÍNH

Căn cứ Luật An ninh mạng số 116/2025/QH15 ngày 10/12/2025;

Căn cứ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 ngày 26/6/2025;

Căn cứ Nghị định số 356/2025/NĐ-CP ngày 31/12/2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 376/2026/NĐ-CP ngày 01/10/2026 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Tài chính;

Căn cứ Quyết định số 2405/QĐ-BTC ngày 08/7/2025 của Bộ Tài chính ban hành Quy chế An toàn thông tin mạng và An ninh mạng Bộ Tài chính;

Theo đề nghị của Chánh Văn phòng Bộ Tài chính.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý, sử dụng và khai thác Hệ thống camera giám sát an ninh tại các trụ sở cơ quan Bộ Tài chính.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 3. Chánh Văn phòng Bộ, Thủ trưởng các đơn vị, công chức, viên chức, người lao động thuộc Bộ Tài chính và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3;
- Bộ trưởng Ngô Văn Tuấn (để báo cáo);
- Các đồng chí Thứ trưởng;
- Lưu: VT, VP (3b).

KT. BỘ TRƯỞNG

THỨ TRƯỞNG



Nguyễn Thị Bích Ngọc

QUY CHẾ
QUẢN LÝ, SỬ DỤNG VÀ KHAI THÁC HỆ THỐNG CAMERA
GIÁM SÁT AN NINH TẠI CÁC TRỤ SỞ CƠ QUAN BỘ TÀI CHÍNH
(Kèm theo Quyết định số ~~2999~~ /QĐ-BTC ngày 16 /10 /2026 của Bộ Tài chính)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Mục đích

1. Hỗ trợ công tác giám sát, bảo đảm an ninh, trật tự, an toàn phòng, chống cháy nổ, bảo vệ tài sản công của cơ quan Bộ Tài chính và tài sản cá nhân của công chức, viên chức, người lao động, khách đến liên hệ công tác.
2. Chủ động phòng ngừa, phát hiện và ngăn chặn kịp thời các hành vi xâm nhập bất hợp pháp, trộm cắp, phá hoại hoặc các hành vi vi phạm pháp luật và nội quy cơ quan.
3. Hỗ trợ giám sát, vận hành các hệ thống thiết bị kỹ thuật và các hoạt động chung phục vụ hoạt động, vận hành tại các trụ sở.
4. Ghi nhận, cung cấp bằng chứng khách quan phục vụ công tác xác minh sự cố nội bộ hoặc theo đề nghị phối hợp của cơ quan chức năng khi xảy ra tranh chấp, mất mát, tai nạn lao động hoặc sự cố khẩn cấp (cháy nổ, thiên tai).

Điều 2. Phạm vi, đối tượng áp dụng

1. Quy chế này quy định về các hoạt động quản lý, sử dụng, quản lý tài khoản, khai thác, trích xuất và bảo mật dữ liệu của hệ thống camera giám sát an ninh trong khuôn viên và bên trong tòa nhà tại các trụ sở cơ quan Bộ Tài chính.
2. Quy chế này áp dụng đối với công chức, viên chức, người lao động, các đơn vị làm việc tại trụ sở cơ quan Bộ và các tổ chức, cá nhân bên ngoài (bao gồm cả các đơn vị thuộc Bộ Tài chính không làm việc tại các trụ sở cơ quan Bộ Tài chính) đến giao dịch, liên hệ công tác.
3. Việc đầu tư, mua sắm lắp đặt, bảo trì bảo dưỡng Hệ thống camera giám sát an ninh thực hiện theo quy định của pháp luật có liên quan.

Điều 3. Giải thích từ ngữ

1. Hệ thống camera giám sát an ninh (sau đây gọi tắt là Hệ thống camera) tại trụ sở cơ quan Bộ Tài chính bao gồm thiết bị camera giám sát tại các vị trí lắp đặt, hệ thống thiết bị phục vụ ghi hình, quản lý và lưu trữ dữ liệu, các ứng dụng, phần mềm sử dụng trong hệ thống, mạng truyền dẫn dữ liệu và các thành phần khác để vận hành, khai thác dữ liệu và đảm bảo hoạt động hệ thống.
2. Dữ liệu camera: Bao gồm toàn bộ video, hình ảnh tĩnh, âm thanh (nếu có) do Hệ thống camera ghi lại, kèm theo thông tin về thời gian, địa điểm.



