MAJOKA WORKFORCE SOLUTIONS

MWS DATA PRIVACY & DATA HANDLING FRAMEWORK

Protecting client information through controlled access, secure working practices and defined workforce obligations.

Purpose

MWS provides workforce solutions to clients through structured professional engagements. During these engagements, assigned professionals may access confidential business information, personal information, intellectual property, source code, credentials, technical documentation, internal records and other client-controlled information.

MWS recognises that unauthorised access, disclosure, copying, retention or misuse of such information can create material security, operational and commercial risks.

This framework describes MWS's approach to protecting client information through enforceable contractual obligations, controlled access, secure working environments, endpoint safeguards, responsible data handling and documented workforce procedures.

MWS aims to incorporate security into the way each engagement is structured and operated, rather than relying solely on contractual assurances.

01 Data Protection Principles & Scope

MWS applies the following principles when handling client information:

Purpose limitation:
Information is used only for authorised engagement activities.

Data minimisation:
Access to information is limited to what is reasonably required for assigned responsibilities.

Confidentiality:
Client information must not be disclosed to unauthorised persons or organisations.

Controlled access:
Access is granted according to approved responsibilities and permissions.

Secure handling:
Information is handled through approved systems, tools and communication channels.

Retention limitation:
Information is not retained beyond the authorised purpose or applicable retention requirements.

Accountability:
Relevant approvals, access changes, security incidents and offboarding actions are documented where appropriate.

This framework applies to MWS personnel (MP) and assigned professionals who access, process, receive, store or otherwise handle client information through MWS engagements.

It covers information held electronically, displayed on screens, communicated verbally, printed, transferred between systems or otherwise made accessible through the engagement.

02 Contractual & Confidentiality Safeguards

MWS establishes contractual obligations to define the responsibilities of the parties for protecting client information, confidential materials and intellectual property.

2.1 Client Confidentiality Agreements

The applicable Master Services Agreement (MSA), Non-Disclosure Agreement (NDA) or other contractual documentation establishes the confidentiality obligations governing the engagement.

Depending on the agreement, these obligations address:

- The definition and treatment of confidential information.
- Permitted use and authorised disclosure.
- Protection of client information, credentials, records and intellectual property.
- Restrictions on unauthorised copying, retention, transfer and commercial use.
- Security incident reporting and cooperation.
- Return or deletion of information when access or the engagement ends.
- Continuing confidentiality obligations after termination.

2.2 Professional Confidentiality Obligations

Assigned professionals are bound by applicable confidentiality and information-security obligations through their MWS employment agreement and other relevant undertakings.

These obligations prohibit unauthorised disclosure, copying, retention, personal use or commercial exploitation of client information and intellectual property.

The obligations are intended to remain enforceable in accordance with the applicable contractual terms and law, including after the engagement or employment relationship ends where the obligations survive termination.

2.3 Flow-Down of Client Security Requirements

Relevant client security requirements are communicated to assigned professionals and incorporated into applicable working obligations before access is granted.

These requirements may cover acceptable use, access restrictions, confidentiality, information handling, approved tools, security incident reporting, intellectual property and offboarding.

MWS reviews material requirements to determine whether they can be implemented within the proposed engagement structure. Requirements that cannot be met must be escalated and resolved before the affected access or activity proceeds.

2.4 Intellectual Property & Contractual Remedies

The applicable contractual documentation addresses ownership or assignment of engagement-related work product, including deliverables, source code, scripts, documentation, designs, inventions and other materials created within the scope of the engagement.

Where appropriate, contractual documentation may include indemnification, remedies and liability provisions relating to confidentiality breaches, unauthorised use of information and intellectual property infringement.

The precise scope of these provisions, including applicable exclusions and limitations, is governed by the executed agreements and applicable law.

03 Access Management & Control

Access to client systems and information is granted only for authorised engagement purposes.

MWS expects the following controls to be applied through client systems, MWS procedures or both, as appropriate to the engagement.

3.1 Individual Accounts

Professionals use individually assigned accounts wherever supported. Shared accounts and credentials are avoided unless specifically authorised and appropriately controlled.

