BAN CHẤP HÀNH TRUNG ƯƠNG
VĂN PHÒNG
*
Số 348-QĐ/VPTW

ĐẢNG CỘNG SẢN VIỆT NAM

Hà Nội, ngày 19 tháng 6 năm 2026

QUY ĐỊNH
về Cổng ứng dụng nội bộ của các cơ quan đảng

- Căn cứ Quyết định số 259-QĐ/TW, ngày 24/01/2025 của Bộ Chính trị khoá XIII quy định chức năng, nhiệm vụ, tổ chức bộ máy của Văn phòng Trung ương Đảng;

- Căn cứ Nghị quyết số 57-NQ/TW, ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia;

- Căn cứ Quyết định số 204-QĐ/TW, ngày 29/11/2024 của Ban Bí thư phê duyệt Đề án Chuyển đổi số trong các cơ quan đảng;

- Căn cứ Chỉ thị số 57-CT/TW, ngày 31/12/2025 của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị;

- Căn cứ Luật Bảo vệ bí mật nhà nước số 29/2018/QH14, ngày 15/11/2018; Luật Giao dịch điện tử số 20/2023/QH15, ngày 22/6/2023; Luật An ninh mạng số 116/2025/QH15, ngày 10/12/2025;

- Căn cứ Nghị định số 69/2024/NĐ-CP, ngày 25/6/2024 của Chính phủ quy định về định danh và xác thực điện tử;

- Căn cứ Quy chế số 07-QC/TW, ngày 31/10/2025 của Ban Chấp hành Trung ương Đảng về tổ chức, quản lý, sử dụng và bảo vệ hệ thống mạng máy tính của Đảng;

- Căn cứ Quy định số 347-QĐ/VPTW, ngày 12/6/2026 của Chánh Văn phòng Trung ương Đảng ban hành Quy định về định danh và xác thực điện tử;

- Xét đề nghị của Cục Chuyển đổi số - Cơ yếu.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

1. Quy định này điều chỉnh việc quản lý, vận hành, tích hợp, khai thác và cung cấp dịch vụ số thông qua Cổng ứng dụng nội bộ của các cơ quan đảng (sau

đây gọi tắt là Cổng ứng dụng); bao gồm các nội dung: Quản lý tài khoản truy cập; quy trình tích hợp và gỡ bỏ ứng dụng; xác thực và kiểm soát quyền truy cập; bảo đảm an toàn thông tin; trách nhiệm của các bên liên quan.

2. Cổng ứng dụng vận hành trên hai môi trường mạng

a) Vùng mạng thông tin diện rộng của Đảng (Intranet): Triển khai các ứng dụng tích hợp phục vụ xử lý thông tin theo phạm vi, độ mật được cơ quan có thẩm quyền cho phép theo quy định của Đảng và pháp luật về bảo vệ bí mật nhà nước; bảo đảm theo Quy chế số 07-QC/TW, ngày 31/10/2025 của Ban Chấp hành Trung ương Đảng (sau đây gọi là Quy chế số 07-QC/TW).

b) Vùng mạng Internet (môi trường Internet công cộng): Triển khai các ứng dụng tích hợp phục vụ cán bộ truy cập, khai thác; chỉ sử dụng để xử lý thông tin không có độ mật, bảo đảm theo Quy chế số 07-QC/TW.

Điều 2. Đối tượng áp dụng

Quy định này áp dụng đối với:

1. Cán bộ, công chức, viên chức, người lao động làm việc trong các cơ quan đảng các cấp và đảng viên có khai thác, sử dụng Cổng ứng dụng (sau đây gọi chung là cán bộ).

2. Tổ chức, cá nhân được cấp quyền truy cập vào hệ thống thông tin của cơ quan đảng thông qua Cổng ứng dụng.

3. Các đơn vị phát triển, vận hành và chủ quản ứng dụng nghiệp vụ tích hợp trên Cổng ứng dụng.

4. Các cơ quan nhà nước, Mặt trận Tổ quốc Việt Nam, các tổ chức chính trị - xã hội và các tổ chức khác được cơ quan có thẩm quyền cho phép kết nối, khai thác hoặc thực hiện giao dịch điện tử với các cơ quan đảng qua Cổng ứng dụng.

Điều 3. Giải thích từ ngữ

Trong Quy định này, các từ ngữ dưới đây được hiểu như sau:

1. *Cổng ứng dụng* là hệ thống nền tảng số tập trung của các cơ quan đảng, tích hợp các hệ thống thông tin nghiệp vụ vào một điểm truy cập duy nhất, triển khai trên cả máy tính và thiết bị di động, vận hành tại tên miền chính thức dcs.vn, vận hành trên hai môi trường mạng: Vùng mạng thông tin diện rộng của Đảng (Intranet) và vùng Internet (môi trường Internet công cộng), cho phép cán bộ truy cập theo đúng phân cấp và quyền hạn được giao.

2. *Ứng dụng thành phần (ứng dụng tích hợp)* là các phần mềm, hệ thống thông tin nghiệp vụ được tích hợp vào và hoạt động trong Cổng ứng dụng.

3. *Đơn vị chủ quản ứng dụng* là cơ quan, đơn vị được giao nhiệm vụ chủ đầu tư (tổ chức xây dựng, phát triển phần mềm) chịu trách nhiệm toàn diện về

chất lượng, an toàn thông tin và hiệu quả khai thác của ứng dụng thành phần trên Cổng ứng dụng.

4. *Nhật ký hệ thống* là toàn bộ thông tin được ghi nhận tự động về các thao tác, truy cập, đăng nhập, thay đổi quyền và hoạt động phát sinh trên hệ thống.

