CHANGE AND RELEASE MANAGEMENT POLICY

CHÍNH SÁCH QUẢN LÝ THAY ĐỔI VÀ PHÁT HÀNH

Right-Sized Approval • Every Release Reversible • No Surprise Freezes

Tổ chức / Organization	[Tên tổ chức]
Chủ sở hữu / Document Owner	Release Manager / Head of DevOps
Phê duyệt / Approved by	Engineering Governance Council
Ngày hiệu lực / Effective Date	[DD/MM/YYYY]
Phiên bản / Version	1.0
Chu kỳ rà soát / Review Cycle	Hằng năm, hoặc ngay khi có thay đổi đáng kể về mô hình phát hành
Tài liệu cấp trên / Parent Documents	Engineering Constitution v1.0 (Tầng 1); Software Development Governance Policy v1.0 (Tầng 2)
Phân loại / Classification	INTERNAL

SAMPLE DOCUMENT

A. Kiểm soát tài liệu

DOCUMENT CONTROL

Phiên bản	Ngày	Người soạn	Mô tả thay đổi
1.0	[DD/MM/YYYY]	[Tên / Vai trò]	Ban hành lần đầu

B. Mục lục nội dung

CONTENTS

- 1. Mục đích
- 2. Phạm vi áp dụng
- 3. Liên kết với Engineering Constitution
- 4. Định nghĩa
- 5. Yêu cầu bắt buộc
- 6. Vai trò và trách nhiệm
- 7. Đo lường tuân thủ
- 8. Cơ chế ngoại lệ
- 9. Không tuân thủ
- 10. Chủ sở hữu tài liệu và chu kỳ rà soát
- 11. Tài liệu liên quan
- 12. Phê duyệt

1. Mục đích

PURPOSE

1. Bảo đảm mọi thay đổi đưa vào môi trường production được thực hiện với mức độ kiểm soát tương xứng với rủi ro của thay đổi đó — không quá lỏng lẻo gây sự cố, không quá nặng nề làm chậm nhịp độ phát hành.
2. Mở rộng chi tiết các nguyên tắc kiểm soát thay đổi và thay đổi nhỏ/có thể đảo ngược đã nêu tại Software Development Governance Policy (SDGP), Điều 5.4 và Điều 5.7, thành một quy trình phân loại thay đổi, phê duyệt, versioning, rollback và freeze window cụ thể, áp dụng thống nhất cho toàn tổ chức.
3. Bảo đảm mọi bản phát hành (release) production đều có thể truy vết, có phương án thu hồi, và được đo lường sức khỏe bằng các chỉ số vận hành khách quan.

Chính sách này bổ sung cho SDGP, không thay thế — các yêu cầu về SDLC, vai trò, cơ chế ngoại lệ và không tuân thủ tại SDGP vẫn áp dụng đầy đủ.

2. Phạm vi áp dụng

SCOPE

- Áp dụng cho mọi thay đổi (change) đưa vào môi trường production hoặc môi trường có ảnh hưởng trực tiếp đến người dùng/khách hàng: triển khai mã nguồn mới, thay đổi cấu hình, thay đổi hạ tầng (kể cả Infrastructure as Code), thay đổi dữ liệu quy mô lớn, và thay đổi quyền truy cập hệ thống production.
- Áp dụng cho mọi thành phần phần mềm/dịch vụ do tổ chức vận hành, không phân biệt mô hình phát hành (liên tục/continuous deployment hay theo lịch/scheduled release).
- Không áp dụng cho thay đổi trong môi trường phát triển/kiểm thử nội bộ (dev/test) chưa ảnh hưởng đến người dùng thật — các môi trường này vẫn tuân theo SDLC tại SDGP Điều 5.1.

3. Liên kết với Engineering Constitution

ALIGNMENT WITH THE CONSTITUTION

Yêu cầu trong Policy	Nguyên tắc Constitution tương ứng
5.1 Phân loại thay đổi theo rủi ro	Điều 4 — Segregation of Duties; Điều 7 — Small, Reversible Changes
5.2 Phê duyệt tương xứng rủi ro	Điều 4 — Segregation of Duties
5.3 Versioning và release note	Điều 6 — Observable and Operable by Default; Điều 8 — Evidence over Opinion
5.4 Rollback/roll-forward bắt buộc	Điều 7 — Small, Reversible Changes
5.5 Freeze window	Điều 1 — Business Value First; Điều 7 — Small, Reversible Changes
5.6 Rà soát sau triển khai cho Emergency Change	Điều 8 — Evidence over Opinion

5.7 Đo lường bằng DORA metrics	Điều 8 — Evidence over Opinion; Điều 10 — Continuous Learning