3. Trụ sở cơ quan Bộ Tài chính: Các trụ sở Bộ Tài chính giao Văn phòng Bộ quản lý, bố trí trụ sở làm việc, kho lưu trữ của các đơn vị.

4. Khu vực công cộng: Khu vực để xe, hành lang, sảnh đón các tầng, đường giao thông nội bộ, tường rào bảo vệ, Phòng truyền thống, khu vực cần giám sát hoạt động của các hệ thống máy móc, thiết bị, tài liệu lưu trữ.

5. Phòng làm việc của CBCC (bao gồm cả các khu vực làm việc tập trung) và phòng họp, hội trường.

6. Khu vực riêng tư: Phòng thay đồ, nhà vệ sinh, phòng nghỉ ngơi của CBCC, phòng chăm sóc sức khỏe, phòng y tế, và các khu vực khác liên quan đến quyền riêng tư tối thiểu của con người.

Chương II

YÊU CẦU KỸ THUẬT, BẢO MẬT DỮ LIỆU

Điều 4. Quy định chung

1. Hệ thống camera phục vụ công tác giám sát an ninh trật tự, đảm bảo an toàn và vận hành các hoạt động chung tại các trụ sở cơ quan Bộ Tài chính. Việc thu thập và xử lý dữ liệu từ Hệ thống camera chỉ được thực hiện vì mục đích quy định tại Điều 1.

2. Khu vực được lắp đặt camera: Khu vực công cộng nêu tại khoản 4 Điều 3. Tại khu vực có lắp đặt camera được công khai bằng hình thức biển báo, bảng chỉ dẫn tại các lối vào chính hoặc bảng thông báo điện tử tại các tầng, khu vực có lắp đặt camera để cá nhân biết mình đang được ghi hình theo quy định pháp luật.

3. Khu vực không được lắp đặt camera: Phòng làm việc của CBCC, phòng họp, hội trường quy định tại khoản 5 Điều 3 và Khu vực riêng tư quy định tại khoản 6 Điều 3.

4. Trường hợp cần thiết phải lắp đặt camera giám sát tại các khu vực quy định tại khoản 5 Điều 3 phải được Lãnh đạo Bộ phê duyệt trên cơ sở ý kiến đề nghị, thống nhất của Thủ trưởng đơn vị được giao quản lý hoặc bố trí sử dụng các khu vực trên.

5. Khu vực được đặt các màn hình giám sát gồm:

5.1. Phòng thường trực bảo vệ;

5.2. Phòng thường trực kỹ thuật;

5.3. Phòng trung tâm giám sát hệ thống camera.

6. Chánh Văn phòng Bộ quyết định: Việc bố trí các khu vực đặt màn hình giám sát quy định tại khoản 5 Điều này phù hợp với quy mô, nhu cầu, điều kiện tại các trụ sở Bộ giao Văn phòng quản lý và số lượng điểm lắp đặt camera hiển thị tại màn hình giám sát của các khu vực này đảm bảo phù hợp với tính chất, nhiệm vụ được giao trong công tác đảm bảo an ninh, an toàn và giám sát, vận hành các hệ thống thiết bị, kỹ thuật tại các trụ sở.

7. Dữ liệu camera thuộc danh mục dữ liệu được bảo vệ, nghiêm cấm mọi cá nhân tự ý sao chép, trích xuất, sử dụng dữ liệu này cho các mục đích riêng, giải quyết mâu thuẫn cá nhân, hoặc làm phương tiện đe dọa, xúc phạm danh dự, nhân phẩm của người khác và thực hiện các hành vi trái pháp luật.

