Security and Access Policy

Jennifer Lewis – Consulting Engagements

This document outlines the security, confidentiality, and access control practices followed during consulting engagements.
It ensures that client data, intellectual property, and infrastructure remain protected throughout all phases of the project.

---

1. Data Handling Practices

Data Receipt and Storage

- Client data is accessed only for the duration of the project and only for tasks defined in the Statement of Work.
- Data is never transferred to personal cloud storage, external services, or unapproved systems.
- Data is stored only on client-approved environments or secured local encrypted storage when explicitly authorized.

Data Retention

- No client data is retained beyond project completion.
- All datasets, credentials, logs, and artifacts are deleted upon delivery unless written authorization is provided.

---

2. Access Credentials

Credential Scope

- Access is limited to the minimum credentials required to complete the engagement.
- If possible, temporary or scoped credentials are preferred.

Credential Storage

- Credentials are stored only in secure configuration methods approved by the client (environment variables, Vault, encrypted key stores).
- Credentials are never hardcoded, logged, or included in source repositories.

---

3. Infrastructure Access

Approved Channels

- Access may be provided via VPN, jump hosts, cloud IAM roles, or other secure methods.
- SSH and remote access must follow client-defined policies.

Restrictions

- No changes to production systems are made without formal approval.
- Work is conducted only in designated development or sandbox environments unless otherwise specified.

---

4. Code and Artifact Security

- Proprietary client code is never redistributed or shared.
- Development artifacts remain within the client's infrastructure unless explicitly permitted.
- Git repositories used for collaboration must adhere to the client's access policies.

---

5. Confidentiality

- All information, datasets, model outputs, research insights, design documents, and internal processes are treated as confidential by default.
- Confidentiality obligations continue after the engagement unless otherwise negotiated.

---

6. Communication and Reporting

- Sensitive information is communicated only through client-approved channels.
- Periodic progress updates are provided according to the Statement of Work.

---

7. Compliance

Client-specific compliance requirements (NDA, data handling restrictions, additional policies) will be followed as defined in the contracting agreement or SOW.

Contact

Questions regarding this policy may be directed to:
jenn.lewis5789@gmail.com