

DATA SECURITY PROTOCOL

(Remote Staff & Client Data Handling Policy)

This Data Security Protocol ("Protocol") forms part of and is governed by the Master Service Agreement ("MSA") between:

[Your Company Name] ("Company")

and

[Client Name] ("Client")

This document applies to all remote staff, contractors, freelancers, and third-party collaborators ("Remote Staff") engaged by the Company.

Effective Date: [Insert Date]

1. PURPOSE

The purpose of this Protocol is to establish strict guidelines for the secure handling, storage, access, and disposal of all Client data and project-related materials.

The objective is to:

- Protect Client confidentiality
- Prevent unauthorized access or data breaches
- Ensure proper data lifecycle management, including mandatory deletion after project completion

2. SCOPE

This Protocol applies to all forms of Client data, including but not limited to:

- Design files, documents, and source files
- Login credentials and access details
- Business information, strategies, and internal communications
- Media assets (images, videos, audio)
- Any proprietary or confidential material provided by the Client

3. ACCESS CONTROL

3.1 Authorized Access Only

Remote Staff may only access data strictly necessary for their assigned tasks.

3.2 Account Security

- All accounts must be protected with strong passwords
- Two-Factor Authentication (2FA) is required where available
- Login credentials must never be shared

3.3 Device Restrictions

Access to Client data must only occur on:

- Secure, personal devices
- Devices with updated antivirus and operating systems

Public or shared computers are strictly prohibited.

4. DATA HANDLING & STORAGE

4.1 Approved Storage Platforms

All Client files must be stored and managed using approved platforms such as:

- [Google Drive / Dropbox / Company Server / Other]

4.2 Local Storage Limitations

- Files may only be temporarily stored on local devices when necessary
- Sensitive files must not be permanently stored on personal devices

4.3 File Organization

All files must be:

- Clearly labeled
- Stored in designated project folders
- Managed in accordance with Company workflow standards

5. DATA TRANSMISSION

5.1 Client data must only be shared via secure and approved channels.

5.2 The use of:

- Personal email accounts
- Messaging apps (unless approved)
- Unauthorized file-sharing platforms

is strictly prohibited.

5.3 Sensitive data must not be transmitted without encryption or secure access controls where applicable.

6. CONFIDENTIALITY OBLIGATION

6.1 All Remote Staff must treat Client data as strictly confidential.

6.2 Remote Staff shall not:

- Disclose Client information to unauthorized parties
- Use Client data for personal or external purposes
- Retain copies for future use

6.3 This obligation continues even after the project or engagement ends.

7. DATA RETENTION & MANDATORY DELETION

7.1 Project Completion Rule

Upon final delivery and completion of the project, all Remote Staff are required to:

- Delete all Client-related files from:
 - Personal devices
 - Local storage
 - Unauthorized cloud platforms

7.2 Deletion Timeline

All data must be deleted within **2 days** of project completion unless otherwise instructed.

7.3 Confirmation Requirement

Remote Staff may be required to provide written confirmation that all Client data has been permanently deleted.

7.4 Exception

Only the Company may retain archival copies where necessary for legal, contractual, or portfolio purposes, subject to Client approval.

8. DATA BREACH & INCIDENT RESPONSE

8.1 Any suspected or actual data breach must be reported immediately to the Company.

8.2 Remote Staff must:

- Provide full details of the incident
- Cooperate with investigation and mitigation efforts

8.3 Failure to report a breach is considered a serious violation of this Protocol.

9. PROHIBITED ACTIONS

Remote Staff are strictly prohibited from:

- Downloading or copying data beyond project needs
- Using unauthorized software or tools
- Sharing files outside approved systems
- Retaining Client data after project completion
- Using Client work for personal portfolios without approval

10. COMPLIANCE & ENFORCEMENT

10.1 Compliance with this Protocol is mandatory.

10.2 Violations may result in:

- Immediate termination of engagement
- Legal action
- Financial liability for damages caused

11. ACKNOWLEDGMENT

By signing below, the Remote Staff acknowledges that they have read, understood, and agree to comply with this Data Security Protocol.

REMOTE STAFF

Name: _____

Signature: _____

Date: _____

COMPANY REPRESENTATIVE

Name: _____

Signature: _____

Date: _____