# 📌 Project Title

ExfilEye – Monitor & Flag Risky Outbound Emails with AI-Powered Insights

# 🎯 Main Objective

Develop a fully functional web application on Replit that enables users to:  
- Detect and analyze potential data exfiltration risks.  
- Visualize outbound email patterns.  
- Use AI-powered anomaly detection and risk scoring.  
- Generate polite follow-up communications automatically.  
- Adapt dynamically to different CSV formats.  
- Run with no agent checkpoints, fully contained within Replit.

# 📁 User Uploads

## Email Data (CSV)

\_Required fields:\_

\_time, sender, recipients, email\_domain, word\_list\_match, recipient\_status, subject, attachments, act, delivered, deliveryErrors, direction, eventtype, aggreatedid, tessian, tessian\_response, mimecast, tessian\_outcome, tessian\_policy, last\_working\_day, bunit, department, businessPillar

## BAU Whitelist (CSV + UI)

\_Fields:\_

email\_address, domain

Users can view, add, edit, or remove whitelist entries through the interface.

# ✨ Core Features

## ✅ Domain Classification

Classify recipient domains as internal, business, or public/free using datasets.

## ✅ BAU Whitelist Exclusion

Exclude known-safe domains or emails; CRUD UI included.

## ✅ Leaver Detection

Flag emails ±7 days from sender’s last working day. Score: +30.

## ✅ IP Detection

Scan for sensitive keywords in subject/body/attachments. Score: +25.

## Anomaly Detection Engine

Risk Score Calculation Table:

|  |  |  |
| --- | --- | --- |
| Condition | Score | Description |
| Volume spike vs. user average | +10 | High email activity |
| Sent after hours/weekend | +10 | Outside business hours |
| Free email domain recipient | +20 | Non-corporate domains |
| New external domain for sender | +15 | First-time domain recipient |
| Unusual file type / large attachment | +15 | Potentially risky content |
| Leaver within 7-day window | +30 | Departure-related activity |
| IP keywords in attachment/body | +25 | Sensitive content |
| Burst to same domain | +15 | Mass emailing patterns |
| New file type for user | +10 | Unusual file usage |

Risk Levels:  
- 0–30: Normal  
- 31–60: Medium Risk  
- 61+: High Risk

# 🧠 AI-Driven Analytics & Insights

- Behavioral Baselines  
- Unsupervised Learning  
- NLP Analysis  
- Predictive Models  
- Smart Whitelisting  
- Integrated Insights

# 📊 Interactive Reporting Dashboard

- Filters: department, bunit, businessPillar, risk score, domain type, etc.  
- Visuals: Pie charts, trends, anomaly clusters  
- Export: CSV, scheduled reports

# 🌐 Visual Network Map

- Graphs with nodes (users/domains) and risk status  
- Click = metadata popup  
- Follow-up tasks integration

# 📬 Polite Follow-up Email Generator

- Generate/edit/send polite emails from flagged entries  
- Supports bulk and manual selection  
- Integrates with follow-up tasks

# 🛠 Replit Deployment Notes

To run this project on Replit:  
1. Create a new Replit project (Python + Flask or Node.js).  
2. Add packages: pandas, networkx, matplotlib, scikit-learn, transformers, flask, dash, etc.  
3. Include:  
 - upload route for CSVs  
 - visualization module for graphs  
 - anomaly scoring engine  
 - AI insights and behavior analysis  
 - follow-up email generator  
4. Build UI with Flask, Dash, or Streamlit.  
  
make sure all buttons and upload buttons work