5. *Mạng riêng ảo (VPN - Virtual Private Network)* là phương thức kết nối mạng được mã hoá, cho phép cán bộ truy cập Cổng ứng dụng một cách an toàn từ môi trường Internet công cộng.

6. *Chủ quản Cổng ứng dụng* là Cục Chuyển đổi số - Cơ yếu (đơn vị được Văn phòng Trung ương Đảng giao nhiệm vụ là chủ quản Cổng ứng dụng).

(Các thuật ngữ về định danh điện tử, hệ thống định danh tập trung (SSO), VNeID, xác thực đa yếu tố (MFA), tài khoản, đầu mối công nghệ thông tin đơn vị áp dụng theo giải thích tại Quy định về định danh và xác thực điện tử trong hệ thống thông tin của các cơ quan đảng).

Điều 4. Nguyên tắc quản lý và sử dụng Cổng ứng dụng

1. Yêu cầu bảo mật, bảo đảm an toàn thông tin trong khi xử lý thông tin trên Cổng ứng dụng vận hành phải tương ứng với mỗi môi trường mạng hoạt động

a) Đối với vùng mạng thông tin diện rộng của Đảng (Intranet) được triển khai các ứng dụng tích hợp phục vụ xử lý thông tin có độ mật được cơ quan có thẩm quyền cho phép, bảo đảm tuân thủ đầy đủ Quy chế số 07-QC/TW và các quy định của Đảng và pháp luật về bảo vệ bí mật nhà nước.

b) Đối với vùng mạng Internet (môi trường Internet công cộng) chỉ sử dụng để xử lý thông tin thường, không có yêu cầu bảo mật, bảo đảm theo đúng Quy chế số 07-QC/TW.

2. Quản lý định danh, xác thực và quyền truy cập tập trung tại Cổng ứng dụng: Toàn bộ tài khoản cán bộ các cơ quan đảng được quản lý, xác thực thống nhất tại Cổng ứng dụng. Chủ quản Cổng ứng dụng thống nhất quản lý và cấp quyền truy cập vào Cổng ứng dụng; các đơn vị chủ quản ứng dụng không tự tổ chức hệ thống định danh riêng mà thực hiện phân quyền nghiệp vụ nội bộ chi tiết theo vai trò, chức danh, quyền hạn được giao trên cơ sở kế thừa, đồng bộ thông tin định danh, xác thực từ Cổng ứng dụng.

3. Mỗi cán bộ được cấp một tài khoản duy nhất: Mỗi cán bộ chỉ được cấp một tài khoản trên Cổng ứng dụng; trường hợp đảm nhiệm nhiều chức vụ hoặc nhiều vai trò nghiệp vụ thì được cấp một tài khoản duy nhất và được gán nhiều vai trò, quyền hạn tương ứng; việc cấp tài khoản quản trị để thực hiện nhiệm vụ chuyên môn thực hiện theo Quy định số 347-QĐ/VPTW, ngày 12/6/2026 quy định về định danh và xác thực điện tử trong hệ thống thông tin của các cơ quan đảng (sau đây gọi tắt là Quy định 347-QĐ/VPTW).

4. Kiểm soát vòng đời ứng dụng: Mọi ứng dụng phải qua quy trình thẩm định và phê duyệt trước khi đưa lên Cổng ứng dụng; phải thực hiện đúng thủ tục khi tạm dừng hoặc gỡ bỏ.

5. Quyền hạn gắn với nhiệm vụ: Cán bộ chỉ được cấp quyền truy cập đúng với chức danh và nhiệm vụ được giao, không cấp quyền vượt phạm vi cần thiết.

6. Bảo mật nhiều lớp: Áp dụng nhiều biện pháp bảo mật đồng thời, ưu tiên sử dụng VNeID, các tài khoản được tạo trên Cổng ứng dụng phải kết hợp xác thực đa yếu tố (MFA).

7. Ghi nhật ký đầy đủ: Mọi hành vi đăng nhập, truy cập, thay đổi quyền đều được hệ thống ghi lại tự động và lưu trữ để phục vụ kiểm tra khi cần.

8. Tuân thủ pháp luật: Việc quản lý, vận hành và sử dụng hệ thống phải tuân thủ các quy định của Đảng và pháp luật về bảo vệ bí mật nhà nước, an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân.

9. Tích hợp không làm thay đổi thẩm quyền nghiệp vụ: Việc tích hợp ứng dụng lên Cổng ứng dụng không làm thay đổi thẩm quyền quản lý nghiệp vụ, quản lý dữ liệu và trách nhiệm vận hành của đơn vị chủ quản ứng dụng; bảo đảm một lần khai báo, nhiều lần sử dụng dữ liệu; tránh đầu tư trùng lặp, phát sinh nhiều tài khoản và kho dữ liệu riêng lẻ.

Chương II
TÍCH HỢP ỨNG DỤNG THÀNH PHẦN

Điều 5. Nguyên tắc quản lý ứng dụng tích hợp

1. Mọi ứng dụng nghiệp vụ của các cơ quan đảng muốn tích hợp và vận hành trên Cổng ứng dụng phải thực hiện đăng ký, kiểm thử, thẩm định và được phê duyệt trước khi đưa vào vận hành chính thức. Trong đó, cơ quan chủ trì nghiệp vụ là cơ quan có nhu cầu sử dụng, chịu trách nhiệm về yêu cầu và nội dung nghiệp vụ của ứng dụng; cơ quan chủ đầu tư là cơ quan tổ chức đầu tư, xây dựng và triển khai ứng dụng. Việc lập hồ sơ và thực hiện thủ tục theo Điều 7 Quy định này được thực hiện như sau:

a) Đối với ứng dụng do cơ quan, đơn vị khác làm chủ đầu tư.

