Third Party's Background Check Policy

2COMS Background Check Policy for Third-Party Partners

Effective Date: January 2, 2025

Policy Owner: 2COMS Group Compliance Department

1. Introduction

This **Third-Party Partner Background Check Policy** establishes the mandatory framework for conducting background checks on all personnel engaged by third-party organizations (hereafter "Partners") to perform services for or on behalf of 2COMS Group.

The purpose is to ensure all such personnel meet the standards of integrity and reliability required to protect the assets, reputation, and stakeholders of 2COMS Group. Adherence to this policy is critical for mitigating security risks and fostering a safe, compliant, and trustworthy work environment.

2. Scope

This policy applies to **all Partners** who engage personnel to work on behalf of 2COMS Group. It covers background checks for all potential and current personnel, including, but not limited to:

- Full-Time Employees
- Part-Time Employees
- Contract Workers and Freelancers
- Temporary Staff
- Interns

3. Background Check Requirements

The Partner must initiate a comprehensive background check after a conditional offer of engagement is made to a candidate.

3.1. Authorized Providers

Background checks must be conducted by the Partner's authorized and trained personnel or a reputable, professional third-party screening provider. The chosen provider must comply with all applicable data privacy and employment laws. 2COMS Group reserves the right to audit the provider's credentials and compliance standards.

3.2. Standard Components of the Background Check

The background check must, at a minimum, include the following components:

- **Identity Verification**: Confirmation of the candidate's identity using valid, government-issued photo identification.
- **Criminal History Check**: A review of criminal records at the local, state, and national levels, as permissible by law.
- **Employment History Verification**: Verification of the candidate's employment history for the past seven years, confirming positions, dates, and reasons for leaving.
- **Education Verification**: Confirmation of the highest degree or relevant certification claimed by the candidate.
- **Professional Reference Check**: Contacting at least two professional references to assess the candidate's qualifications, character, and work ethic.
- **Citizenship & Work Authorization**: Verification of the candidate's legal right to work in the country of employment.

4. Adjudication of Adverse Findings

Should a background check reveal adverse information, the Partner must follow a structured process to determine the candidate's suitability.

4.1. Individualized Risk Assessment

An automatic rejection based on a finding is prohibited. The Partner must conduct an individualized assessment, considering factors such as:

- The **nature and gravity** of the offense or discrepancy.
- The **time that has passed** since the offense or conduct.
- The **relevance of the finding** to the essential duties and responsibilities of the specific position.

4.2. Process for Handling Adverse Findings

If the initial assessment leads to a potential adverse decision (e.g., rescinding an offer), the Partner must:

1. **Pre-Adverse Action Notice**: Notify the candidate in writing of the potential adverse action. This notice must include a copy of the background check report and a summary of their rights under applicable law.

2. **Opportunity to Dispute**: Provide the candidate a period of **five (5) business days** to review the report and dispute the accuracy or completeness of the information with the screening provider.
3. **Final Decision & Adverse Action Notice**: After the dispute period, if the Partner finalizes the decision to reject or terminate, they must provide a second written notification (Adverse Action Notice) to the individual.
4. **Documentation**: All steps, communications, and the final rationale for the decision must be thoroughly documented and maintained.

5. Compliance and Data Protection

- **Legal Compliance**: All background checks must be performed in strict compliance with all applicable national, state, and local laws regarding employment, data privacy, and fair credit reporting.
- **Confidentiality**: All information obtained during the background check process is strictly confidential. Access is restricted to authorized personnel directly involved in the hiring decision.
- **Data Security**: Partners must implement and maintain robust technical and physical security measures, such as encryption and secure access controls, to protect background check data from unauthorized access or disclosure.

6. Policy Review

This policy will be reviewed annually by the 2COMS Group Compliance Department to ensure it remains current with evolving laws, regulations, and best practices.