...Surpassing Imagination

Data Protection Policy

Effective Date: January, 2025

Prepared By: Globalclique

Approved By: Board of Globalclique

1. Introduction

Globalclique is committed to maintaining the confidentiality, integrity, and availability of data entrusted to us. This policy outlines the measures we take to protect data, prevent breaches, and respond effectively in case of incidents, ensuring compliance with applicable data protection regulations.

2. Scope

This policy applies to:

- All job candidates, employees, contractors, clients and third-party stakeholders.
- Digital and physical data handled and coordinated by Globalclique.
- Identified security incidents or vulnerabilities affecting the organization's data.

3. Key Definitions

- **Client:** Any individual or entity engaging with Globalclique for professional services.
- **Staff:** All employees of Globalclique.
- **Data Protection Officer (DPO):** The individual responsible for overseeing the implementation and monitoring of this policy.

4. Responsibilities

- **Data Protection Officer (DPO):**
    - Oversees data protection responsibilities, risks, and compliance.
    - Reviews and updates data protection procedures.
    - Organizes staff training on data security practices.

    - Manages data access, amendment, or deletion requests.
    - Evaluates and approves contracts involving third-party data handlers.
- **Employees and Contractors:**
    - Handle data responsibly and in compliance with this policy.
    - Report potential or actual data breaches immediately.

5. Data Breach Management

To respond swiftly and effectively to data breaches, Globalclique follows these steps:

- **Immediate Suspension:** Suspend affected user accounts upon identifying a breach.
- **Password Reset:** Reset passwords for all relevant accounts and devices within 30 minutes.
- **Stakeholder Notification:** Notify affected clients and stakeholders within 24 hours of breach detection.
- **Breach Analysis:** Investigate and document the source, cause, and scope of the breach.
- **Reporting to Authorities:** Report breaches to regulatory authorities.
- **Implementation of Remedies:** Apply recommended measures to mitigate future risks.

6. Data Storage and Handling

- **Digital Data:**
    - Stored on secured, password-protected cloud platforms and servers.
    - Mandatory monthly password updates for all employees.
    - Devices used must have biometric or encryption security enabled.
- **Physical Data:**
    - Kept in locked storage when not in use.
    - Disposed of securely through shredding when no longer required.
- **Removable Media:**
    - Data stored temporarily must be erased immediately after use.
- **Client Communication:**
    - Restricted to company-approved platforms (e.g., official email accounts).
    - Proposals and reports sent in encrypted formats like PDF.

7. Security Measures

- **Technical Security:**
    - Regular updates of firewalls and antivirus software.
    - Biometric and password-protected devices for official use.

    - Monitoring of system logs to detect unusual activities.
    - Conduct regular penetration testing to identify and correct potential vulnerabilities in our system and processes.
    - Set-up multi-factor authentication - MFA for all critical applications / tools we use for our day to day operation.
- **Physical Security:**
    - Installation of security cameras, fire alarms, and access controls.
    - Proper disposal of outdated devices.

8. Compliance and Review

Globalclique commits to reviewing this policy bi-annually or as necessitated by changes in regulations or industry standards.

9. Contact Information

For inquiries regarding this policy, please contact:

Data Protection Office

- Globalclique Data Protection Team
- info.admin@globalclique.net
- Whatsapp: +2347047009990

10. Conclusion

Globalclique is committed to excellence in data protection, fostering trust and ensuring the security of all information assets - by adhering to this policy,we aim to uphold the highest standards of data privacy and integrity, complying to international data management standards and practices.