Cơ quan chủ đầu tư chủ trì, phối hợp với cơ quan chủ trì nghiệp vụ lập hồ sơ đăng ký, gửi chủ quản Cổng ứng dụng thẩm định và phê duyệt theo quy trình quy định tại Điều 7. Trường hợp một cơ quan đồng thời là chủ đầu tư và chủ trì nghiệp vụ, thì thực hiện đầy đủ trách nhiệm của cả cơ quan chủ đầu tư và cơ quan chủ trì nghiệp vụ trong chuẩn bị hồ sơ, gửi đến chủ quản Cổng ứng dụng để thẩm định, phê duyệt.

b) Đối với ứng dụng do chủ quản Cổng ứng dụng làm chủ đầu tư.

Chủ quản Cổng ứng dụng không phải thực hiện thủ tục đề nghị thẩm định, phê duyệt, nhưng phải chủ trì, phối hợp với cơ quan chủ trì nghiệp vụ lập đầy đủ hồ sơ kỹ thuật; tổ chức kiểm thử, đánh giá an toàn thông tin theo quy định tại Điều 7; ban hành quyết định đưa ứng dụng vào vận hành chính thức trên Cổng ứng dụng sau khi có xác nhận của cơ quan chủ trì nghiệp vụ; lưu trữ đầy đủ hồ sơ và cập nhật vào danh mục ứng dụng theo khoản 2 Điều này.

Trường hợp chủ quản Cổng ứng dụng đồng thời là cơ quan chủ trì nghiệp vụ thì thực hiện đầy đủ trách nhiệm của cả cơ quan chủ đầu tư và cơ quan chủ trì nghiệp vụ trong chuẩn bị hồ sơ.

2. Chủ quản Cổng ứng dụng duy trì và công khai trong nội bộ danh mục ứng dụng đang hoạt động, tạm dừng và đã gỡ bỏ trên Cổng ứng dụng.

Điều 6. Điều kiện đưa ứng dụng lên Cổng ứng dụng

Ứng dụng nghiệp vụ được đưa lên Cổng ứng dụng khi đáp ứng đủ các điều kiện sau (không áp dụng với các ứng dụng do chủ quản Cổng ứng dụng trực tiếp làm chủ đầu tư hoặc đóng vai trò đơn vị chủ quản ứng dụng).

1. Được cơ quan có thẩm quyền phê duyệt đầu tư hoặc đặt hàng phát triển, phục vụ hoạt động nghiệp vụ của cơ quan đảng.

2. Đã hoàn thành kiểm thử kỹ thuật và kiểm thử an toàn thông tin đạt yêu cầu.

3. Đơn vị chủ quản ứng dụng đã nộp đủ hồ sơ đề nghị theo quy định tại Điều 7 Quy định này và được phê duyệt.

4. Bảo đảm khả năng kết nối, chia sẻ dữ liệu thông qua giao diện lập trình ứng dụng (API) và nền tảng tích hợp, chia sẻ dữ liệu dùng chung của các cơ quan đảng; tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật về kết nối, tích hợp.

Điều 7. Hồ sơ và quy trình đưa ứng dụng lên Cổng ứng dụng

1. Hồ sơ đề nghị đưa ứng dụng lên Cổng ứng dụng gồm:

a) Văn bản đề nghị của đơn vị chủ quản ứng dụng, có chữ ký của lãnh đạo cơ quan, đơn vị, nêu rõ mục đích, đối tượng cán bộ và phạm vi dữ liệu của ứng dụng.

b) Hồ sơ đề xuất cấp độ an toàn thông tin mạng của ứng dụng đã được cơ quan có thẩm quyền phê duyệt theo quy định; phương án bảo đảm an toàn thông tin theo cấp độ kèm theo; kết quả đánh giá hoặc kiểm tra an toàn thông tin gần nhất của ứng dụng (nếu có).

c) Phương án xử lý dự phòng khi ứng dụng mất kết nối với Cổng ứng dụng.

2. Quy trình xét duyệt

Bước 1 - Nộp hồ sơ: Đơn vị chủ quản ứng dụng nộp hồ sơ đầy đủ theo quy định về chủ quản Cổng ứng dụng.

Bước 2 - Thẩm định hồ sơ: Chủ quản Cổng ứng dụng thẩm định tính đầy đủ, hợp lệ của hồ sơ trong thời hạn 5 ngày làm việc kể từ khi nhận được hồ sơ.

Trường hợp cần bổ sung, thông báo bằng văn bản trong vòng 3 ngày làm việc. Trường hợp hồ sơ hợp lệ, thông báo chấp thuận chủ trương tích hợp bằng văn bản.

Bước 3 - Kiểm thử kỹ thuật đơn vị chủ quản ứng dụng chủ trì tổ chức kiểm thử kỹ thuật và an toàn thông tin đối với ứng dụng đề nghị tích hợp; chủ quản Cổng ứng dụng phối hợp kiểm tra kết nối tích hợp và xác nhận kết quả trong thời hạn 10 ngày làm việc kể từ ngày thông báo chấp thuận.

Bước 4 - Phê duyệt: Trường hợp đạt yêu cầu, chủ quản Cổng ứng dụng ban hành văn bản phê duyệt tích hợp. Đối với các hệ thống thông tin quan trọng, chủ quản Cổng ứng dụng trình lãnh đạo Văn phòng Trung ương Đảng xem xét, phê duyệt.

