# Software Requirements Specification

## สำหรับโครงการ: Advance agent for Cybersecurity


### รายชื่อ สมาชิก

1. นายภูวิศ จารุรัตน์กิจ รหัสนักศึกษา 67056056

2. นายสิรภพ กิจเจริญรุ่งโรจน์ รหัสนักศึกษา 67056078

3. นายสุทธิ ดิลกเลิศพลากร รหัสนักศึกษา 67056082

# ภาพรวมของระบบ (System Overview)

ระบบ Advance Agent for Cybersecurity เป็นระบบที่พัฒนาขึ้นเพื่อช่วยองค์กรในการ จัดเก็บ, วิเคราะห์, และติดตามข้อมูลความมั่นคงปลอดภัยทางไซเบอร์ ภายในองค์กร โดยมีองค์ประกอบหลักดังนี้

**1. Knowledge Management Module**

โมดูลนี้ทำหน้าที่ในการจัดการองค์ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ เช่น รายงานเหตุการณ์ (Incident Report), บทวิเคราะห์ช่องโหว่, และแนวทางการป้องกัน

- ผู้ดูแลระบบ (Admin) สามารถ นำเข้าเอกสาร ที่เกี่ยวข้องเข้าสู่ระบบได้
- ระบบจะทำการ ประมวลผลและแปลงข้อมูลเอกสารเป็น Vector Embedding
- จากนั้นจัดเก็บข้อมูลลงใน Vector Database เพื่อให้สามารถค้นหาและเรียกดูเนื้อหาได้อย่างรวดเร็วในอนาคต

**2. Log Management Module**

โมดูลนี้ใช้สำหรับ รวบรวมและจัดการข้อมูล Log จากอุปกรณ์ต่าง ๆ เช่น Firewall, Router, Windows Server และ Endpoint

- ผู้ดูแลระบบสามารถ ตั้งค่า Agent เพื่อรับข้อมูล Syslog ผ่านโปรโตคอล UDP หรือ TCP
- ข้อมูล Log ที่ได้รับจะถูกจัดเก็บไว้ในฐานข้อมูล เพื่อใช้ในการวิเคราะห์เหตุการณ์ทางความปลอดภัย (Security Event Analysis)

**3. System Monitoring Module**

โมดูลนี้ทำหน้าที่ ติดตามสถานะของระบบแบบ Real-time

- แสดงผลผ่าน Dashboard ที่รวมข้อมูลจากทุกโมดูล เช่น
    - สถานะของ Agent (Active / Inactive)
    - สถิติของ Log ที่เก็บรวบรวม
    - จำนวนเอกสารใน Knowledge Base
    - สถานะสุขภาพของระบบ (System Health)
- Dashboard จะอัปเดตข้อมูลอัตโนมัติทุก 5 นาที เพื่อให้ผู้ดูแลระบบสามารถตรวจสอบความพร้อมของระบบได้อย่างต่อเนื่อง

**4. System Architecture Overview**

ภาพรวมของสถาปัตยกรรมระบบมีองค์ประกอบดังนี้:

1. Admin Interface – ส่วนที่ผู้ดูแลระบบใช้งานผ่าน Web Application เพื่อจัดการ Knowledge Base, Log, และ Dashboard
2. Agent Component – ทำหน้าที่รวบรวมข้อมูล Log จากอุปกรณ์ในเครือข่ายและส่งเข้าสู่ระบบกลาง
3. Server & Processing Layer – ประมวลผลข้อมูลเอกสารและ Log รวมถึงแปลงข้อมูลเป็น Vector Embedding
4. Vector Database & Log Storage – จัดเก็บข้อมูลที่ผ่านการประมวลผลแล้ว เพื่อให้เรียกใช้ได้รวดเร็ว
5. Dashboard Service – ดึงข้อมูลจากฐานข้อมูลมาสร้างการแสดงผลแบบ Real-time

