sensys

CONFIDENTIAL PROPOSAL · MAY 2026

Managed IT, security & systems for Walks Devour.

A two-phase engagement to take Walks Devour from a parent-company tenancy to an independent, secure, 24/7-monitored IT estate — delivered cloud-to-cloud.

PREPARED FOR	PREPARED BY	ENGAGEMENT	DATE
Walks Devour	Sensys	Phase 1 + MSP	May 2026

01 EXECUTIVE SUMMARY

A clean break from the parent estate

Walks Devour is separating from its parent group's Microsoft 365 tenancy. It is proposed that Sensys will deliver the full transition to an independent Google Workspace estate over five weeks, then operate it as your managed services partner.

Phase 1 is a tightly-scoped migration project: email, identity and devices. Phase 2 is a long-term, fully-managed service combining 24/7 monitoring, EDR, email & phishing protection, SaaS backup, RMM patching and a single point of contact for every IT question your team will ever have. Both phase 1 and 2 are interdependent.

96 USERS MIGRATED	100 DEVICES TRANSITIONED
5 WEEK CUTOVER	24/7 MONITORED FROM DAY ONE

02 ENGAGEMENT MODEL

Two phases. One partner. Continuous outcome.

PHASE 1 · PROJECT

WEEKS 1–5

Migration & device transition

- M365 → Google Workspace email + contacts
- SPF / DKIM / DMARC hardening on walksdevour.com
- Windows laptops separated from parent domain
- Google-managed login installed remotely
- Mac devices configured with guidance

PHASE 2 · SERVICE

FROM WEEK 5 — CONTINUOUS

Ongoing managed IT & security

- 24/7 monitoring & SOC response
- RMM, patching & asset management
- Lola EDR, phishing defence, email filtering
- Google SaaS backup
- Helpdesk, reporting & quarterly roadmap

03 PHASE 1

Microsoft 365 → Google Workspace. Cloud-to-cloud, fully managed.

Email & identity

All mailboxes, folders, sent items, drafts, contacts, aliases and shared inboxes migrated using Google's native tooling.

Windows & Mac devices

Laptops separated from the parent domain and transitioned to Google-managed login — files, apps and settings preserved.

Security foundations

SPF, DKIM and DMARC published on walksdevour.com before any email is sent — anti-impersonation from day one.

04 EMAIL MIGRATION

How it works.

01

Authorise

A Global Admin on the Microsoft tenant approves read-only access. No passwords shared — single sign-in, single click.

02

Copy

Migration process copies every mailbox directly cloud-to-cloud. No data ever touches anyone's laptop.

03

Verify

We sample mailboxes and confirm dates, attachments and folder structure arrived intact before cutover.

WHAT MOVES

- All received and sent emails
- Folders (become Gmail labels)
- Contacts
- Shared inboxes (→ Google Groups)
- Distribution lists (→ Google Groups)
- Email aliases (info@, sales@…)
- Read / unread & flagged status

HANDLED SEPARATELY

- Calendar events — recreated by staff
- Files (OneDrive / SharePoint) — moved by dept. heads
- Outlook rules & signatures — recreated in Gmail
- Teams chat history — archived separately if needed
- OneNote notebooks — exported by users
- Outlook categories — not supported in Gmail

05 EMAIL SECURITY

Three layers, configured before the first email is sent.

SPF

Sender Policy Framework

Tells receiving servers which servers are allowed to send email for walksdevour.com — prevents impersonation.

DKIM

DomainKeys Identified Mail

Adds a digital signature to every outgoing email proving it hasn't been tampered with in transit.

DMARC

Domain-based Message Authentication

Tells receivers what to do when SPF or DKIM fails — monitor, quarantine, or reject.

06 CONTINUITY

No-one misses an email during handover.

The parent company retains the existing domains. After migration, their IT team configures forwarding so any mail sent to the old address arrives in the new @walksdevour.com inbox — automatically.

SENDER WRITES TO
john@cityexperiences.com

MICROSOFT FORWARDS
to john@walksdevour.com

ARRIVES IN GMAIL
no user action required

ACTIVE 6–12 MONTHS
while contacts are updated

07 DEVICE TRANSITION

Windows laptops, separated from the parent domain — without losing a single file.

THE PROBLEM

Today, staff sign in to laptops with parent-company credentials stored (cached) on each device. When those accounts are removed from the parent's system, those cached credentials stop working — and without a plan, staff could be locked out of their own laptops.

OUR SOLUTION

We transition each laptop to a local account first — preserving everything on the machine — then connect it to Google so staff log in with their new @walksdevour.com credentials going forward. All remote.

01

Management tool installed

Parent IT deploys our RMM agent via ManageEngine. Users notice nothing.

02

Laptop separated

Disconnect from parent domain, convert to local account, all files preserved by migration software.

03

Google login installed

Google Credential Provider replaces the Windows login screen with a Google sign-in.

04

User signs in

On next restart, sign in with @walksdevour.com. Desktop, files and apps load exactly as before.

08 STAFF EXPERIENCE

Monday morning, with one new login screen.

BEFORE

Email already working in Gmail. Files already in Google Drive. The laptop works as normal.

THE CHANGE

Done remotely over a weekend. Zero action required from staff.

MONDAY

A Google sign-in appears. Enter your @walksdevour.com login. Desktop loads exactly as you left it.