Bước 5 - Đưa lên Cổng ứng dụng: Sau khi có văn bản phê duyệt, chủ quản Cổng ứng dụng phối hợp với đơn vị chủ quản ứng dụng kết nối chính thức ứng dụng vào Cổng ứng dụng, thiết lập phân quyền và thông báo cho đầu mối công nghệ thông tin đơn vị.

3. Trong thời gian chờ xét duyệt, ứng dụng chỉ được kiểm thử trên môi trường thử nghiệm riêng, không được kết nối vào Cổng ứng dụng chính thức và không được sử dụng dữ liệu thực tế.

Điều 8. Trách nhiệm của đơn vị chủ quản ứng dụng khi ứng dụng đang hoạt động

1. Duy trì đầy đủ các điều kiện kỹ thuật và an toàn thông tin trong suốt thời gian ứng dụng hoạt động trên Cổng ứng dụng. Khi phát hiện lỗ hổng bảo mật phải khắc phục và báo cáo chủ quản Cổng ứng dụng ngay trong ngày làm việc.

2. Mọi thay đổi về chức năng, phạm vi dữ liệu hoặc danh sách cán bộ của ứng dụng phải thông báo cho chủ quản Cổng ứng dụng trước khi thực hiện; những thay đổi ảnh hưởng đến an toàn thông tin phải được chủ quản Cổng ứng dụng chấp thuận bằng văn bản.

3. Bảo đảm dữ liệu phân quyền được đồng bộ theo thời gian thực ngay sau khi quản trị hệ thống lưu cấu hình trên Cổng ứng dụng; trường hợp áp dụng cơ chế đồng bộ định kỳ, thời gian đồng bộ không vượt quá 3 phút kể từ khi lưu cấu hình đến khi ứng dụng thành phần cập nhật thành công.

4. Phối hợp đầy đủ và cung cấp kịp thời tài liệu kỹ thuật khi chủ quản Cổng ứng dụng yêu cầu phục vụ kiểm tra hoặc xử lý sự cố.

5. Định kỳ hằng năm tổ chức rà soát, đánh giá an toàn thông tin của ứng dụng; rà soát danh mục dữ liệu, quyền truy cập và mức độ khai thác dữ liệu của ứng dụng; kịp thời khắc phục các lỗ hổng, nguy cơ mất an toàn thông tin phát sinh trong quá trình vận hành; báo cáo kết quả về chủ quản Cổng ứng dụng.

6. Bảo đảm phân loại dữ liệu, duy trì chế độ sao lưu và kiểm soát việc chia sẻ, kết nối dữ liệu trong quá trình vận hành ứng dụng; khi ứng dụng bị gỡ bỏ, phải xử lý toàn bộ dữ liệu theo quy định.

Điều 9. Quy trình tạm dừng và gỡ bỏ ứng dụng khỏi Cổng ứng dụng

1. Ứng dụng bị tạm dừng ngay lập tức khi:

a) Phát hiện lỗ hổng bảo mật nghiêm trọng hoặc ứng dụng bị tấn công, có nguy cơ lây lan ảnh hưởng đến toàn bộ Cổng ứng dụng.

b) Chủ quản Cổng ứng dụng ra quyết định tạm đình chỉ vì vi phạm nghiêm trọng quy định kỹ thuật hoặc an toàn thông tin.

2. Ứng dụng được gỡ bỏ chính thức khỏi Cổng ứng dụng khi:

a) Đơn vị chủ quản ứng dụng có văn bản đề nghị ngừng cung cấp dịch vụ.

b) Ứng dụng được thay thế bởi hệ thống mới đã được phê duyệt và đưa vào vận hành chính thức.

c) Đơn vị chủ quản ứng dụng bị giải thể hoặc hợp nhất mà không có đơn vị kế thừa.

d) Ứng dụng vi phạm nghiêm trọng Quy định này sau khi đã được nhắc nhở bằng văn bản mà không khắc phục trong thời hạn quy định.

3. Quy trình gỡ bỏ chủ động (đối với trường hợp quy định tại điểm a, điểm b, khoản 2 Điều này)

Bước 1 - Đề nghị: Đơn vị chủ quản ứng dụng gửi văn bản đề nghị gỡ bỏ lên chủ quản Cổng ứng dụng, nêu rõ lý do, thời điểm dự kiến và phương án chuyển tiếp nghiệp vụ, xử lý dữ liệu cho cán bộ.

Bước 2 - Phê duyệt và thông báo: Chủ quản Cổng ứng dụng ban hành quyết định gỡ bỏ; thông báo trên Cổng ứng dụng tối thiểu 15 ngày trước ngày gỡ bỏ chính thức.

Bước 3 - Thực hiện: Gỡ bỏ ứng dụng khỏi Cổng ứng dụng, hoàn tất xử lý và chuyển giao dữ liệu theo quy định; lưu hồ sơ gỡ bỏ tối thiểu 5 năm.

4. Đối với các trường hợp quy định tại điểm c, điểm d, khoản 2 Điều này, chủ quản Cổng ứng dụng lập hồ sơ gỡ bỏ, xác định đơn vị tiếp nhận và phương án xử lý, bàn giao dữ liệu (nếu có), ban hành quyết định gỡ bỏ; thông báo trên Cổng ứng dụng tối thiểu 15 ngày trước ngày gỡ bỏ chính thức; hồ sơ gỡ bỏ được lưu tối thiểu 5 năm.

5. Đơn vị chủ quản ứng dụng có trách nhiệm bảo đảm cán bộ không bị gián đoạn công việc trong quá trình chuyển tiếp và dữ liệu không bị mất khi gỡ bỏ ứng dụng.