3.2 Least-Privilege Access

Permissions are restricted to the systems, applications, information, resources and actions required for assigned responsibilities.

Access to sensitive information and administrative functions must not exceed what is reasonably necessary for the authorised work.

3.3 Access Approval

Access is granted following the required approval from the client or authorised system owner. Employment by MWS does not, by itself, authorise access to client systems or information.

3.4 Multi-Factor Authentication

Professionals enroll in multi-factor authentication (MFA) wherever the client's systems offer it. MWS recommends that clients enforce MFA for remote access, sensitive systems and privileged accounts.

3.5 Access Reviews

Access permissions are reviewed when responsibilities change, access is no longer required or the engagement requires reassessment. MWS also confirms with the client, 6 months, the list of assigned professionals and whether their access is still required.

3.6 Logging & Traceability

Available system logs and access records are used to support accountability, review and investigation, subject to the relevant platform configuration, authorisation and retention requirements.

3.7 Prompt Access Revocation

Access is removed when it is no longer required, when an assignment ends or when suspension is necessary to address a security concern. MWS notifies the client (by the professional's last working day, or within 48 hours of an unplanned exit or role change) and requests revocation of the related access.

04 Client-Controlled Infrastructure & Secure Working Environment

4.1 Preferred Operating Model

MWS prioritises client-controlled infrastructure and approved working environments wherever technically feasible.

Depending on the engagement, these may include:

- Client-managed Virtual desktop infrastructure (VDI).
- Client-controlled remote cloud workspaces.
- Session-based access to authorised systems.
- Client-approved VPN and authentication mechanisms.
- Client-managed applications, cloud platforms, repositories and collaboration environments.

The selected arrangement depends on the client's security requirements, technical architecture and the work being performed.

4.2 Keeping Client Information Within the Authorised Environment

Where technically feasible, client information, credentials, source code, documents, records and other sensitive materials should remain within the client's authorised environment.

Professionals must not download, export, copy or transfer client information to a local device, personal account or external system unless the activity is necessary, authorised and consistent with the applicable security requirements.

4.3 Local Processing & Storage

Some work may require local applications, command-line tools, development utilities, scripts, testing resources or other processing capabilities.

Where local processing or storage is necessary, it must be authorised and the device must meet the controls in Section 5, including full-disk encryption (5.6). Additional controls may include:

- Restricted local storage and file-transfer permissions.
- Secure credential handling.
- Removal of local copies when no longer authorised or necessary.

> MWS does not assume that all work can be performed entirely within a client-controlled environment. The objective is to minimise unnecessary local handling while preserving the technical requirements of the engagement.

05 Device & Endpoint Security

Where a professional uses a personal or otherwise non-MWS-managed device to access client systems or information, the device must meet the applicable security requirements established for the engagement.

The minimum expected controls include:

5.1 Supported & Updated Operating System

The device must run a supported operating system, with security updates and critical patches applied within the required timeframes.

5.2 Malware Protection

Built-in or approved endpoint protection must be enabled and kept updated.

5.3 Screen Lock & Device Authentication

Strong device authentication and automatic screen locking must be enabled to reduce the risk of unauthorised physical access.

5.4 Multi-Factor Authentication

MFA must be used for supported client access wherever required.

5.5 Password Management

Credentials must be stored securely through an approved password manager or equivalent control. Password reuse, insecure credential storage and unauthorised credential sharing are prohibited.

5.6 Full-Disk Encryption

Full-disk encryption is required where client information or credentials are stored locally, or where the client requires it.

5.7 Device Integrity

Unauthorised software, disabling required security controls and insecure device configurations must be avoided. Devices that do not meet required security conditions must not be used to access affected client resources until the issue is resolved.

5.8 Local Data Restrictions

Client information must not be stored locally unless authorised. Where local storage is approved, the applicable security and deletion requirements must be followed.

5.9 Lost or Compromised Devices

Loss, theft, suspected compromise or unauthorised access involving a device used for client work must be reported promptly through the designated reporting channel.