4. Định nghĩa

DEFINITIONS

- **Thay đổi (Change):** việc thêm, sửa hoặc loại bỏ bất kỳ thành phần nào có thể ảnh hưởng đến dịch vụ production, bao gồm mã nguồn, cấu hình, hạ tầng hoặc dữ liệu.
- **Standard Change (Thay đổi chuẩn/tiền phê duyệt):** thay đổi có rủi ro thấp, lặp lại thường xuyên, quy trình thực hiện đã được xác định và kiểm chứng trước, do đó được phê duyệt trước một lần cho toàn bộ các lần thực hiện tương tự sau này (không cần phê duyệt riêng lẻ từng lần). Đây là một trong ba loại thay đổi theo thực hành "Change Enablement" của ITIL 4 (tên gọi hiện hành thay cho "Change Management" của ITIL v3 trước đây).
- **Normal Change (Thay đổi thường):** thay đổi không đủ điều kiện là Standard Change, cần được đánh giá rủi ro và phê duyệt theo mức độ khẩn cấp, mức độ phức tạp và mức ảnh hưởng cụ thể của từng lần thay đổi trước khi triển khai (theo Điều 5.2).
- **Emergency Change (Thay đổi khẩn cấp):** thay đổi khẩn cấp, ngoài kế hoạch, cần triển khai ngay để khắc phục sự cố đang ảnh hưởng hoặc có nguy cơ cận kề ảnh hưởng nghiêm trọng đến dịch vụ, đến mức không thể chờ hoàn tất quy trình phê duyệt thông thường trước khi triển khai.
- **Semantic Versioning (SemVer 2.0.0):** quy ước đánh số phiên bản công khai theo semver.org, dạng MAJOR.MINOR.PATCH (X.Y.Z là các số nguyên không âm), trong đó MAJOR tăng khi có thay đổi không tương thích ngược (breaking change) với API công khai, MINOR tăng khi bổ sung chức năng vẫn tương thích ngược, PATCH tăng khi sửa lỗi vẫn tương thích ngược; khi MAJOR tăng thì MINOR và PATCH phải đặt lại về 0, khi MINOR tăng thì PATCH phải đặt lại về 0. Một phiên bản đã phát hành thì nội dung của phiên bản đó không được sửa đổi lại (immutable).
- **Freeze Window (Giai đoạn tạm dừng thay đổi):** khoảng thời gian được xác định trước, trong đó thay đổi rủi ro cao vào production bị hạn chế hoặc cấm, nhằm bảo vệ sự ổn định của hệ thống trong giai đoạn nhạy cảm về kinh doanh hoặc vận hành.
- **Rollback:** đưa hệ thống trở lại trạng thái/phiên bản hoạt động ổn định trước khi thay đổi được triển khai.
- **Roll-forward:** khắc phục sự cố do một thay đổi gây ra bằng cách triển khai tiếp một bản sửa lỗi, thay vì quay lại phiên bản cũ.
- **DORA metrics:** các chỉ số đo hiệu năng chuyển giao phần mềm do nghiên cứu DevOps Research and Assessment (DORA)/Accelerate xác định, đã được dùng thống nhất trong bài viết gốc của khung quản trị này: lead time for change (thời gian từ khi commit đến khi chạy production), deployment frequency (tần suất triển khai), change failure rate (tỷ lệ thay đổi gây sự cố), và mean time to restore — MTTR (thời gian trung bình khôi phục dịch vụ sau sự cố).

5. Yêu cầu bắt buộc

MANDATORY REQUIREMENTS

5.1 Phân loại thay đổi theo rủi ro

1. Mọi thay đổi đưa vào production **PHẢI (MUST)** được phân loại vào một trong ba nhóm trước khi triển khai: Standard, Normal, hoặc Emergency (định nghĩa tại Điều 4).
2. Một thay đổi chỉ được xếp vào nhóm Standard khi thỏa đồng thời: (a) đã từng được thực hiện thành công nhiều lần trước đó theo đúng một quy trình cố định, (b) rủi ro thất bại và mức ảnh hưởng nếu thất bại đều thấp, (c) có phương án rollback đã kiểm chứng. Danh mục thay đổi Standard **PHẢI (MUST)** được rà soát định kỳ và có thể bị rút khỏi danh mục nếu phát sinh sự cố liên quan.
3. Thay đổi không đáp ứng điều kiện Standard nhưng chưa đến mức khẩn cấp được xử lý theo nhóm Normal, với mức độ phê duyệt theo Điều 5.2.
4. Việc xếp một thay đổi vào nhóm Emergency **KHÔNG ĐƯỢC PHÉP (MUST NOT)** được dùng như cách né tránh quy trình phê duyệt thông thường khi tình huống không thực sự khẩn cấp; nghi vấn lạm dụng được xử lý theo Điều 5.6 và SDGP Điều 9.