Chương III
XÁC THỰC VÀ KIỂM SOÁT TRUY CẬP

Điều 10. Cơ chế xác thực theo môi trường mạng

Mọi truy cập vào Cổng ứng dụng phải xác thực danh tính. Nghiêm cấm truy cập ẩn danh, đăng nhập bằng tài khoản của người khác hoặc truy cập qua

địa chỉ không phải tên miền chính thức dưới bất kỳ hình thức nào. Tuỳ theo môi trường mạng, phương thức xác thực bắt buộc như sau:

1. Vùng mạng thông tin diện rộng của Đảng (Intranet): Cán bộ truy cập qua địa chỉ nội bộ do chủ quản Cổng ứng dụng cấp phát thông qua địa chỉ https://dcs.vn hoặc qua mạng truyền số liệu chuyên dùng; đăng nhập qua cơ chế SSO tập trung một lần và được truy cập tất cả ứng dụng tích hợp đã được phân quyền. Thiết bị truy cập phải được đăng ký và kiểm tra an toàn thông tin trước khi sử dụng. Kênh truyền sử dụng giải pháp bảo mật của Ban Cơ yếu Chính phủ nhằm bảo đảm bí mật, toàn vẹn và xác thực dữ liệu.

2. Vùng mạng Internet (môi trường Internet công cộng): Cán bộ truy cập tại địa chỉ https://dcs.vn hoặc qua App ứng dụng (ICPV). Đối với một số ứng dụng quan trọng, nhạy cảm, chủ quản Cổng ứng dụng quyết định việc bổ sung giải pháp kết nối VPN để tăng mức độ an toàn cho hệ thống và dữ liệu. Ưu tiên xác thực bằng VNeID mức độ 2 trở lên hoặc các phương thức định danh, xác thực điện tử khác được cơ quan có thẩm quyền cho phép sử dụng trong các cơ quan đảng. Đối với tài khoản chưa liên kết VNeID bắt buộc sử dụng xác thực đa yếu tố (MFA) nội bộ. Toàn bộ kết nối phải sử dụng giao thức HTTPS; các kết nối không được mã hoá sẽ bị hệ thống tự động từ chối.

Điều 11. Cơ chế xác thực và kiểm soát quyền truy cập

1. Luồng xác thực cán bộ: Khi truy cập vào ứng dụng thành phần, cán bộ được chuyển hướng tới hệ thống xác thực tập trung SSO của Cổng ứng dụng kèm theo thông tin định danh ứng dụng và địa chỉ nhận phản hồi sau xác thực. Sau khi xác thực thành công, hệ thống SSO cấp mã truy cập và xác nhận thông tin phân quyền để ứng dụng thành phần quyết định việc cấp quyền truy cập. Cán bộ chỉ được phép truy cập, khai thác các chức năng và dữ liệu thuộc phạm vi đơn vị, lĩnh vực công tác, nhiệm vụ được giao và cấp độ bảo mật tương ứng.

2. Phân quyền sử dụng ứng dụng được thực hiện theo hai cấp độ

a) Quyền truy cập vào Cổng ứng dụng: Do chủ quản Cổng ứng dụng phê duyệt và cấp phát trên cơ sở đề nghị của cơ quan, đơn vị hoặc phân cấp, uỷ quyền cho đầu mối công nghệ thông tin đơn vị thực hiện đối với cán bộ thuộc phạm vi quản lý.

b) Quyền nghiệp vụ chi tiết bên trong ứng dụng: Do đơn vị chủ quản ứng dụng trực tiếp cấp phát, phân quyền dựa trên chức danh, nhiệm vụ của người dùng, trên cơ sở kế thừa và đồng bộ thông tin định danh từ Cổng ứng dụng. Việc cấp quyền, điều chỉnh quyền và thu hồi quyền ở cả hai cấp độ phải được lưu vết đầy đủ trên hệ thống để phục vụ kiểm tra, giám sát và truy xuất trách nhiệm.

3. Xử lý khi xác thực thất bại: Sau 5 lần đăng nhập sai liên tiếp, tài khoản bị khoá tạm thời và phải được mở khoá theo Quy định 347-QĐ/VPTW. Mọi xác thực thất bại đều được ghi vào nhật ký hệ thống.

Chương IV
BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 12. Yêu cầu an toàn thông tin đối với hệ thống

1. Cổng ứng dụng phải được xây dựng, vận hành đáp ứng tiêu chuẩn an toàn hệ thống thông tin tối thiểu cấp độ 3 theo quy định của pháp luật; đối với các phân hệ, ứng dụng hoặc cơ sở dữ liệu có yêu cầu bảo vệ cao hơn, đặc biệt là hệ thống xử lý thông tin chứa bí mật nhà nước, phải xác định cấp độ an toàn phù hợp và áp dụng các biện pháp bảo vệ tương ứng theo quy định hiện hành, được cấp có thẩm quyền phê duyệt.

2. Hệ thống phải được triển khai song song tại hai trung tâm dữ liệu (trung tâm chính và trung tâm dự phòng) để bảo đảm hoạt động liên tục và khôi phục nhanh khi có sự cố.

3. Yêu cầu tối thiểu về tính sẵn sàng

a) Hệ thống hoạt động liên tục, ổn định, bảo đảm tính sẵn sàng cao.

b) Khi xảy ra sự cố, hệ thống phải được khôi phục hoạt động trong vòng 4 giờ.

c) Dữ liệu được sao lưu liên tục, thời điểm phục hồi dữ liệu không xa hơn 1 giờ trước thời điểm xảy ra sự cố.

4. Các yêu cầu kỹ thuật và tiêu chuẩn bảo mật cụ thể áp dụng cho Cổng ứng dụng, tên miền dcs.vn và các ứng dụng tích hợp do chủ quản Cổng ứng dụng hướng dẫn.