**5. ประโยชน์ของระบบ (System Benefits)**

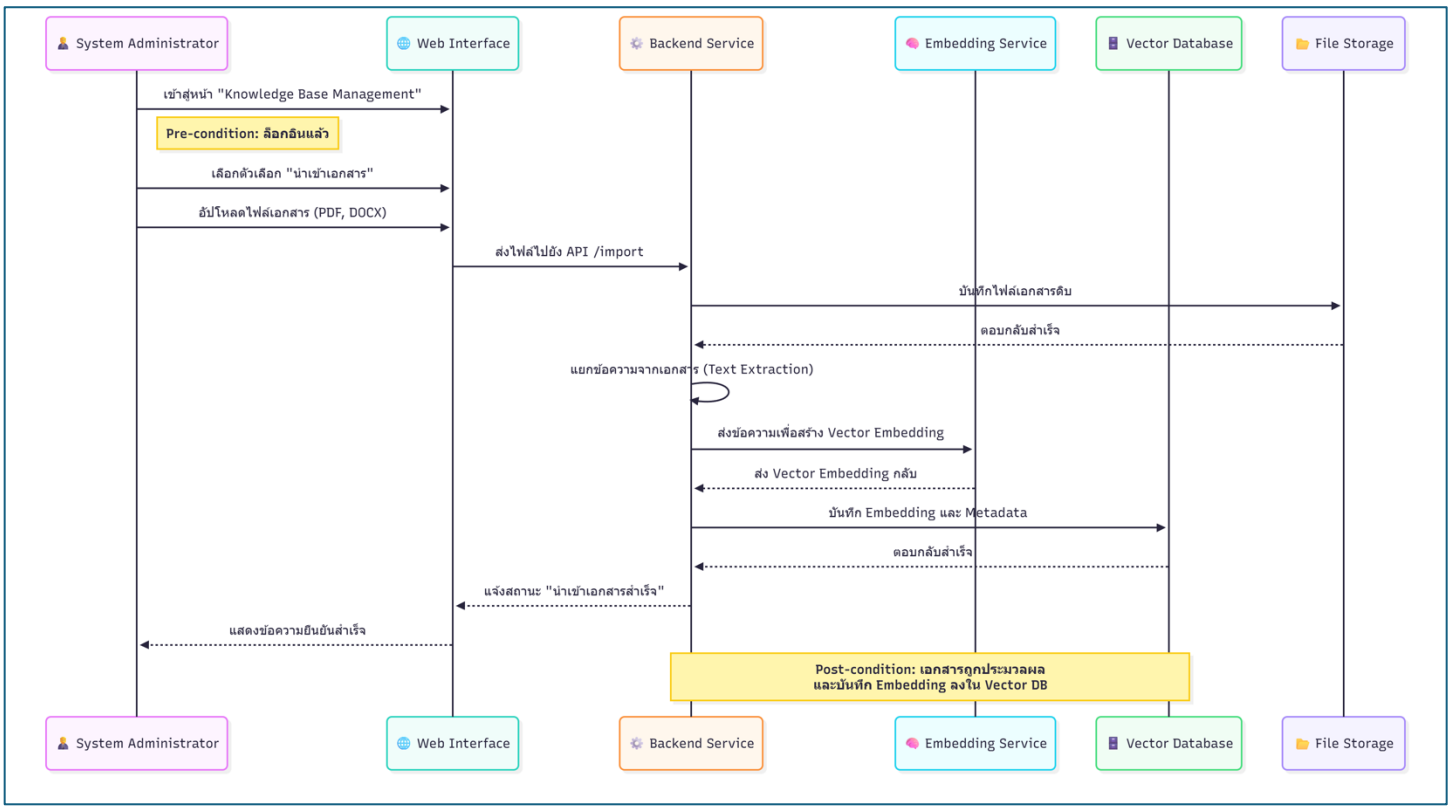
- ลดภาระงานของผู้ดูแลระบบด้าน Cybersecurity
- สามารถเข้าถึงองค์ความรู้ภัยคุกคามได้อย่างรวดเร็ว
- มีระบบติดตามสถานะและตรวจสอบข้อมูลแบบ Real-time
- รองรับการขยายระบบในอนาคตทั้งด้านข้อมูลและจำนวนอุปกรณ์

