# Audit Check List

| | |
|---|---|
| Audited Company | Nguyen Auditing Services |
| Reason for Audit | Deployment at client sites |
| Date | 17/07/2025 |
| Auditor | Khuong Nguyen |
| Approval:<br>(signature of lead auditor) | K. Nguyen |
| Date of approval | 20/07/2025 |

### Table of Contents

# 1. **On-Premise Lakehouse (Data Storage & Processing Environment)**

- [ ] Verify asset inventory completeness (hardware, software, data assets)
- [ ] Confirm classification of information assets (data sensitivity levels)
- [ ] Validate physical security controls for on-prem hardware (limited given home setup)
- [ ] Assess PostgreSQL database access controls:
    - Role-based access enforcement
    - Audit logs for queries
    - MFA enforcement status
- [ ] Review data storage:
    - Secure storage of analytics logs on SSDs
    - Backup and recovery processes
- [ ] Examine network segmentation:
    - Public vs private network boundaries
    - Firewall/endpoint protections
- [ ] Review GPU and computing cluster security configurations
- [ ] Confirm incident logging and monitoring capabilities

# 2. **Public-Facing Site**

- [ ] Check for secure deployment of site content (HTTPS enforced)
- [ ] Validate use of Google Analytics and compliance with privacy standards:
    - Presence/absence of consent banner
    - Privacy policy publicly available
- [ ] Assess risks related to public exposure of aggregated data

☐ Review CI/CD pipeline for secure deployment:

- Branch protection
- Dependency and secrets scanning enabled

## 3. GitHub Repo and CI/CD Pipeline

☐ Confirm repository access management:

- Role-based permissions
- Quarterly permission reviews
- Immediate revocation for departed contributors

☐ Validate branch protection and pull request policies

☐ Check CI/CD pipeline security scans:

- Dependency scanning
- Secrets scanning

☐ Review source code for security best practices and sensitive information exposure

## 4. Security Controls

☐ MFA enforcement across critical systems

☐ Check audit logs and their retention, integrity, and review processes

☐ Review incident response:

- Incident logging
- Ad hoc incident management
- Annual incident response plan review

☐ Physical security adequacy given environment (single user setup)

## 5. GDPR Compliance

☐ Verify data processing mechanism (types of data collected and processed)

☐ Check if Data Subject Rights processes are formally documented and enforced:

- Access and erasure request handling
- 30-day SLA adherence

☐ Review breach notification process:

- Awareness of 72-hour notification rule
- Documentation and formal procedures

☐ Assess privacy policy and cookie consent mechanisms:

- Presence of public privacy policy
- Implementation of consent banner for analytics

☐ Confirm anonymisation and aggregation of analytics data

# 6. Risk Management

☐ Review Risk Register for identified High and Medium risks:

- MFA
- Formal GDPR access/erasure process
- Consent banner on site

☐ Confirm risk mitigation plans and timelines

☐ Verify monitoring and update cycles for risk register