5. Cổng ứng dụng và các ứng dụng tích hợp phải được kết nối, giám sát tập trung thông qua hệ thống giám sát an toàn thông tin (SOC) của các cơ quan đảng nhằm phát hiện sớm, cảnh báo và xử lý kịp thời các nguy cơ, sự cố an toàn thông tin.

Điều 13. Các hành vi nghiêm cấm

Nghiêm cấm các hành vi sau trong quá trình quản lý, vận hành và sử dụng Cổng ứng dụng

1. Sử dụng tài khoản của người khác hoặc chia sẻ, cho mượn tài khoản cá nhân cho người khác sử dụng dưới bất kỳ hình thức nào.

2. Cố ý truy cập, can thiệp, sửa đổi, xoá dữ liệu trái phép trên hệ thống; xâm nhập trái phép hoặc cố ý phá hoại, làm gián đoạn hoạt động của hệ thống.

3. Sử dụng thiết bị không an toàn để truy cập hệ thống, kết nối thiết bị lưu trữ ngoài (USB, ổ cứng di động) vào thiết bị đang xử lý thông tin có độ mật (trừ thiết bị lưu trữ ngoài chuyên dụng do Ban Cơ yếu Chính phủ cấp phát).

4. Phát tán mã độc, cài đặt phần mềm không được phép; sao chép, chuyển ra ngoài hoặc chia sẻ tài liệu, dữ liệu ngoài phạm vi quyền được giao.

5. Cố tình làm lộ, lọt thông tin bí mật nhà nước, thông tin nội bộ của Đảng hoặc dữ liệu cá nhân.

6. Đưa ứng dụng lên Cổng ứng dụng hoặc gỡ bỏ ứng dụng khỏi Cổng ứng dụng khi chưa có phê duyệt của cơ quan có thẩm quyền.

7. Sử dụng hệ thống cho mục đích không phải công vụ, ngoài phạm vi được phân quyền hoặc trái quy định của Đảng và pháp luật.

8. Xây dựng, vận hành hoặc phát tán đường dẫn giả mạo tên miền dcs.vn nhằm đánh lừa cán bộ hoặc thu thập thông tin đăng nhập trái phép.

9. Tự ý kết nối công cụ, phần mềm, tiện ích mở rộng, API hoặc hệ thống tự động vào Cổng ứng dụng khi chưa được chủ quản Cổng ứng dụng cho phép.

10. Sử dụng công cụ trí tuệ nhân tạo, dịch vụ đám mây công cộng hoặc nền tảng bên thứ ba để xử lý, truyền tải thông tin, dữ liệu trên Cổng ứng dụng khi chưa được cơ quan có thẩm quyền cho phép.

Điều 14. Kiểm tra và giám sát

1. Chủ quản Cổng ứng dụng tổ chức giám sát liên tục hoạt động của Cổng ứng dụng, tự động cảnh báo khi phát hiện các dấu hiệu bất thường như: Đăng nhập thất bại nhiều lần, truy cập khối lượng lớn dữ liệu, đăng nhập ngoài giờ làm việc từ vị trí lạ.

2. Thực hiện kiểm tra an toàn thông tin định kỳ, kiểm tra đột xuất khi có thay đổi về phạm vi dữ liệu, ứng dụng tích hợp hoặc đơn vị vận hành hoặc khi có cảnh báo nguy cơ mất an toàn thông tin từ cơ quan có thẩm quyền hoặc sau mỗi sự cố bảo mật nghiêm trọng.

3. Nhật ký hoạt động hệ thống được lưu trữ tự động, không thể chỉnh sửa hoặc xoá bởi người dùng thông thường, được bảo quản và lưu trữ theo quy định của pháp luật về lưu trữ và an toàn thông tin.

4. Cổng ứng dụng có chức năng kết xuất báo cáo thống kê định kỳ về tình hình sử dụng hệ thống (tần suất, thời lượng truy cập theo nhóm cán bộ, cơ quan, đơn vị) phục vụ công tác quản lý, theo dõi, đánh giá và báo cáo kết quả chuyển đổi số.

Điều 15. Quy trình xử lý sự cố an toàn thông tin

1. Sự cố an toàn thông tin trên Cổng ứng dụng được phân thành ba mức

a) Mức 1 - Nghiêm trọng: Sự cố an toàn thông tin có phạm vi ảnh hưởng đặc biệt lớn, làm mất tính bí mật, tính toàn vẹn hoặc tính sẵn sàng của hệ thống, bao gồm các trường hợp: Hệ thống bị xâm nhập trái phép; dữ liệu quan trọng hoặc bí mật nhà nước bị lộ lọt, bị sửa đổi trái phép; toàn bộ dịch vụ bị ngừng hoạt động. Sự cố Mức 1 phải được kích hoạt quy trình ứng cứu khẩn cấp và báo cáo ngay cấp có thẩm quyền.

b) Mức 2 - Quan trọng: Tài khoản bị chiếm quyền, có người truy cập dữ liệu không được phép hoặc một bộ phận dịch vụ bị gián đoạn.

c) Mức 3 - Thông thường: Cảnh báo phần mềm độc hại, vi phạm quy định sử dụng chưa gây hậu quả trực tiếp.

Tiêu chí phân loại chi tiết theo mức độ tác động đến hoạt động của hệ thống, số lượng cán bộ và phạm vi dữ liệu bị ảnh hưởng thực hiện theo quy định, hướng dẫn của cơ quan có thẩm quyền về ứng cứu, xử lý sự cố an toàn thông tin.