# ส่วนที่ 1: การจัดการองค์ความรู้ (Knowledge Management) - สำหรับ Admin

## UC-ADM-01 : นำเข้าเอกสาร (Import Documents)

- Primary Actor: ผู้ดูแลระบบ (System Administrator)
- Objective: เพื่อเพิ่มองค์ความรู้ใหม่ๆ (เช่น รายงานวิเคราะห์ภัยคุกคาม) เข้าสู่ระบบ
- Pre-condition:
    - ผู้ดูแลระบบล็อกอินเข้าสู่ระบบแล้ว
    - มีไฟล์เอกสารในรูปแบบที่รองรับ (PDF, DOCX)
- Post-condition: เอกสารที่นำเข้าถูกจัดเก็บและประมวลผลเป็น Vector Embedding บันทึกลงใน Vector DB
- Normal Flow of Events:
    1. ผู้ดูแลระบบเข้าสู่หน้า "Knowledge Base Management"
    2. เลือกตัวเลือก "นำเข้าเอกสาร"
    3. อัปโหลดไฟล์ที่ต้องการผ่านหน้าเว็บอินเทอร์เฟซ
    4. ระบบยืนยันการรับไฟล์และเริ่มกระบวนการประมวลผลอัตโนมัติ

Sequence Diagram UC01

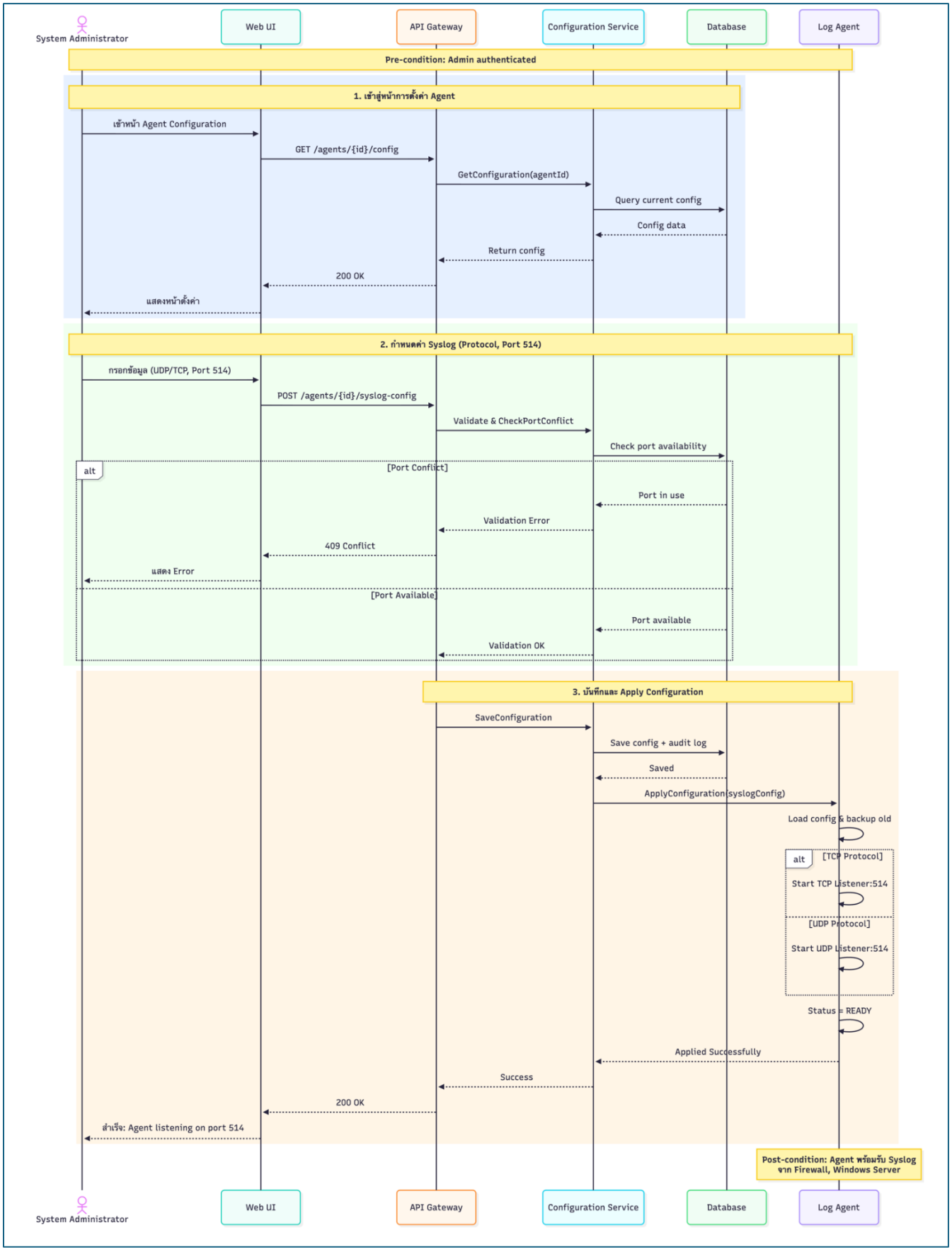


# ส่วนที่ 2: การจัดการข้อมูล Log (Log Management) - สำหรับ Admin

**UC- ADM-02 : ตั้งค่าการรับข้อมูล Log (Configure Log Collection)**

- Primary Actor: ผู้ดูแลระบบ (System Administrator)
- Objective: เพื่อให้สามารถตั้งค่า Agent ให้รับข้อมูล Syslog จากอุปกรณ์ต่างๆ เช่น Firewall และ Windows Server ได้
- Pre-condition: ผู้ดูแลระบบล็อกอินเข้าสู่ระบบแล้ว
- Post-condition: Agent พร้อมรับข้อมูล Log จากแหล่งที่กำหนดผ่านโปรโตคอล UDP หรือ TCP
- Normal Flow of Events:
    1. ผู้ดูแลระบบเข้าสู่หน้าการตั้งค่า Agent
    2. กำหนดค่าการรับข้อมูล Syslog เช่น โปรโตคอล (UDP/TCP) และพอร์ต (514)
    3. บันทึกการตั้งค่า