Điều 5. Yêu cầu kỹ thuật, bảo mật dữ liệu

1. Hệ thống camera phải đáp ứng các yêu cầu về bảo đảm an toàn hệ thống thông tin theo cấp độ quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và quy định tại Thông tư số 48/2026/TT-BCA ngày 12/5/2026 của Bộ trưởng Bộ Công an ban hành Quy chuẩn kỹ thuật quốc gia về thiết bị camera giám sát sử dụng giao thức Internet - Các yêu cầu an ninh mạng cơ bản.

2. Hệ thống camera (bao gồm tất cả các thiết bị có sử dụng nguồn điện) phải được kết nối với bộ lưu điện (UPS) và máy phát điện dự phòng đảm bảo vận hành liên tục 24 giờ/ngày và 7 ngày/tuần, không được ngắt quãng trừ trường hợp bảo trì định kỳ đã được phê duyệt bằng văn bản hoặc sự cố bất khả kháng (mất điện diện rộng, thiên tai).

3. Dữ liệu camera đảm bảo được lưu trữ tối thiểu 30 ngày. Quá thời hạn trên Hệ thống camera được cấu hình tự động xóa/ghi đè theo thứ tự thời gian từ cũ nhất đến mới nhất.

4. Nhật ký truy cập: Thiết bị đầu ghi hoặc phần mềm quản lý camera phải luôn bật tính năng tự động ghi nhận nhật ký hệ thống (System Log). Nhật ký phải thể hiện rõ: Tên tài khoản truy cập, thời gian đăng nhập/đăng xuất, hành động thực hiện (xem trực tiếp, xem lại, vị trí xem, vị trí trích xuất) để phục vụ công tác hậu kiểm an ninh. Nhật ký truy cập phải được lưu trữ tối thiểu 30 ngày.

5. Thiết bị ghi lưu trữ dữ liệu, tủ rack chứa thiết bị mạng camera phải được đặt trong tủ có khóa và đặt trong phòng có khóa, chỉ những người có tên trong danh sách quản trị mới được giữ chìa khóa/thẻ từ vào/ra.

6. Hệ thống mạng dùng cho camera phải là mạng LAN độc lập hoặc phân tách phân đoạn mạng (VLAN riêng), không đi chung với mạng Wi-Fi công cộng để tránh nguy cơ bị tin tặc tấn công, xâm nhập trái phép.

7. Việc xem lại, trích xuất dữ liệu của Hệ thống camera thực hiện theo quy định cụ thể tại Chương III Quy chế này.

8. Khi thực hiện sửa chữa hoặc bảo trì định kỳ Hệ thống camera liên quan đến thiết bị lưu trữ dữ liệu, tủ rack hoặc phải sử dụng Tài khoản Quản trị Hệ thống camera (Tài khoản Admin) phải có tối thiểu 02 người (trong đó ít nhất có 01 nhân viên của Văn phòng Bộ đối với trường hợp đơn vị cung cấp dịch vụ sửa chữa, bảo trì), mật khẩu Tài khoản Admin phải được thay đổi ngay sau khi hoàn thành việc sửa chữa, bảo trì.

Điều 6. Phân quyền sử dụng

1. Tài khoản Quản trị Hệ thống camera (Tài khoản Admin) do Chánh Văn phòng quản lý hoặc ủy quyền cho Phó Chánh Văn phòng phụ trách tương ứng với từng Hệ thống camera tại các trụ sở (trên địa bàn các thành phố Hồ Chí Minh, Hà Nội, Đà Nẵng) quản lý. Tài khoản Admin có toàn quyền cấu hình hệ thống, cài đặt phần mềm, thiết lập/xóa, phân quyền đối với các tài khoản sử dụng, tài khoản trích xuất. Mật khẩu tài khoản Admin phải được đặt ở mức độ bảo mật cao và thay đổi định kỳ tối thiểu 06 tháng/lần hoặc thay đổi ngay lập tức khi: Có sự thay đổi người được phân công quản lý Tài khoản Admin; Sau khi sử dụng Tài khoản Admin để thực hiện việc tạo, phân quyền tài khoản hoặc sửa chữa, bảo trì Hệ thống camera.