5.2 Phê duyệt tương xứng rủi ro

1. Tổ chức áp dụng mô hình phê duyệt tương xứng rủi ro (risk-based approval) thay vì bắt buộc mọi thay đổi phải qua một hội đồng xét duyệt thay đổi (Change Advisory Board — CAB) cố định, nặng nề cho mọi loại thay đổi — mức độ rà soát tăng dần theo mức ảnh hưởng và khả năng đảo ngược của thay đổi.
2. Lựa chọn này dựa trên nghiên cứu DORA về năng lực "Streamlining Change Approval": tổ chức có quy trình phê duyệt tập trung bởi một hội đồng/cấp quản lý bên ngoài đội thực hiện thay đổi có xu hướng lead time dài hơn, tần suất triển khai thấp hơn (do dồn thành lô lớn), trong khi KHÔNG có bằng chứng cho thấy cách làm đó giúp giảm tỷ lệ thay đổi gây lỗi so với việc kết hợp peer review trong quá trình phát triển với tự động hóa kiểm thử/tích hợp/giám sát.
3. Thay đổi Standard **ĐƯỢC PHÉP (MAY)** tự động phê duyệt và triển khai qua pipeline CI/CD khi đã vượt qua các cổng kiểm soát tự động (kiểm thử, quét bảo mật) quy định tại SDGP Điều 5.5, không cần phê duyệt thủ công riêng lẻ từng lần.
4. Thay đổi Normal **PHẢI (MUST)** được ít nhất một người có thẩm quyền, độc lập với người thực hiện thay đổi, phê duyệt trước khi triển khai — theo đúng nguyên tắc phân tách trách nhiệm tại SDGP Điều 5.4. Với thay đổi có mức ảnh hưởng cao (nhiều hệ thống, nhiều người dùng, hoặc khó đảo ngược), tổ chức **NÊN (SHOULD)** yêu cầu thêm rà soát của một nhóm liên chức năng (ví dụ đại diện vận hành, bảo mật) trước khi phê duyệt.
5. Emergency Change **ĐƯỢC PHÉP (MAY)** được triển khai trước, với phê duyệt tối thiểu của một người có thẩm quyền tại thời điểm xử lý sự cố (ví dụ người trực on-call cấp quản lý), và **PHẢI (MUST)** được phê duyệt/rà soát hồi tố đầy đủ ngay sau đó theo Điều 5.6.
6. Tổ chức **NÊN (SHOULD)** định kỳ rà soát và tinh giản danh mục thay đổi cần phê duyệt thủ công, nhằm tránh hội đồng xét duyệt trở thành nút thắt cổ chai cho nhịp độ phát hành liên tục.

5.3 Versioning và release note

1. Các thành phần/dịch vụ có API công khai hoặc được tiêu thụ bởi hệ thống khác **PHẢI (MUST)** đánh số phiên bản theo quy ước Semantic Versioning (MAJOR.MINOR.PATCH) như định nghĩa tại Điều 4.

2. Thay đổi không tương thích ngược đối với một API công khai **PHẢI (MUST)** tăng số MAJOR và được công bố trước cho các bên tiêu thụ theo thời hạn hợp lý, trừ trường hợp khắc phục lỗ hổng bảo mật khẩn cấp.
3. Mỗi bản phát hành production **PHẢI (MUST)** có release note ghi nhận tối thiểu: nội dung thay đổi chính, mức ảnh hưởng, và (nếu có) hướng dẫn dành cho bên tiêu thụ API khi có breaking change.
4. Một phiên bản đã công bố (đã gắn tag/publish) **KHÔNG ĐƯỢC PHÉP (MUST NOT)** bị sửa đổi nội dung mà không đổi số phiên bản, theo đúng nguyên tắc bất biến (immutability) của Semantic Versioning tại Điều 4 — nếu cần sửa, phải phát hành phiên bản PATCH/MINOR/MAJOR mới tương ứng.