2. Khi phát hiện sự cố, người phát hiện báo cáo ngay cho đầu mối công nghệ thông tin đơn vị, chậm nhất 1 giờ kể từ khi phát hiện; đầu mối công nghệ thông tin đơn vị tiếp nhận, xử lý ban đầu và báo cáo chủ quản Cổng ứng dụng chậm nhất 1 giờ tiếp theo. Đối với sự cố Mức 1, người phát hiện và đầu mối công nghệ thông tin đơn vị báo cáo ngay bằng phương tiện liên lạc nhanh nhất, đồng thời tiến hành các biện pháp xử lý ban đầu theo quy định.

3. Chủ quản Cổng ứng dụng chủ trì điều tra, xác định nguyên nhân và phối hợp khắc phục. Đối với sự cố Mức 1, báo cáo ngay lãnh đạo Văn phòng Trung ương Đảng và phối hợp với các cơ quan, đơn vị liên quan xử lý khắc phục sự cố.

4. Trong vòng 7 ngày làm việc kể từ khi khắc phục xong sự cố, chủ quản Cổng ứng dụng phải hoàn thành báo cáo đầy đủ: Nguyên nhân, phạm vi ảnh hưởng, biện pháp khắc phục và các biện pháp phòng ngừa tái diễn.

Chương V
TRÁCH NHIỆM CỦA CÁC BÊN

Điều 16. Trách nhiệm của cán bộ

1. Giữ bí mật tuyệt đối mật khẩu và thông tin đăng nhập tài khoản; không cung cấp, cho mượn, chia sẻ hoặc nhờ người khác đăng nhập thay dưới bất kỳ hình thức nào. Chịu trách nhiệm về mọi hành động thực hiện trên hệ thống dưới tên tài khoản của mình.

2. Đổi mật khẩu ngay khi nhận tài khoản lần đầu, liên kết với VNeID và bật xác thực đa yếu tố (MFA) theo hướng dẫn của đơn vị.

3. Đăng xuất khỏi hệ thống ngay sau khi làm xong việc, đặc biệt trên thiết bị dùng chung hoặc khi rời khỏi nơi làm việc.

4. Báo cáo ngay cho đầu mối công nghệ thông tin đơn vị, chậm nhất 1 giờ, khi phát hiện tài khoản bị đăng nhập trái phép, mật khẩu bị lộ hoặc có dấu hiệu bị chiếm quyền sử dụng.

5. Chỉ sử dụng Cổng ứng dụng để thực hiện công việc được giao, không sử dụng vào mục đích cá nhân, thương mại hoặc trái quy định của Đảng và pháp luật.

6. Sử dụng kết nối VPN theo quy định khi truy cập Cổng ứng dụng từ môi trường Internet; kiểm tra địa chỉ truy cập trước khi đăng nhập, bảo đảm đúng tên miền chính thức dcs.vn và kết nối có biểu tượng khoá bảo mật (HTTPS). Không đăng nhập khi phát hiện cảnh báo chứng chỉ không hợp lệ hoặc địa chỉ đáng ngờ.

7. Được hỗ trợ kỹ thuật và hướng dẫn sử dụng khi có yêu cầu; được phản ánh, kiến nghị về các bất cập kỹ thuật hoặc quy trình sử dụng hệ thống.

Điều 17. Trách nhiệm của đơn vị quản lý nhân sự

1. Thông báo bằng văn bản hoặc bằng hình thức điện tử trên môi trường số (kèm theo tài liệu minh chứng nếu có) cho đầu mối công nghệ thông tin đơn vị trong vòng 2 ngày làm việc khi có thay đổi nhân sự liên quan đến việc cấp, điều chỉnh hoặc thu hồi tài khoản; riêng trường hợp phải vô hiệu hoá tài khoản, thông báo ngay khi có quyết định hoặc phát sinh sự kiện, chậm nhất trong ngày làm việc cuối cùng của cán bộ.

2. Lập danh sách và ký xác nhận cán bộ đề nghị cấp tài khoản; chịu trách nhiệm về tính chính xác của thông tin.

3. Phối hợp với đầu mối công nghệ thông tin đơn vị rà soát định kỳ danh sách tài khoản, bảo đảm khớp với danh sách nhân sự thực tế.

Điều 18. Trách nhiệm của đầu mối công nghệ thông tin đơn vị

1. Thực hiện cấp phát, điều chỉnh và vô hiệu hoá tài khoản cán bộ thuộc đơn vị theo phân cấp, uỷ quyền của chủ quản Cổng ứng dụng và đúng quy trình tại Quy định này.

2. Tiếp nhận và xử lý ban đầu các yêu cầu, sự cố liên quan đến tài khoản của đơn vị; báo cáo chủ quản Cổng ứng dụng chậm nhất 1 giờ khi xảy ra sự cố bảo mật, theo quy trình tại Điều 15 Quy định này.

3. Rà soát định kỳ 6 tháng một lần danh sách tài khoản đang hoạt động, đối chiếu với thực tế nhân sự; đề xuất vô hiệu hoá tài khoản không còn phù hợp theo hướng dẫn của chủ quản Cổng ứng dụng.

4. Hướng dẫn cán bộ thuộc đơn vị về cách sử dụng hệ thống và các quy định an toàn thông tin cần thiết.

5. Lưu trữ đầy đủ hồ sơ cấp phát và điều chỉnh tài khoản theo quy định lưu trữ.

Điều 19. Trách nhiệm của đơn vị chủ quản ứng dụng

1. Tuân thủ đầy đủ quy trình đăng ký, thẩm định và phê duyệt trước khi đưa ứng dụng lên Cổng ứng dụng; chịu trách nhiệm về chất lượng kỹ thuật và an toàn thông tin của ứng dụng trong suốt thời gian vận hành.

