# REVIEW GUIDANCE FOR MASTER SERVICES AGREEMENT (CUSTOMER)

## REVIEW GUIDANCE FOR MASTER SERVICES AGREEMENT (CUSTOMER)

This document is intended to provide a practical, non-binding checklist for reviewing and negotiating a **customer-provided** Master Services Agreement (MSA).

It is not part of any agreement. It does not modify any agreement, create obligations, or grant rights. It is operational guidance only.

## 1. How to use this guidance

- **Goal.** Triage customer paper quickly, identify negotiation hotspots, and protect Alescent's minimum viable contracting posture.
- **Method.** Review clause families in the order below and classify each as: **Critical**, **Essential**, **Important**, or **Preferred**.
- **Escalation.** If a **Critical** item cannot be resolved within acceptable range, escalate before signature.

## 2. Priority tiers

- **Critical.** Must be addressed to avoid disproportionate legal/financial exposure.
- **Essential.** Strongly preferred; exceptions require explicit acceptance and mitigation.
- **Important.** Material, but flexible within bounds.
- **Preferred.** Nice-to-have; negotiate opportunistically.

## 3. Checklist by clause family

### 3.1 Definitions, structure, and order of precedence (Essential)

- Ensure SOW precedence is clear.
- Ensure a later SOW can override the MSA only as explicitly stated.
- Confirm no hidden incorporation by reference to documents you have not reviewed.

### 3.2 Confidentiality and non-disclosure (Critical)

- Confirm confidentiality scope is reasonable and workable.
- Confirm confidentiality term is not perpetual for ordinary confidential information.
- Confirm trade secrets receive appropriate protection.
- Confirm compelled disclosure clause exists.
- Confirm confidentiality obligations can flow down to subcontractors reasonably.

### 3.3 Data protection, security, audit, and privacy (Critical)

- Confirm obligations match what Alescent can actually perform.
- Avoid unlimited audit rights, on-site audits, or excessive frequency.
- Confirm security obligations are bounded to what is in scope.
- Confirm breach notification timelines are realistic.

### 3.4 Intellectual property, work product, and background IP (Critical)

- Protect Alescent Background IP (methods, frameworks, patterns, tools, templates).
- Avoid language that assigns all work product, tools, or know-how to the customer.
- Ensure licenses are limited to the customer's internal use (unless otherwise intended).

### 3.5 Acceptance and change control (Essential)

- Ensure acceptance is time-bounded.
- Ensure rejection requires a single, comprehensive deficiency list.
- Ensure change control exists for scope changes.

### 3.6 Fees, invoicing, taxes, and payment terms (Critical)

- Avoid pay-when-paid / contingent payment unless explicitly intended.
- Avoid broad unilateral setoff rights.
- Ensure invoicing cadence and payment terms are workable.

### 3.7 Termination and effect of termination (Critical)

- Prefer no-fault termination with notice.
- Ensure payment for work performed and committed costs.
- Ensure survival clauses are sensible (confidentiality, IP, liability, etc.).

### 3.8 Warranties and disclaimers (Important)

- Avoid broad warranties inconsistent with advisory services.
- Ensure disclaimers are not prohibited outright.

### 3.9 Indemnities (Critical)

- Avoid broad indemnities unrelated to IP infringement or willful misconduct.
- Avoid indemnifying the customer for the customer's own negligence.

### 3.10 Limitation of liability (Critical)

- Ensure there is a cap.
- Avoid carve-outs that swallow the cap.
- Prefer consequential damages exclusion.

### 3.11 Subcontractors and personnel (Essential)

- Preserve the right to use subcontractors.
- Ensure flow-down obligations are manageable.

### 3.12 Publicity and branding (Preferred)

- Mutual consent for naming/logo use.

### 3.13 Dispute resolution and venue (Important)

- Ensure dispute mechanism is workable.
- Avoid one-sided remedies.

### 3.14 Miscellaneous (Important/Preferred)

- Assignment, force majeure, notices, counterparts.

## 4. Output artifact

When review is complete, produce:

- A short summary of redline hotspots and risk tiering.
- A list of Critical items accepted, rejected, or pending.
- Any mitigations (insurance, caps, scope limitations) tied to exceptions.