

## CÔNG TY CỔ PHẦN CÔNG NGHỆ ABC

# HƯỚNG DẪN IT SUPPORT & AN NINH THÔNG TIN

Tài khoản - VPN - mật khẩu - phân quyền - xử lý sự cố (Mẫu cho Chatbot RAG)

THÔNG TIN TÀI LIỆU	
Mã tài liệu	ABC-IT-SEC-001
Phiên bản	1.1
Hiệu lực từ	20/12/2025
Đơn vị sở hữu	Phòng CNTT (IT)
Phân loại	Nội bộ

Mục đích: Cung cấp bộ dữ liệu mẫu (nhiều ngữ cảnh, nhiều ngoại lệ, có SLA, có biểu mẫu) để kiểm thử Chatbot RAG nội bộ. Nội dung cố ý có các tình huống gần giống nhau để kiểm tra khả năng truy xuất và tổng hợp của hệ thống.

# MỤC LỤC

Mục	Nội dung
1.	Tổng quan hệ thống: SSO, Email, VPN, Jira, Git
2.	Quy định mật khẩu & xác thực đa yếu tố (MFA)
3.	Cấp tài khoản, phân quyền & thời hạn quyền
4.	Xử lý sự cố: phân loại P1/P2/P3 & SLA
5.	Quy trình reset mật khẩu & khôi phục tài khoản
6.	Chính sách thiết bị: BYOD, phần mềm được phép
7.	Bảo mật dữ liệu & chia sẻ file
8.	Phụ lục: Mẫu ticket & câu hỏi hay gặp

Gợi ý ingest: chunk theo tiêu đề H2/H3; giữ lại metadata ở đầu mỗi mục để làm filter (department, effective\_date, owner).

## 1. Tổng quan hệ thống: SSO, Email, VPN, Jira, Git

ABC sử dụng SSO làm cổng truy cập chung. Một số hệ thống yêu cầu VPN khi truy cập ngoài mạng nội bộ.

Hệ thống	Mục đích	Yêu cầu truy cập
SSO Portal	Đăng nhập tập trung	Bắt buộc MFA
Email (abc.example)	Trao đổi nội bộ	SSO + MFA
Jira	Quản lý công việc	SSO
GitLab	Mã nguồn	SSO + SSH key
Intranet	Tài liệu & form	Trong mạng nội bộ/VPN

## 2. Quy định mật khẩu & xác thực đa yếu tố (MFA)

- Mật khẩu tối thiểu 12 ký tự, gồm chữ hoa, chữ thường, số và ký tự đặc biệt.
- Không dùng lại 5 mật khẩu gần nhất.
- Bắt buộc bật MFA cho SSO và Email.
- Không chia sẻ mã OTP qua chat/email.

Tình huống kiểm thử: User hỏi 'Mật khẩu tối thiểu bao nhiêu ký tự?' -> 12. User hỏi 'SSO có bắt buộc MFA không?' -> có.

## 3. Cấp tài khoản, phân quyền & thời hạn quyền

Quyền truy cập được cấp theo nguyên tắc 'least privilege'. Quyền dự án có ngày hết hạn (expiry) và tự thu hồi nếu không gia hạn.

Loại quyền	AI yêu cầu	AI duyệt	Thời hạn mặc định
VPN	Trưởng bộ phận/PM	IT Lead	90 ngày
Repo Git dự án	PM	Tech Lead	Theo dự án
Database Read-only	Tech Lead	Security Officer	30 ngày
Admin hệ thống	Head IT	BGD	Theo quyết định

## 4. Xử lý sự cố: phân loại P1/P2/P3 & SLA

Mức	Ví dụ	SLA phản hồi	SLA khắc phục mục tiêu
P1	SSO/Email down diện rộng	15 phút	4 giờ
P2	VPN lỗi cho một nhóm	1 giờ	1 ngày
P3	Quên mật khẩu cá nhân	4 giờ	1-2 ngày

Lưu ý: SLA khắc phục là mục tiêu; nếu phụ thuộc nhà cung cấp, IT phải cập nhật ETA mỗi 4 giờ (P1) hoặc mỗi ngày (P2).

5. Quy trình reset mật khẩu & khôi phục tài khoản

5.1. Reset mật khẩu Email/SSO

- Tạo ticket 'Password Reset' trên cổng IT Support.
- Xác minh danh tính: gọi số nội bộ hoặc xác minh qua quản lý trực tiếp.
- IT gửi link reset qua kênh an toàn (SSO portal).
- User bắt buộc đổi mật khẩu ngay lần đăng nhập đầu.

5.2. Trường hợp mất điện thoại MFA

Nếu mất thiết bị MFA, user phải báo IT ngay trong 30 phút kể từ khi phát hiện. IT sẽ khóa phiên đăng nhập, thu hồi token và cấp phương án MFA dự phòng.

Tình huống kiểm thử: 'Em mất điện thoại MFA thì làm sao?' -> cần trả lời: báo IT trong 30 phút + khóa phiên + cấp dự phòng.

6. Chính sách thiết bị: BYOD, phần mềm được phép

- Thiết bị công ty: bắt buộc mã hóa ổ đĩa, bật firewall, cập nhật tự động.
- BYOD (thiết bị cá nhân) chỉ áp dụng cho email và chat; không được truy cập repo mã nguồn hoặc DB.
- Cấm cài phần mềm không bản quyền; IT có quyền gỡ bỏ phần mềm vi phạm.

7. Bảo mật dữ liệu & chia sẻ file

Loại dữ liệu	Ví dụ	Được chia sẻ qua	Không được chia sẻ qua
Nội bộ	Quy trình, tài liệu training	Intranet, Drive nội bộ	Email cá nhân
Nhạy cảm	Lương, hợp đồng, dữ liệu khách hàng	Drive nội bộ + quyền hạn chế	Link công khai
Bí mật	Source code, khóa API	GitLab + secret manager	Chat/ảnh chụp màn hình

8. Phụ lục: Mẫu ticket & câu hỏi hay gặp

Mẫu tiêu đề ticket (khuyến nghị):

- [P2] VPN không kết nối - nhóm dự án MayFest - lỗi 720

Thông tin bắt buộc trong ticket:

- Hệ thống bị lỗi
- Thời điểm bắt đầu
- Ảnh chụp màn hình/lỗi log (nếu có)
- Mức độ ảnh hưởng (một người/nhóm/toàn công ty)
- Cách liên hệ khẩn