Where the required endpoint controls cannot be implemented on a professional's device, the issue must be resolved before access is granted. A client-managed device or controlled virtual workspace may be used as an alternative.

MWS does not represent that all personal endpoints are centrally monitored or managed unless such controls are actually implemented.

5.10 Device Verification

Before access is granted, the professional confirms these controls through a signed device checklist (with supporting evidence, such as screenshots of encryption and update status). The confirmation is repeated 6 months and whenever the device changes. MWS can provide completed checklists to the client on request.

06 Secure Work Practices & Data Handling

Professionals must follow the client's applicable security instructions and MWS's confidentiality and information-handling obligations.

Unless specifically authorised, professionals must not:

- Send client information to personal email accounts or personal cloud-storage services.
- Copy confidential documents, source code, credentials, records or other client materials to personal repositories.
- Upload client information to public or unapproved AI tools and external services.
- Transfer confidential information through unauthorised messaging or file-sharing platforms.
- Share credentials, bypass access restrictions or disable required security controls.
- Retain client information for personal projects, demonstrations, portfolios or unauthorised commercial use.
- Photograph, record or reproduce confidential information without authorisation.
- Retain copies of client information after the authorised business purpose has ended.

Where AI-assisted tools or external processing services are proposed for client work, their use must be authorised and appropriate to the sensitivity of the information involved.

6.1 Secure Clean-Desk & Workspace Practices

Professionals must maintain a working environment appropriate to the sensitivity of the information they access.

This includes:

- Locking screens when devices are unattended.
- Preventing unauthorised persons from viewing confidential information.
- Keeping printed confidential information secure and out of public view.
- Avoiding unauthorised photographs, screen recordings or screenshots.
- Disposing of authorised printed material securely.
- Conducting work in a setting that reasonably protects confidential information from unauthorised observation or access.

6.2 Secure Communications & Electronic Records

Engagement-related communications should take place through approved workplace channels wherever possible.

Relevant business records should be retained through the applicable platform or agreed process where available and appropriate. These records may support traceability, incident investigation and resolution of disputes.

Recording or monitoring of communications must follow applicable law, required notices or consents, and client policy. MWS does not assume that every communication is recorded.

07 Personnel Verification & Security Responsibilities

MWS's talent vetting and verification process provides a foundation for assessing professional background and relevant identity information before deployment.

Depending on the role and applicable requirements, verification may include:

- Identity verification.
- Employment history.
- Education or qualification verification.
- Professional references.
- Other relevant checks agreed for the engagement.

7.1 Security Onboarding

Before access is granted, applicable requirements include:

- Completion of required verification.
- Acknowledgement of confidentiality and information-security obligations.
- Completion of relevant security onboarding.
- Understanding of approved access methods, tools and working procedures.
- Awareness of the process for reporting suspected security incidents.

7.2 Ongoing Responsibilities

Professionals must follow approved access and information-handling requirements, protect credentials, report suspected incidents promptly and cooperate with authorised investigations and corrective actions.

7.3 Protection of Identity & Personnel Records

MWS collects and retains identity and verification information only for defined, legitimate purposes and subject to applicable requirements.

Access to identity documents and sensitive personnel records is restricted to authorised personnel. Collection, storage, sharing and retention must be proportionate to the purpose.

Government-issued identity documents, including Aadhaar or PAN where relevant, are not collected or shared indiscriminately. Appropriate verification alternatives, masking and restricted access should be used where applicable.

Client-facing verification outcomes or reports should be preferred over sharing raw identity documents unless disclosure is necessary, authorised and legally appropriate.

08 Security Incident Reporting & Response

A security incident may include suspected or confirmed unauthorised access, disclosure, copying, loss or misuse of client information, compromised credentials, a lost device or a failure of an applicable security control.

MWS follows a structured response approach.



8.1 Detect & Report

The professional promptly reports the suspected incident through the designated MWS or client reporting channel. Suspected incidents must not be concealed or deliberately delayed.

8.2 Contain

Appropriate steps are taken to limit further exposure. These may include suspending credentials, restricting access or coordinating other containment measures with the relevant system owner.