# Sequence Diagram UC02

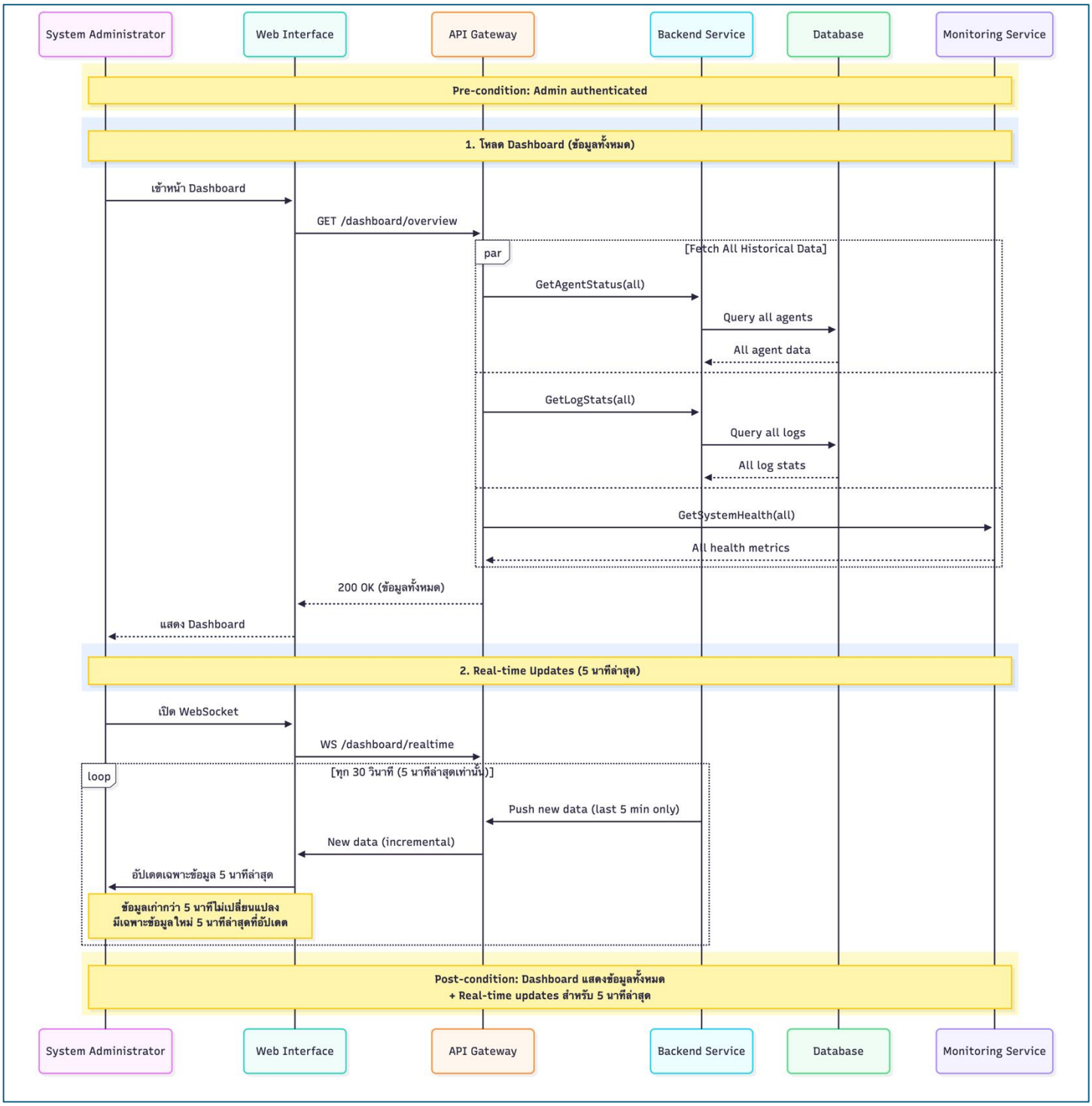


# ส่วนที่ 3: การติดตามและตรวจสอบระบบ (System Monitoring) - สำหรับ Admin

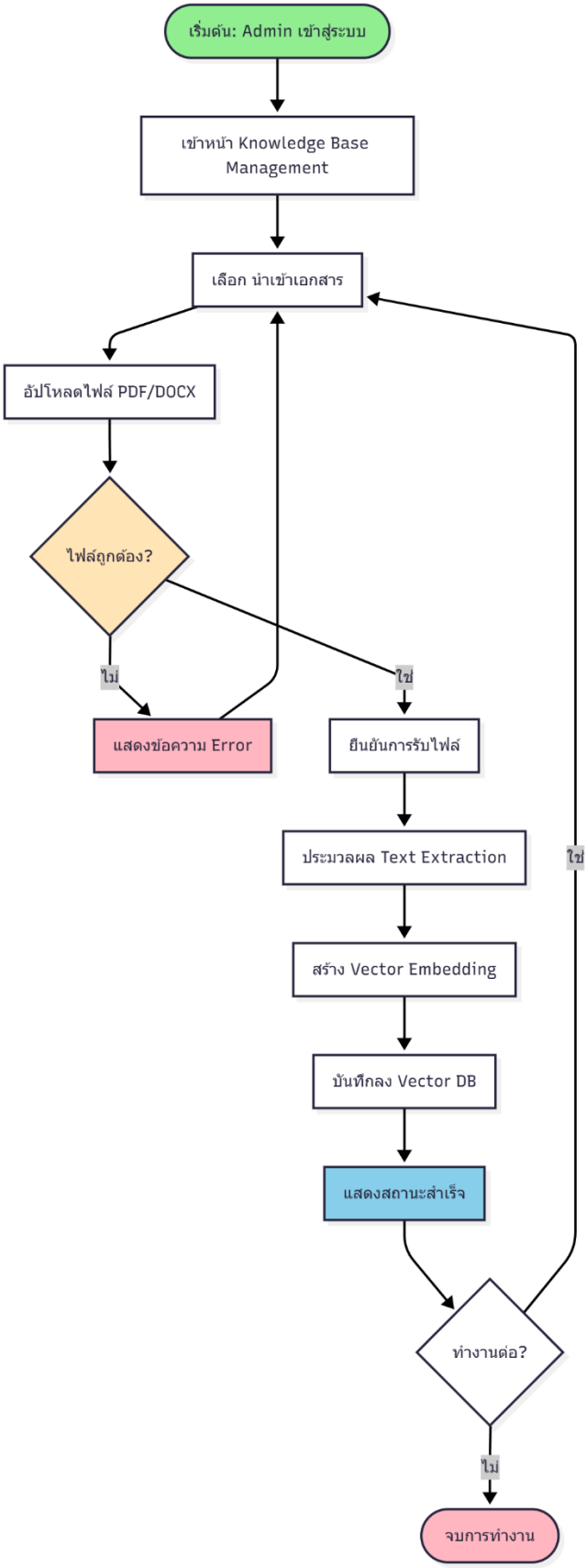
**UC-ADM -03 : ดู Dashboard แบบ Real-time (View Real-time Dashboard)**