2. Tài khoản trích xuất được phân quyền xem lại lịch sử ghi hình (Playback) và xuất file dữ liệu (Export) ra thiết bị ngoại vi. Tài khoản trích xuất do Chánh Văn phòng hoặc Chánh Văn phòng ủy quyền cho Phó Chánh Văn phòng phụ trách tương ứng với từng Hệ thống camera tại các trụ sở (trên địa bàn các thành phố Hồ Chí Minh, Hà Nội, Đà Nẵng) quản lý, chỉ được sử dụng trong các trường hợp quy định tại Điều 7 và được cấp có thẩm quyền quy định tại khoản 1 Điều 8 phê duyệt. Mật khẩu tài khoản trích xuất phải được đặt ở mức độ bảo mật cao và thay đổi định kỳ tối thiểu 06 tháng/lần hoặc thay đổi ngay lập tức sau khi hoàn thành xem lại, trích xuất dữ liệu (trường hợp giao cho Trưởng phòng Quản trị hoặc Trưởng phòng Đại diện Văn phòng Bộ tại thành phố Hồ Chí Minh thực hiện xem lại, trích xuất dữ liệu) hoặc khi có sự thay đổi người được phân công quản lý Tài khoản.

3. Trường hợp có sự thay đổi người được giao quản lý Tài khoản Admin và Tài khoản trích xuất: Các bên liên quan có trách nhiệm ghi nhận việc bàn giao các Tài khoản nêu trên bằng biên bản (trong đó có ghi nhận nội dung đổi mật khẩu sử dụng tài khoản ngay tại thời điểm bàn giao).

4. Tài khoản giám sát trực tuyến: Lực lượng bảo vệ, lực lượng trực kỹ thuật được cung cấp tài khoản sử dụng có tính năng xem trực tiếp theo thời gian thực (live-view) đối với một số điểm đặt camera phù hợp với nhiệm vụ được giao phục vụ công tác đảm bảo an ninh, an toàn và giám sát, vận hành các hệ thống thiết bị, kỹ thuật.

5. Khi phát hiện sự cố lộ, mất dữ liệu camera hoặc Hệ thống camera bị xâm nhập trái phép, nhân viên trực kỹ thuật có trách nhiệm báo cáo ngay Lãnh đạo Phòng Quản trị, Lãnh đạo Phòng Đại diện Văn phòng Bộ tại thành phố Hồ Chí Minh để báo cáo Lãnh đạo Văn phòng Bộ và phối hợp lập biên bản xác nhận sự việc, có phương án xử lý, khắc phục.

Chương III

SỬ DỤNG DỮ LIỆU, QUY TRÌNH TIẾP NHẬN, TRÍCH XUẤT DỮ LIỆU

Điều 7. Các trường hợp được xem lại, trích xuất dữ liệu

1. Xảy ra các sự cố: mất mát, hư hỏng tài sản công hoặc tài sản cá nhân trong tòa nhà (ghi nhận bằng biên bản), trường hợp khiếu nại của công dân; Mất

an toàn, phòng cháy, chữa cháy, an toàn lao động, cứu nạn cứu hộ; ứng phó sự cố khẩn cấp; ...Phục vụ vận hành, kiểm tra sự cố kỹ thuật.

2. Có dấu hiệu xâm nhập bất hợp pháp, phá hoại, hoặc xảy ra xung đột, xô xát làm mất an ninh, trật tự tại cơ quan (ghi nhận bằng biên bản).

3. Để xác minh, làm rõ các hành vi vi phạm kỷ luật lao động theo yêu cầu của Hội đồng Thi đua khen thưởng, Lãnh đạo Bộ hoặc Chánh Văn phòng Bộ.

4. Có yêu cầu chính thức bằng văn bản từ các cơ quan chức năng có thẩm quyền.

Điều 8. Thẩm quyền phê duyệt xem lại, trích xuất dữ liệu

1. Mọi hoạt động xem lại, trích xuất dữ liệu ra khỏi hệ thống lưu trữ đều phải được sự đồng ý của Chánh Văn phòng hoặc Phó Chánh văn phòng được giao phụ trách công tác quản trị, cơ sở vật chất tại các trụ sở có lắp đặt Hệ thống Camera và phải báo cáo lại Chánh Văn phòng để biết chỉ đạo.