5.4 Rollback và roll-forward

1. Mọi thay đổi production **PHẢI (MUST)** có phương án rollback hoặc roll-forward được xác định trước khi triển khai, kế thừa nguyên tắc thay đổi nhỏ, có thể đảo ngược tại SDGP Điều 5.7.
2. Thay đổi không thể đảo ngược hoàn toàn bằng kỹ thuật (ví dụ một số migration dữ liệu một chiều) chỉ được triển khai khi có kế hoạch giảm thiểu rủi ro thay thế (ví dụ sao lưu đầy đủ trước khi chạy, triển khai theo giai đoạn có thể dừng giữa chừng) và được phê duyệt như một ngoại lệ theo SDGP Điều 8. Với thay đổi cấu trúc cơ sở dữ liệu, đội dự án **NÊN (SHOULD)** ưu tiên kỹ thuật thay đổi theo từng bước tương thích ngược (ví dụ mẫu "expand/contract": mở rộng schema trước, chuyển dữ liệu, rồi mới thu gọn schema cũ ở một thay đổi sau) để mã nguồn có thể rollback độc lập mà không kéo theo rollback dữ liệu.
3. Người phê duyệt thay đổi theo Điều 5.2 **PHẢI (MUST)** xác nhận phương án rollback/roll-forward đã được xác định là một điều kiện phê duyệt, không phê duyệt thay đổi thiếu phương án này trừ trường hợp đã có ngoại lệ hợp lệ.

5.5 Freeze window (giai đoạn tạm dừng thay đổi)

1. Tổ chức **ĐƯỢC PHÉP (MAY)** thiết lập freeze window — giai đoạn tạm dừng các thay đổi rủi ro cao vào production — trước các sự kiện kinh doanh quan trọng (ví dụ đợt khuyến mãi lớn, ra mắt sản phẩm), trong các mốc vận hành nhạy cảm (ví dụ cuối kỳ tài chính, cao điểm giao dịch), hoặc theo yêu cầu của lãnh đạo vận hành.
2. Freeze window **PHẢI (MUST)** được công bố trước cho toàn bộ đội ngũ liên quan, nêu rõ thời gian bắt đầu/kết thúc và phạm vi thay đổi bị hạn chế.
3. Trong thời gian freeze, thay đổi Standard rủi ro thấp và thay đổi khắc phục sự cố (theo cơ chế Emergency Change tại Điều 5.1 và 5.2) **VẪN ĐƯỢC PHÉP (MAY)** thực hiện; các thay đổi Normal khác chỉ được triển khai khi có phê duyệt ngoại lệ riêng cho giai đoạn freeze từ cấp lãnh đạo phù hợp. Với hệ thống có dùng cơ chế bật/tắt tính năng (feature flag), việc triển khai mã nguồn ở trạng thái tắt (chưa hiển thị với người dùng) **ĐƯỢC PHÉP (MAY)** tiếp tục trong giai đoạn freeze và chỉ cần xin phê duyệt riêng khi bật tính năng đó cho người dùng.
4. Freeze window **KHÔNG ĐƯỢC PHÉP (MUST NOT)** được dùng để trì hoãn vô thời hạn các bản vá bảo mật khẩn cấp.

5.6 Rà soát sau triển khai đối với Emergency Change

1. Mọi Emergency Change **PHẢI (MUST)** được rà soát sau triển khai (post-implementation review) trong một thời hạn ngắn xác định sau khi triển khai (ví dụ trong vòng một số ngày làm việc do đội ngũ vận hành quy định cụ thể), nhằm xác nhận: thay đổi thực sự cần thiết ở mức khẩn cấp, thay đổi đã đạt hiệu quả khắc phục sự cố, và không phát sinh rủi ro mới cần xử lý.

2. Kết quả rà soát **PHẢI (MUST)** được ghi nhận lại, bao gồm cả trường hợp phát hiện việc phân loại Emergency là không phù hợp — trường hợp này được xử lý theo cơ chế cải tiến liên tục tại SDGP Điều 5.13, không nhằm mục đích quy trách nhiệm cá nhân trừ khi có dấu hiệu cố ý lạm dụng.
3. Tần suất Emergency Change và tỷ lệ Emergency Change bị đánh giá là phân loại không phù hợp khi rà soát **NÊN (SHOULD)** được báo cáo định kỳ cho Engineering Governance Council như một chỉ số sức khỏe của chính sách này.

5.7 Đo lường bằng DORA metrics

1. Tổ chức **NÊN (SHOULD)** theo dõi bốn chỉ số DORA (định nghĩa tại Điều 4, nhất quán với các chỉ số đã nêu trong bài viết giới thiệu khung quản trị) làm thước đo sức khỏe tổng thể của quy trình quản lý thay đổi và phát hành: lead time for change, deployment frequency, change failure rate, và mean time to restore (MTTR).
2. Change failure rate và mean time to restore **NÊN (SHOULD)** được đối chiếu định kỳ với tỷ lệ và thời gian xử lý Emergency Change tại Điều 5.6, nhằm phát hiện sớm xu hướng suy giảm chất lượng thay đổi.
3. Các chỉ số DORA của tổ chức **NÊN (SHOULD)** được xem xét cùng đo lường tuân thủ tại Điều 7 của Policy này khi đánh giá hiệu quả tổng thể của mô hình phê duyệt tương xứng rủi ro tại Điều 5.2.

