# Microsoft 365 Audit Log Data Collection Process Steps

Step 1: Activate Microsoft 365 Business Premium Trial

Step 2: Create 8 Users (1 Admin + 7 Users)

Step 3: Access Microsoft Purview Portal

Step 4: Enable 'Start recording user and admin activity'

Step 5: Login to all user accounts and perform actions

Step 6: Perform Suspicious Activities (VPN, failed logins, etc.)

Step 7: Wait for a few hours to let logs generate

Step 8: Search Audit Logs in Purview (with filters)

Step 9: Download and Export Audit Logs (CSV)

Step 10: Clean and Format Logs using Excel Power Query

Step 11: Save as Final Dataset File

# Process Details for Collecting Microsoft 365 Audit Log Data

## Phase 1: Setup Microsoft 365 Environment

1. **Activate Trial Subscription**:
   - Subscribed to **Microsoft 365 Business Premium (Trial)**.
2. **Create User Accounts**:
   - Created **8 total users** (1 Admin + 7 Standard Users).

---

## Phase 2: Enable Audit Logging

3. **Access Microsoft Purview**:
   - Navigated to **Microsoft Purview Compliance Portal**.
4. **Enable Audit Logging**:
   - Enabled **"Start recording user and admin activity"** to begin capturing logs.

---

## Phase 3: Perform User Activities

5. **User Logins and File Activities**:
   - Logged into all **8 user accounts** individually.
   - Performed the following activities:

        - **Created** new files in Word, Excel, and PowerPoint.
        - **Read, sent, and received** emails among the users.
        - **Deleted multiple files** at once.
        - **Downloaded files** from OneDrive.
6. **Suspicious and Security-Test Activities**:
    - Logged in to the same user account from **multiple laptops**.
    - Logged in using a **VPN** to simulate suspicious access.
    - **Sent emails** to invalid/unavailable email addresses.
    - Attempted **multiple failed logins** with incorrect passwords.

---

## Phase 4: Retrieve Audit Logs

7. **Wait for Log Generation**:
    - Waited **a few hours** after performing the activities to ensure log capture.
8. **Search Audit Logs in Purview**:
    - Accessed **Microsoft Purview → Audit** section.
    - Applied:
        - **Date and time range** filter.
        - **All 8 user accounts** in the search.
9. **Run the Search**:
    - Executed the audit log search.
    - Waited for the search results to complete.

---

## Phase 5: Format and Export Logs

10. **Export Logs**:
    - Downloaded the audit log **CSV file** from the portal.
11. **Clean and Format Logs**:
    - Used **Excel Power Query** to clean and transform the audit data.
    - Selected **only required columns** for analysis.
    - Saved the formatted data as a **dataset file** for further use.