2. Đơn vị được giao quản lý, vận hành Hệ thống camera (Phòng Quản trị, Đại diện Văn phòng Bộ tại thành phố Hồ Chí Minh), Nhân viên trực kỹ thuật tuyệt đối không thực hiện lệnh trích xuất dữ liệu dựa trên yêu cầu truyền miệng hoặc tin nhắn cá nhân không chính thức.

Điều 9. Quy trình xử lý yêu cầu xem lại, trích xuất dữ liệu

1. Khi có nhu cầu khai thác trích xuất dữ liệu: Cá nhân, đơn vị phải điền đầy đủ thông tin vào “*Phiếu đề nghị xem lại, trích xuất dữ liệu camera*” (Mẫu số 01 kèm theo), nêu rõ lý do, khoảng thời gian và vị trí camera cần khai thác, gửi về Văn phòng Bộ (Phòng Quản trị hoặc Đại diện Văn phòng Bộ tại thành phố Hồ Chí Minh).

Đối với yêu cầu phối hợp từ cơ quan chức năng có thẩm quyền thực hiện trên cơ sở Văn bản đề nghị chính thức gửi đến Bộ Tài chính. Cơ quan chức năng phải xuất trình Giấy giới thiệu, Thẻ căn cước công dân/Chứng minh, Thẻ ngành để đối chiếu với Văn bản đề nghị phối hợp.

2. Phòng Quản trị hoặc Đại diện Văn phòng Bộ tại thành phố Hồ Chí Minh có trách nhiệm tiếp nhận, thẩm định lý do, mục đích phù hợp với quy định tại Điều 7 và kiểm tra tính hợp pháp, sự cần thiết (chỉ xem lại/xem lại, trích xuất dữ liệu) của yêu cầu trước khi trình Chánh Văn phòng hoặc Phó Chánh Văn phòng xem xét, phê duyệt (Thời gian tối đa là 04 giờ làm việc, đối với các trường hợp khẩn cấp thời gian tối đa là 01 giờ làm việc kể từ khi nhận đủ hồ sơ hợp lệ).

3. Trên cơ sở kết quả phê duyệt của Lãnh đạo Văn phòng; trường hợp đề nghị được phê duyệt, Trưởng phòng Quản trị hoặc Trưởng phòng Đại diện Văn phòng Bộ tại thành phố Hồ Chí Minh, nhân viên trực kỹ thuật sử dụng tài khoản trích xuất do người có thẩm quyền quản lý quy định tại khoản 2 Điều 6 cung cấp để tiến hành xem lại, tìm kiếm hình ảnh. Quá trình này phải có tối thiểu 02 người cùng thực hiện.

4. Xử lý dữ liệu xem lại, trích xuất: Căn cứ kết quả xem lại, tìm kiếm hình ảnh tại khoản 3 Điều này, trường hợp không cần thiết phải trích xuất bản giao hình ảnh/video cho bên đề nghị khai thác mà vẫn xác minh được khi phát sinh các vụ việc quy định tại Điều 7, các trường hợp khác không cần thiết phải trích xuất bản giao dữ liệu hoặc hình ảnh/video sau khi trích xuất thuộc dữ liệu cá nhân nhạy cảm theo quy định của pháp luật bảo vệ dữ liệu cá nhân, Trưởng phòng Quản trị hoặc Trưởng phòng Đại diện Văn phòng Bộ tại thành phố Hồ Chí Minh có trách nhiệm báo cáo lại Lãnh đạo Văn phòng về sự phù hợp khi cung cấp, bản giao dữ liệu trích xuất.