- Primary Actor: ผู้ดูแลระบบ (System Administrator)
- Objective: เพื่อติดตามสถานะระบบ, Agent, Log และ Knowledge Base แบบ Real-time
- Pre-condition: ผู้ดูแลระบบล็อกอินเข้าสู่ระบบแล้ว
- Post-condition: Dashboard แสดงข้อมูลทั้งหมดย้อนหลังและอัปเดตอัตโนมัติทุก 5 นาที
- Normal Flow of Events:
    1. ผู้ดูแลระบบเข้าสู่หน้า "Dashboard"
    2. ระบบแสดงข้อมูลทั้งหมดย้อนหลัง ประกอบด้วย:
        - สถานะ Agent (Active/Inactive)
        - สถิติ Log ที่เก็บรวบรวม
        - จำนวนเอกสารใน Knowledge Base
        - สถานะสุขภาพระบบ (System Health)
    3. Dashboard อัปเดตข้อมูลอัตโนมัติทุก 5 นาที
    4. ผู้ดูแลระบบสามารถคลิกดูรายละเอียดเพิ่มเติมในแต่ละส่วนได้

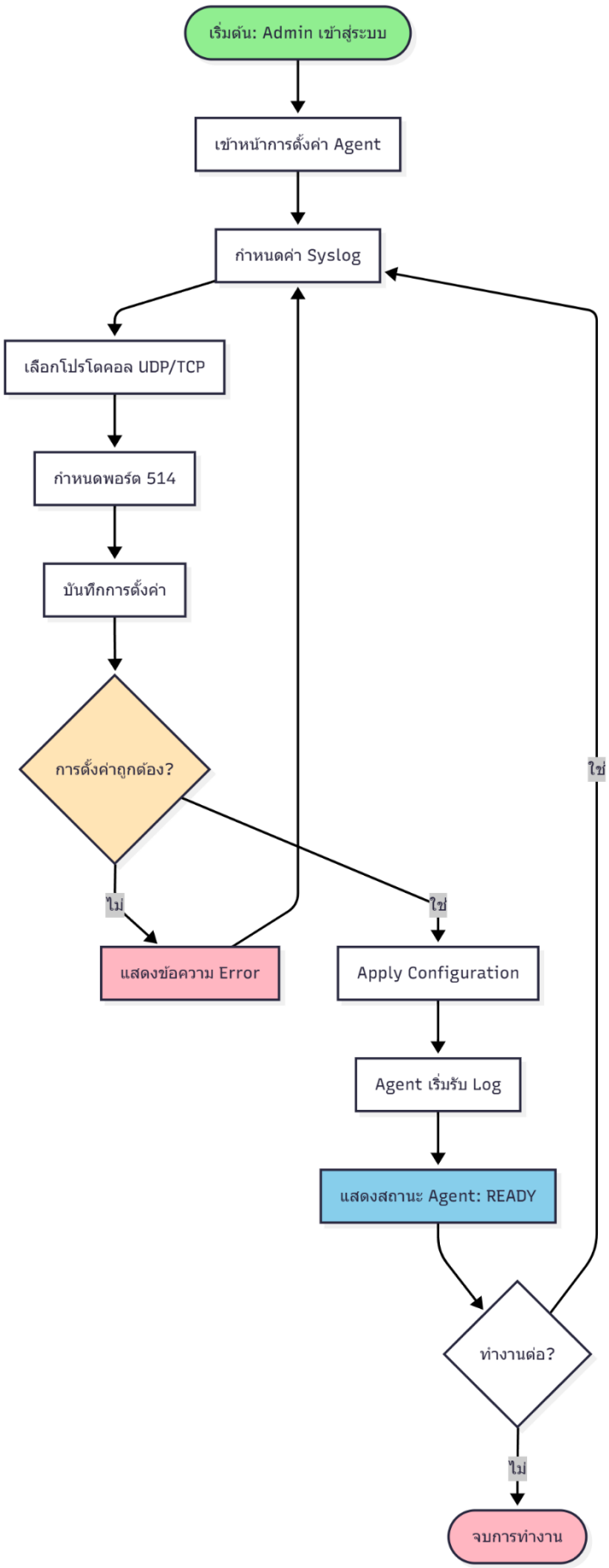
Sequence Diagram UC03



# Activity Diagram: UC-ADM-01



# Activity Diagram: UC-ADM-02



# Activity Diagram: UC-ADM-03