# Service Attachment for Co Managed Services

PUBLICATION PREVIEW | VERSION 0.2

This attachment describes Kortech's work alongside a customer's internal IT team. It applies only to the functions selected in the accepted order. The customer retains its internal IT leadership and business priorities, while each party performs the responsibilities assigned to it.

## 1 Scope and Ownership

Co-managed services may include escalation support, network administration, security operations, backup administration, after-hours coverage, field work, project assistance or evidence preparation. The service schedule identifies the systems, tools, access levels, support windows, exclusions and prices. Shared involvement does not replace a named owner for each task.

## 2 Responsibility Schedule

The parties maintain a responsibility schedule covering the applicable functions. It identifies who performs the work, who is accountable, who approves changes, the backup contact and the required evidence. Typical functions include monitoring, patching, firewalls, identity, backup and restore testing, security incidents, vendor escalation, compliance evidence and physical infrastructure. Unassigned functions must be resolved expressly rather than assumed to be covered by the other party.

## 3 Requests and Escalation

Requests use the designated intake and include business impact, affected assets and work already performed. The customer handles its agreed first-line scope and Kortech handles its selected escalation scope. Each escalation remains assigned until the receiving party accepts ownership. Parallel investigation must be coordinated to avoid conflicting or duplicate changes.

## 4 Access and Changes

Administrative roles, multifactor authentication, credential handling, logging and revocation follow the agreed access plan. Each party uses individually attributable accounts where supported and limits access to its authorized work. Material changes follow the approval process. Emergency containment authority must be expressly established; neither party may assume unrestricted authority over the other's systems or responsibilities.

## 5 Incident Coordination

The incident plan identifies technical leadership, customer decision makers, communication channels, evidence handling and external notification responsibilities. The parties promptly share relevant incident information and material actions. Personal information and health information duties follow the applicable DPA or business associate agreement. Assistance does not grant general authority to make public statements, admit liability or take destructive action.

## 6 Projects and Service Review

Project work has its own deliverables, dependencies and completion criteria in an accepted order or change. Repeated escalation demand may prompt a coverage review but does not unilaterally change price. The parties review unresolved tickets, access, asset changes, risks and planned work at the agreed cadence.

## 7 Transition

On transition, each party provides its assigned records and customer-owned access through the agreed secure process. The receiving party confirms ownership and continuity. Data retention, deletion, vendor transfers and any transition fees follow the applicable agreement.