5. Việc quản lý, sử dụng, bản giao dữ liệu và lưu nhật ký:

5.1. Việc quản lý dữ liệu là kết quả trích xuất tại khoản 4 Điều này phải đảm bảo nguyên tắc: Chỉ được lưu duy nhất vào 01 thiết bị ngoại vi (USB, Đĩa CD, Ổ cứng di động) do Văn phòng Bộ chuẩn bị được kiểm tra an toàn, mã hóa mật khẩu và quản lý theo quy định về an toàn thông tin của Bộ Tài chính. Việc quản lý thiết bị ngoại vi lưu trữ dữ liệu do người có thẩm quyền quy định tại khoản 2 Điều 6 chỉ định (đối với các trường hợp không phải bản giao dữ liệu cho các cơ quan chức năng quy định tại khoản 4 Điều 7).

5.2. Người nhận dữ liệu, người được giao quản lý dữ liệu trích xuất chịu trách nhiệm quản lý, sử dụng dữ liệu trích xuất đúng mục đích quy định tại Điều 7. Các trường hợp sử dụng sai mục đích, các hành vi bị cấm quy định tại Điều 10 sẽ bị xử lý theo quy định của pháp luật có liên quan. Dữ liệu lưu trữ tại thiết bị ngoại vi phải được xóa/hủy sau khi hoàn thành việc xác minh các vụ việc cần xem lại, trích xuất dữ liệu camera quy định tại Điều 7.

5.3. Khi bản giao dữ liệu người nhận phải ký vào “*Sổ theo dõi việc khai thác dữ liệu camera*” (Mẫu số 02 kèm theo); đồng thời lập “*Biên bản bàn giao dữ liệu camera*” (Mẫu số 03 kèm theo).

6. Các hồ sơ liên quan đến việc xem lại, trích xuất dữ liệu (*Phiếu đề nghị xem lại, trích xuất dữ liệu camera; Sổ theo dõi việc khai thác dữ liệu camera; Biên bản bàn giao dữ liệu camera*) được lưu trữ tại Văn phòng Bộ (đơn vị quản lý, vận hành các Hệ thống camera: Phòng Quản trị, Đại diện Văn phòng Bộ tại thành phố Hồ Chí Minh).

Chương IV

CÁC HÀNH VI BỊ CẤM, XỬ LÝ VI PHẠM

Điều 10. Các hành vi bị cấm

1. Phá hoại, làm hư hỏng vật lý thiết bị của Hệ thống camera, ngắt nguồn điện, ngắt tín hiệu, che khuất ống kính hoặc làm thay đổi cố ý góc quét của camera.

2. Tự ý dò mật khẩu, bẻ khóa hệ thống, reset đầu ghi dữ liệu, xóa nhật ký hệ thống, chia sẻ tài khoản truy cập Hệ thống camera cho người không có trách nhiệm, thẩm quyền; Kết nối trái phép Hệ thống camera vào mạng internet, tự ý



cài đặt các phần mềm xem camera trên máy tính, điện thoại kết nối vào hệ thống.

3. Sử dụng điện thoại thông minh, máy ảnh để quay phim/chụp ảnh lại màn hình giám sát camera.

4. Xóa, sửa đổi, cắt ghép file hình ảnh làm sai lệch bản chất sự thật của dữ liệu gốc.

5. Phát tán dữ liệu hình ảnh, video camera lên không gian mạng hoặc sử dụng vào mục đích xấu xâm phạm bí mật đời tư cá nhân; sử dụng dữ liệu camera làm công cụ để đe dọa, xúc phạm uy tín, tổng tiền, hoặc quấy rối đời tư của người khác.

6. Sử dụng dữ liệu camera ngoài mục đích quy định tại Điều 7; TỰ Ý sao chép dữ liệu sang các thiết bị ngoại vi khác ngoài thiết bị chứa dữ liệu quy định tại khoản 5 Điều 9.

7. Gây cản trở yêu cầu đã được cấp có thẩm quyền phê duyệt về việc xem lại, trích xuất dữ liệu camera.

Điều 11. Hình thức xử lý

1. Cá nhân, tổ chức vi phạm các điều khoản nghiêm cấm thì tùy theo tính chất, mức độ sẽ bị xử lý kỷ luật theo quy định.

2. Trường hợp hành vi vi phạm gây thiệt hại về tài sản phải bồi thường vật chất. Nếu vi phạm luật bảo vệ dữ liệu cá nhân, an ninh mạng, các quy định của pháp luật có liên quan thực hiện theo quy định của pháp luật có liên quan về xử phạt vi phạm hành chính hoặc truy cứu trách nhiệm hình sự theo quy định của pháp luật.