8.3 Investigate & Preserve Evidence

Available facts and relevant records are reviewed, and appropriate evidence is preserved. Professionals must not destroy or alter relevant evidence outside authorised procedures.

8.4 Notify & Coordinate

MWS communicates with the designated client contact in accordance with the agreed incident process and applicable requirements.

8.5 Remediate

Corrective actions are identified, documented and implemented as appropriate to address the incident and reduce the likelihood of recurrence.

MWS cooperates with the client in investigating and addressing incidents within the scope of its responsibilities. Notification timing and mandatory reporting are governed by applicable law and the relevant contractual obligations.

09 Offboarding, Access Revocation & Data Deletion

Offboarding is a mandatory control when a professional leaves an engagement, changes to a role that no longer requires access, or otherwise ceases to be authorised.

MWS coordinates the applicable offboarding process with the client and relevant system owners.

9.1 Mandatory Offboarding Checklist

The process includes, as applicable:

- ☐ Confirming the effective end date and scope of access removal.
- ☐ Revoking client accounts, VPN, virtual desktop, application, repository, production and privileged access.
- ☐ Removing access to communication channels, portals, shared workspaces and internal systems that are no longer required.
- ☐ Recovering client-owned devices, access tokens, keys, credentials and other issued assets.
- ☐ Returning client information and work product through the authorised channel.
- ☐ Deleting unauthorised local copies, downloads, cached files and other retained client information.
- ☐ Checking for unauthorised copies in personal email, cloud storage, repositories and removable media under the professional's control.
- ☐ Obtaining a signed return, deletion and non-use declaration.
- ☐ Recording authorised retention exceptions, including applicable legal retention requirements or controlled backups.
- ☐ Retaining the appropriate completion record and obtaining client acknowledgement where required.

9.2 Written Return, Deletion & Non-Use Declaration

The departing professional is required to confirm, as applicable, that:

- Client information and property have been returned or handled in accordance with authorised instructions.
- Unauthorised copies have been deleted and no known unauthorised copies have been retained.
- Client credentials and access devices have been returned or surrendered as required.
- Client information and intellectual property have not been retained or used for personal or unauthorised commercial purposes.
- Continuing confidentiality, intellectual property and non-use obligations remain binding where applicable.

MWS may provide the client with the relevant signed declaration or offboarding completion record, subject to applicable confidentiality and privacy requirements.

Where appropriate, MWS may request written client acknowledgement of receipt or closure of the offboarding process.

> A signed declaration is an attestation and does not, by itself, prove technical deletion from every possible storage location. Where client-controlled systems are used, access revocation and available system records provide additional evidence of completion.

10 Responsibilities & Operating Model

The division of responsibility is intended to remain clear throughout the engagement.

Client Responsibilities	MWS Responsibilities	Assigned Professional Responsibilities
The client defines its security requirements, approves access to its systems, determines permitted tools and environments, and maintains control of client-managed infrastructure and its associated security configurations.	MWS manages applicable workforce confidentiality obligations, communicates relevant security requirements, coordinates workforce offboarding and incident escalation, and maintains the operational records within its responsibility.	The assigned professional uses client information only for authorised work, follows approved access and handling requirements, protects credentials, reports suspected incidents and complies with return or deletion instructions.

> Where a requirement depends on a control that MWS or the client has not implemented, the limitation must be identified and resolved before the affected activity proceeds.

MWS Security Operating Principle

> **Authorised access. Controlled environments. Confidential handling. Documented offboarding.**

MWS prioritises secure working environments and applies contractual, access, endpoint and workforce safeguards to reduce the risk of unauthorised access, disclosure, retention or misuse of client information.

The objective is to make information security part of the engagement's operating structure rather than relying solely on contractual promises.

Important Note

This framework describes MWS's data-protection and information-security approach. It is not an ISO/IEC certification, independent security audit, guarantee that data leakage cannot occur, or substitute for legal advice.

Specific security controls and legal obligations may vary according to the client environment, information sensitivity, engagement structure, contractual requirements and applicable law. The applicable contractual documents and agreed security requirements govern the engagement.