2. Thực hiện đúng quy trình tạm dừng và gỡ bỏ ứng dụng theo Điều 9 Quy định này, bảo đảm quyền lợi của cán bộ trong quá trình chuyển tiếp.

3. Kịp thời xử lý các sự cố kỹ thuật, lỗ hổng bảo mật của ứng dụng và báo cáo chủ quản Cổng ứng dụng.

Điều 20. Trách nhiệm của chủ quản Cổng ứng dụng

1. Chủ trì quản lý toàn bộ hoạt động vận hành, bảo đảm an toàn thông tin và phát triển Cổng ứng dụng.

2. Thẩm định, phê duyệt và quản lý danh mục ứng dụng tích hợp trên Cổng ứng dụng; quyết định tạm dừng hoặc gỡ bỏ ứng dụng vi phạm quy định.

3. Phối hợp với Bộ Công an tích hợp VNeID; phối hợp với Ban Cơ yếu Chính phủ quản lý chứng thư số trên mạng thông tin diện rộng của Đảng.

4. Quản lý tên miền dcs.vn và các tên miền phụ: Đăng ký, gia hạn, bảo vệ tên miền; duy trì hiệu lực chứng chỉ SSL/TLS; triển khai các giải pháp bảo mật DNS và giao thức bảo mật kênh truyền theo tiêu chuẩn kỹ thuật do cơ quan có thẩm quyền quy định; công bố và cập nhật danh sách tên miền phụ chính thức cho các đơn vị và cán bộ biết. Xử lý kịp thời các trường hợp giả mạo tên miền dcs.vn được phát hiện.

5. Tổ chức tập huấn, hướng dẫn sử dụng cho đầu mối công nghệ thông tin và cán bộ các cơ quan đảng; hỗ trợ kỹ thuật trong quá trình triển khai.

Điều 21. Trách nhiệm của lãnh đạo các cơ quan đảng

1. Chỉ đạo triển khai Quy định này tại đơn vị, quán triệt đến toàn thể cán bộ trước khi đưa Cổng ứng dụng vào sử dụng.

2. Bảo đảm bố trí đủ nhân sự, kinh phí và các điều kiện cần thiết để thực hiện Quy định này.

3. Chỉ đạo việc cấp tài khoản, định danh điện tử và quản lý; bảo đảm 100% cán bộ thuộc phạm vi quản lý được cấp tài khoản và liên kết VNeID theo đúng lộ trình; thường xuyên chỉ đạo việc rà soát, cập nhật tài khoản theo hướng dẫn của chủ quản Cổng ứng dụng.

4. Xử lý kỷ luật theo quy định của Đảng và pháp luật đối với cán bộ vi phạm Quy định này, đặc biệt các vi phạm gây mất an toàn thông tin hoặc lộ lọt bí mật của Đảng.

5. Tạo điều kiện thuận lợi cho công tác kiểm tra, giám sát hệ thống do chủ quản Cổng ứng dụng và cơ quan có thẩm quyền tiến hành.

6. Kiểm tra, giám sát việc sử dụng tài khoản, quản lý dữ liệu và việc chấp hành các quy định về an toàn thông tin tại cơ quan, đơn vị theo trách nhiệm của người đứng đầu.

Chương VI
XỬ LÝ VI PHẠM

Điều 22. Xử lý vi phạm

Tổ chức, cá nhân vi phạm Quy định này, nhất là các hành vi nghiêm cấm quy định tại Điều 13, tuỳ tính chất và mức độ vi phạm, bị xử lý theo quy định kỷ luật của Đảng, pháp luật về cán bộ, công chức và pháp luật về an toàn thông tin mạng, an ninh mạng.

Chương VII
ĐIỀU KHOẢN THI HÀNH

Điều 23. Hiệu lực thi hành

Quy định này có hiệu lực kể từ ngày ký qpuyết định ban hành và thay thế các quy định trước đây của Văn phòng Trung ương Đảng về quản lý, vận hành và sử dụng Cổng ứng dụng nội bộ của các cơ quan đảng.

Điều 24. Tổ chức thực hiện

1. Chủ quản Cổng ứng dụng chủ trì hướng dẫn, hỗ trợ kỹ thuật các cơ quan, tổ chức thực hiện Quy định này.

2. Lãnh đạo các ban, cơ quan đảng Trung ương căn cứ chức năng, nhiệm vụ được giao tổ chức triển khai thực hiện Quy định này.

3. Các đảng uỷ, tỉnh uỷ, thành uỷ trực thuộc Trung ương tổ chức triển khai thực hiện Quy định này theo thẩm quyền và phạm vi quản lý.

4. Trong quá trình triển khai, thực hiện, trường hợp phát sinh khó khăn, vướng mắc, các cơ quan, tổ chức phản ánh về chủ quản Cổng ứng dụng để tổng hợp, báo cáo lãnh đạo Văn phòng Trung ương Đảng xem xét, quyết định.

Nơi nhận:
- Các cơ quan đảng ở Trung ương;
- Các đảng uỷ trực thuộc Trung ương;
- Các tỉnh uỷ, thành uỷ;
- Đồng chí Chánh Văn phòng Trung ương Đảng (để báo cáo);
- Cục Chuyển đổi số - Cơ yếu;
- Lưu Văn phòng Trung ương Đảng.

K/T CHÁNH VĂN PHÒNG
PHÓ CHÁNH VĂN PHÒNG

ĐẢNG CỘNG SẢN VIỆT NAM
VĂN PHÒNG TRUNG ƯƠNG
BAN CHẤP HÀNH TRUNG ƯƠNG

Võ Thành Hưng