Client Data Protection & Confidentiality

1. Client Data Ownership

All data, information, materials, content, source code, credentials, documentation, and other information provided by a client or generated on behalf of a client during the course of a project ("Client Data") shall remain the sole and exclusive property of the client.

InsightCrew does not claim ownership of Client Data.

---

2. Use of Client Data

Client Data shall be accessed, processed, and used strictly for:

- Performing services agreed under the applicable contract or statement of work
- Meeting legal and regulatory obligations
- Providing support and maintenance related to the client project

Client Data shall not be used for marketing, analytics, training, or any secondary purpose without the client's explicit written consent.

---

3. Confidentiality Obligations

InsightCrew treats all Client Data as confidential information and shall:

- Not disclose Client Data to any unauthorized third party
- Ensure employees are bound by confidentiality agreements
- Limit access to Client Data strictly on a need-to-know basis

These confidentiality obligations survive termination or completion of the client engagement.

---

4. Data Access Controls

Access to Client Data is restricted to authorized personnel assigned to the client project. Role-based access controls and authentication mechanisms are implemented to prevent unauthorized access.

---

5. Data Security Measures

InsightCrew implements reasonable and appropriate technical and organizational security measures to protect Client Data, including but not limited to:

- Secure access controls
- Secure development and deployment practices

---

6. No Storage Beyond Project Scope

Unless otherwise agreed in writing, InsightCrew does not retain Client Data beyond the duration of the project. Temporary data, backups, or copies created for development, testing, or support purposes are securely deleted upon project completion or client request.

---

7. Client Credentials & Access Information

Client-provided credentials (including usernames, passwords, API keys, certificates, tokens, or access secrets) are:

- Used solely for project-related purposes
- Stored securely where required
- Shared internally only with authorized project members

Clients are encouraged to revoke or rotate credentials upon project completion.

---

8. Compliance with Client Requirements

InsightCrew agrees to comply with reasonable data protection, security, and confidentiality requirements specified by the client in applicable agreements, provided such requirements are lawful and mutually agreed upon.

---

9. Client Responsibility

Clients are responsible for:

- Ensuring they have the legal right to share data with InsightCrew
- Providing clear instructions regarding data handling, retention, and access
- Avoiding the sharing of unnecessary or sensitive data unless explicitly required for the project