Điều 12. Tổ chức thực hiện

1. Văn phòng Bộ: Chủ trì, phối hợp với các đơn vị có liên quan phổ biến và kiểm tra, giám sát việc thực hiện các quy định của Quy chế này; kịp thời tổng hợp vấn đề vướng mắc của Quy chế cần xem xét sửa đổi, bổ sung báo cáo Lãnh đạo Bộ xem xét, quyết định.

2. Công chức, viên chức, người lao động, các đơn vị làm việc tại trụ sở cơ quan Bộ và các tổ chức, cá nhân có liên quan: Thực hiện quy định tại Quy chế này; phối hợp với Văn phòng Bộ trong việc bảo vệ Hệ thống camera, cung cấp thông tin phục vụ xử lý các vụ việc có liên quan khi có yêu cầu./.

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày tháng năm 2026

PHIẾU ĐỀ NGHỊ XEM/TRÍCH XUẤT DỮ LIỆU CAMERA AN NINH

Kính gửi: Văn phòng Bộ Tài chính

1. Người/đơn vị đề nghị trích xuất:
2. Chức vụ/đơn vị công tác:
3. Lý do yêu cầu trích xuất dữ liệu:
.....
.....
4. Thông tin dữ liệu camera yêu cầu:
 - Vị trí camera :
 - Mốc thời gian cần xem: Từ giờ ngày .../.../... Đến giờ ngày .../.../.....
5. Hình thức khai thác yêu cầu (Xem lại trực tiếp/Sao chép file video):
 - 5.1. Xem lại trực tiếp (không sao chép file hình ảnh, video):
 - 5.2. Xem lại trực tiếp và sao chép file hình ảnh, video:
6. Số phiếu: (Bộ phận tiếp nhận ghi theo thứ tự tại số theo dõi)

Hà Nội, ngày tháng năm....

Ý KIẾN CỦA PHÒNG QUẢN TRỊ

(Ký, ghi rõ họ tên)

NGƯỜI/ĐƠN VỊ ĐỀ NGHỊ

(Ký, ghi rõ họ tên)

Ý KIẾN PHÊ DUYỆT CỦA LÃNH ĐẠO VĂN PHÒNG

(Hoặc người được ủy quyền)

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

SƠ THEO DÕI VIỆC KHAI THÁC DỮ LIỆU CAMERA

STT	Ngày/giờ khai thác	Tên người yêu cầu & Bộ phận	Lý do khai thác	Vị trí camera & Khoảng thời gian	Văn bản/ Phiếu số	Người thực hiện khai thác (Ký)	Người Xem (Ký)	Ghi chú
01								
02								
03								
...								
...								

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày tháng năm 2026

BIÊN BẢN BÀN GIAO DỮ LIỆU CAMERA

Số phiếu đề nghị trích xuất dữ liệu camera an ninh:

Bên bàn giao: Phòng Quản trị/ Đại diện Văn phòng Bộ tại thành phố Hồ Chí Minh

Bên tiếp nhận:

Ngày bàn giao:

Nội dung dữ liệu:

Thời gian trích xuất:

Vị trí camera:

Tên file:

Dung lượng:

Định dạng:

Thiết bị lưu (*ghi nội dung: tên thiết bị; thiết bị đã được kiểm tra an toàn, mã hóa mật khẩu theo quy định về an toàn thông tin của Bộ Tài chính chưa*):

.....(*Bên tiếp nhận dữ liệu*) cam kết sử dụng dữ liệu đúng mục đích, bảo mật theo quy định pháp luật./.

ĐẠI DIỆN BÊN GIAO
(*ký ghi rõ họ tên*)

NGƯỜI CHỨNG KIẾN
(*ký ghi rõ họ tên*)

ĐẠI DIỆN BÊN NHẬN
(*ký ghi rõ họ tên*)