CareerCraft AI Security & Compliance Documentation

1. Introduction

CareerCraft AI takes security and compliance seriously, ensuring that user data remains protected, and the platform adheres to global data privacy regulations. This document outlines the security measures, compliance frameworks, and privacy policies implemented in CareerCraft AI.

2. Data Security Measures

2.1. Encryption Standards

- **Data at Rest:** AES-256 encryption is applied to all stored data, including resumes, user profiles, and application history.
- **Data in Transit:** All communications between users and servers are secured using TLS 1.3 encryption.

2.2. Authentication & Access Control

- **Multi-Factor Authentication (MFA):** Required for premium users to enhance security.
- **Role-Based Access Control (RBAC):** Different permission levels for job seekers, recruiters, and administrators.
- **Single Sign-On (SSO):** Supported for enterprise users using OAuth, Google, and Microsoft authentication.

2.3. Data Backup & Recovery

- **Automated Backups:** Conducted every 24 hours and stored in geographically distributed data centers.
- **Disaster Recovery Plan:** Ensures data restoration within 4 hours in case of server failures.

3. Compliance Frameworks

CareerCraft AI complies with major global regulations, including:

- **General Data Protection Regulation (GDPR) (EU):** Users have full control over their data with the ability to request deletion.
- **California Consumer Privacy Act (CCPA):** Users can opt out of data collection and request access to stored information.
- **SOC 2 Type II Compliance:** Ensuring secure data handling processes for SaaS products.
- **ISO 27001 Certification:** Industry-standard framework for security risk management.

4. Privacy Policy

4.1. Data Collection

We collect the following types of user data:

- Personal information (name, email, job title)
- Resume details (education, experience, skills)
- Interaction data (resume edits, cover letter generation)

4.2. Data Retention & Deletion

- Free-tier users: Data retained for 6 months of inactivity.
- Paid-tier users: Data retained for 12 months of inactivity.
- Users can delete their account anytime via the settings page.

5. Security FAQs

Q1: Is my resume data shared with third parties?

A: No, CareerCraft AI does not sell or share personal resume data with third parties without user consent.

Q2: How do I enable multi-factor authentication?

A: Go to Account Settings > Security > Enable MFA and follow the setup process.

Q3: Can I download my data?

A: Yes, users can request a data export from their account settings.

6. Reporting Security Issues

Users can report security concerns at security@careercraftai.com. Our security team follows a 24-hour response policy for critical issues.

This document ensures transparency in how CareerCraft AI manages security and compliance while protecting user data.