> **Không lặp lại nội dung của SDGP:** Các yêu cầu về SDLC, vai trò tổng quát, cơ chế ngoại lệ và không tuân thủ đã quy định đầy đủ tại SDGP. Policy này chỉ bổ sung phần đặc thù của quản lý thay đổi và phát hành; khi có xung đột hoặc trùng lặp diễn giải, bản quy định tại SDGP được ưu tiên áp dụng cho phần chung.

6. Vai trò và trách nhiệm

ROLES & RESPONSIBILITIES

- **Release Manager / Head of DevOps (Document Owner):** sở hữu chính sách; sở hữu và duy trì danh mục thay đổi Standard; quyết định thiết lập freeze window.
- **Người phê duyệt thay đổi (Change Approver):** cá nhân có thẩm quyền được chỉ định để phê duyệt thay đổi Normal/Emergency theo Điều 5.2, độc lập với người thực hiện thay đổi.
- **Đội ngũ vận hành/On-call:** thực hiện và phê duyệt tại chỗ Emergency Change; khởi tạo rà soát sau triển khai theo Điều 5.6.
- **Kỹ sư/Engineering Teams:** phân loại đúng thay đổi mình đề xuất, chuẩn bị phương án rollback/roll-forward, tuân thủ freeze window.
- **Engineering Governance Council:** phê duyệt sửa đổi Policy này; nhận báo cáo định kỳ về DORA metrics và tỷ lệ Emergency Change.

7. Đo lường tuân thủ

COMPLIANCE MEASUREMENT

- Tỷ lệ thay đổi được phân loại đúng nhóm (Standard/Normal/Emergency) trước khi triển khai.
- Tỷ lệ thay đổi Normal có phê duyệt độc lập đầy đủ trước khi triển khai.
- Tỷ lệ thay đổi production có phương án rollback/roll-forward được xác định trước khi triển khai.
- Tỷ lệ Emergency Change hoàn thành rà soát sau triển khai đúng thời hạn.
- Bốn chỉ số DORA (lead time for change, deployment frequency, change failure rate, mean time to restore) theo Điều 5.7.
- Số lần vi phạm freeze window không có phê duyệt ngoại lệ hợp lệ.

8. Cơ chế ngoại lệ

EXCEPTIONS

Áp dụng theo đúng cơ chế và giới hạn tại Engineering Constitution, Điều 8 và SDGP, Điều 8.

9. Không tuân thủ

NON-COMPLIANCE

Áp dụng theo đúng nguyên tắc tại SDGP, Điều 9: báo cáo và khắc phục cho vi phạm thông thường; chỉ xem xét kỷ luật lao động — qua HR/Pháp chế, theo Nội quy lao động — đối với hành vi cố ý (ví dụ: cố tình phân loại thay đổi là Emergency để né phê duyệt thông thường khi không thực sự khẩn cấp, hoặc triển khai thay đổi rủi ro cao trong freeze window mà không có ngoại lệ hợp lệ).

10. Chủ sở hữu tài liệu và chu kỳ rà soát

DOCUMENT OWNERSHIP & REVIEW CYCLE

Document Owner: Release Manager / Head of DevOps. Chu kỳ rà soát: hằng năm, hoặc ngay khi có thay đổi đáng kể về mô hình phát hành (ví dụ chuyển sang continuous deployment quy mô lớn hơn) hoặc sau sự cố nghiêm trọng liên quan đến quy trình thay đổi.

11. Tài liệu liên quan

RELATED DOCUMENTS

- Engineering Constitution v1.0, Software Development Governance Policy v1.0 (Tầng 1-2)
- CI/CD Standard, Incident Management Standard (Tầng 3)
- Change Management Procedure, Emergency Change Procedure, Release Checklist (Tầng 4/5)

Không có thay đổi nào lên production mà không biết cách quay lại;
rủi ro thấp thì tin vào pipeline, rủi ro cao mới cần người dừng lại rà soát;
"khẩn cấp" là một tình huống thật, không phải một lối tắt quen dùng;
và freeze window bảo vệ khách hàng, không phải bảo vệ sự trì trệ.

12. Phê duyệt

APPROVAL

Vai trò	Họ tên	Chữ ký	Ngày
Chair, Engineering Governance Council			
Chief Technology Officer			
Release Manager / Head of DevOps (Document Owner)			
Head of Site Reliability / Operations			