1.1. Policy Statement

This Master Service Agreement (MSA) Policy Framework ("Policy") outlines essential requirements and guiding principles for EY when entering into MSAs with the Government of Uganda (GoU), HCL Tech India (HCL), and the Government of India (GoI) ("Target Clients"). Its purpose is to manage risk, ensure consistency, protect EY's interests, and maintain compliant client relationships.

1.2. Objectives

* Standardize EY’s MSA approach with Target Clients.
* Mitigate legal, financial, operational, and reputational risks.
* Ensure compliance with laws, regulations, and EY Global policies.
* Protect EY’s intellectual property and confidential information.

1.3. Scope and Applicability

This Policy applies to all EY personnel involved in the proposal, negotiation, drafting, review, approval, and execution of MSAs and related Statements of Work

(SOWs) with Target Clients for all service lines. Deviations require documented approval from EY Legal and Risk Management.

2.1. General Principles

* **Risk Mitigation:** Prioritize protection of EY's assets, reputation, and financial stability.

* **Clarity & Precision:** Ensure unambiguous terms reflecting mutual intent.

* **Fairness & Reasonableness:** Strive for commercially balanced agreements.

* **Compliance:** Adhere strictly to all applicable laws, regulations, and professional ethics.

* **Scope Definition:** Clearly define service scope in MSAs and SOWs.

2.2. Specific Principles for Government Clients (GoU, GoI)

* **Sovereign Immunity & Procurement:** Understand implications; seek waivers where possible. Comply with public procurement laws and anti-corruption standards.

* **Payment & Termination:** Anticipate longer payment cycles. Negotiate fair compensation for any termination for convenience.

* **Data & Audit:** Address data sovereignty/localization and anticipate heightened audit scrutiny.

2.3. Specific Principles for Large Technology Clients (HCL)

* **Intellectual Property & Data Security:** Expect sophisticated IP negotiations and stringent data security/privacy requirements (including DPAs).

* **Service Levels (SLAs) & Liability:** Prepare for detailed SLAs and robust negotiation on indemnification and limitation of liability.

* **Subcontracting:** Address HCL's likely controls over EY's use of subcontractors.

3.1. Scope of Services & Statements of Work (SOWs)

* MSA governs SOWs. Clear process for SOW execution and change control.

3.2. Term and Termination

* Initial term, renewal. Termination for cause (with cure), and for convenience (negotiate EY's rights/compensation carefully, especially if Client demands this right). Effect of termination (data return, final payments, survival).

3.3. Fees, Invoicing, and Payment Terms

* Reference SOWs for fees. Clear invoicing process, payment terms (e.g., Net 30-60, anticipate longer for Government), late payment provisions, tax handling (fees exclusive of taxes).

3.4. Representations and Warranties

* Mutual (authority, due organization). EY (professional service, rights to perform). Client (accuracy of provided info, rights to data). Disclaimer of other warranties.

3.5. Intellectual Property Rights (IPR)

* **Background IPR:** Each party retains its own.

* **Foreground IPR:**

    * *EY Preferred:* EY owns methodologies, tools. Client licensed for deliverables for internal use.

* *Negotiation Point:* Clearly distinguish Client-specific deliverables from EY's underlying IPR. EY must retain rights to its core assets and residual knowledge.

3.6. Confidentiality

* Definition of Confidential Information. Obligations to protect, use only for MSA purposes, limit disclosure. Exclusions (public domain, prior possession, etc.). Compelled disclosure. Return/destruction on termination. Survival of obligations.

3.7. Data Protection and Privacy

* Compliance with all applicable laws (e.g., Uganda DPA, India DPDP Act, GDPR if relevant).

* If EY is a Data Processor: Process only on Client (Controller) instructions, implement security measures, assist Controller, manage sub-processors, notify breaches, handle data deletion/return.

* Data Processing Addendums (DPAs) are likely required, especially for HCL and sensitive government data, and must align with EY global standards.

3.8. Indemnification

* **EY Indemnifies Client:** For specific third-party claims (e.g., EY gross negligence, IPR infringement by EY deliverables – excluding Client materials). Subject to conditions (notice, control, cooperation).

* **Client Indemnifies EY:** For specific third-party claims (e.g., Client misuse, Client-provided materials/data).

* Seek mutual and appropriately capped indemnities.

3.9. Limitation of Liability (LoL) – CRITICAL FOR EY

* **Exclusion of Indirect/Consequential Damages:** Mandatory.

* **Cap on Direct Damages:** EY's aggregate liability must be capped (e.g., to fees paid under SOW/MSA over a defined period – typically 12 months).

* **Carve-outs from Caps:** Negotiate carefully. Resist unlimited liability. Certain standard carve-outs (e.g., death/personal injury by negligence, willful misconduct) may be unavoidable by law. Aim to keep confidentiality breaches and indemnities subject to the overall cap or a separate, reasonable super-cap.

4.2. HCL Tech India (HCL)

* **IPR & Data Security:** Expect stringent demands for IP ownership (negotiate robustly for EY's background IP/tools) and comprehensive data security/privacy obligations (DPDP Act, global standards). Detailed DPAs are standard.

* **SLAs & Liability:** Detailed SLAs with potential service credits. HCL will push for broad indemnities and high liability caps.

* **Global Operations:** Consider implications if services impact HCL's global operations or data from other jurisdictions (e.g., GDPR).

5.1. Engagement Team Responsibilities

* The Engagement Partner is accountable for initiating the MSA process using EY-approved templates.

* The team must understand client requirements and conduct initial negotiations aligned with this Policy and EY Global risk standards.

5.2. Legal and Risk Review (Mandatory)

* EY Legal and Risk Management must review and approve all MSAs with Target Clients prior to execution.

* This review will assess compliance with this Policy, legal enforceability, risk exposure, and alignment with EY Global standards.

* Guidance will be provided for non-standard clauses or significant deviations. Approved deviations must be documented.

5.3. Partner Approval

* The final MSA, incorporating Legal and Risk feedback, must be approved by the Engagement Partner and any other designated approving Partners (e.g., Risk Management Partner, Regional Leadership) as per EY policy.

* Approval signifies acceptance of commercial terms and residual risks.

6.1. Relevant EY personnel must receive training on this Policy and have access to it via EY internal resources. Regular updates will be provided.

7.1. This Policy will be reviewed annually by the Policy Owner, or as needed due to changes in law, EY strategy, or lessons learned. Amendments require approval from designated EY leadership.

8.1. Standard EY SOW templates and Data Processing Addendum (DPA) templates must be utilized. These

contain detailed checklists and prescribed language for common engagement elements and data protection requirements, respectively. Refer to EY Legal and Risk for the latest versions.

8.2. Country-Specific Legal & Regulatory Checklists (for internal use) should be consulted to ensure local compliance points for Uganda and India are addressed.