09 MAC DEVICES

Lighter touch for Mac users.

Macs typically aren't tied to the parent company's login system in the same way as Windows. Sensys provides remote guidance per device — roughly 15–20 minutes — and the user is done.

- Add the new Google account in System Settings → Internet Accounts
- Remove the old Microsoft / Exchange account
- Install Chrome and sign in with @walksdevour.com
- Email, calendar and contacts sync automatically

Five weeks, end to end.

WEEK	WHAT HAPPENS	OWNER
Week 1	Google Workspace tenant created, accounts set up, email security configured, RMM agent deployed	Sensys + Parent IT
Week 1–2	Email copied in background — users keep working in Outlook, zero disruption	Sensys
Week 2	Mailbox sample verification — history, attachments, folders confirmed intact	Sensys
Week 2–3	Mail flow switched to Google. Users start sending from @walksdevour.com	Sensys
Week 3	Department heads finish moving files to Google Drive	Walks Devour
Week 3–4	Windows laptops transitioned to Google login over a weekend	Sensys
Week 4	Mac devices configured, final checks, go-live support	Sensys
Week 5+	Parent company removes accounts from their system. MSP service active.	Parent IT

Light, well-defined dependencies.

From parent company IT

- Global Admin to approve the migration tool (one click, ~30s)
- Deploy Sensys RMM agent to ~100 devices via ManageEngine
- Configure forwarding from old addresses to new addresses post-migration

From Walks Devour

- Confirm shared inbox list (info@, sales@, accounts@…)
- Department heads migrate files from OneDrive / SharePoint to Drive
- Staff recreate calendar events in Google Calendar
- Staff update external contacts with new addresses

Always-on managed services from the moment Phase 1 lands.

Managed IT

RMM, patching, asset management, helpdesk and a single point of contact for every IT question.

Cyber security

Lola-powered EDR, phishing link detection, email filtering, security awareness and Google SaaS backup.

Systems & platform

Google Workspace administration, identity, MDM policies, integrations and continuous improvement.

Your entire IT estate. One login.

Obeya is the Sensys client command centre. One secure login for Walks Devour to run users, devices, security and strategy — without juggling vendors or consoles.

User lifecycle

Add, remove and re-provision staff in seconds. Joiners, movers and leavers handled from one screen.

Total device ownership

Assign, track and retire every laptop, phone and peripheral against an owner and location.

IT hardware store

Full e-commerce catalogue for approved devices and accessories — built-in approvals and delivery tracking.

Lola security monitoring

Per-user and per-device cyber posture from the Lola stack — EDR, phishing, email and backup status, live.

IT & AI education

On-demand learning paths and AI literacy for every user, tracked against role and team.

Strategy & compliance

Technology roadmap and cyber-compliance evidence — one pane of glass for the board and auditors.

Everything Walks Devour needs from an IT partner — under one contract.

RMM

Continuous remote monitoring and management of every endpoint.

Patching

OS and third-party patching cycles on a defined cadence.

Asset management

Live inventory of every device, user and software entitlement.

Helpdesk

Multi-channel support, named engineers, defined SLAs.

24/7 monitoring

Round-the-clock SOC eyes on every alert from every device.

Reporting

Monthly service review and quarterly roadmap with your sponsor.

Powered by Lola — layered, automated, monitored.

EDR

Endpoint Detection & Response on every device — behaviour-based threat detection with auto-isolation.

Phishing link detection

Real-time inspection of every link before a user clicks — stops credential-harvest pages cold.

Email filtering

Pre-delivery filtering for spam, malware, BEC and impersonation, layered on top of Gmail's native defences.

Google SaaS backup

Daily independent backup of Gmail, Drive, Shared Drives, Contacts and Calendar — restored in minutes, not days.

Security awareness

Continuous phishing simulations and short-form training tuned to each user's risk.

Identity hardening

MFA, conditional access, password posture and admin segregation across the entire Workspace tenant.

16 24/7 MONITORING

Eyes on glass. Every endpoint. Every hour.

The Sensys SOC watches every alert from every device — telemetry from EDR, RMM, email gateway and Workspace audit logs is correlated in one place, with an analyst on shift every minute of every day. When something happens, it gets triaged, contained, and communicated.

<15m CRITICAL ALERT TRIAGE	**<30m** CONTAINMENT FOR ACTIVE THREATS
365d DAYS A YEAR COVERED	**100%** ENDPOINTS MONITORED

Targets you can hold us to.

PRIORITY	DEFINITION	RESPONSE	RESOLUTION TARGET
P1	Business down / major security incident	15 min	4 hours
P2	Single user blocked / degraded service	30 min	8 hours
P3	Standard request / minor issue	2 hours	1 business day
P4	Scheduled change / consult	4 hours	By agreement

A rhythm that keeps IT visible to the business.

Monthly service review

Ticket trends, SLA performance, security posture, asset state — delivered to your nominated sponsor.

Quarterly roadmap

A rolling 12-month view of platform changes, risks closed and improvements proposed.

Annual strategy

Budget-aligned IT plan — capacity, refresh cycles, regulatory and AI-readiness.

Phase 1 hands directly into steady-state — no second mobilisation.

01

Documentation captured during migration

02

RMM, EDR and backup already deployed

03

Helpdesk channels published to staff

04

First service review within 30 days of go-live

A partner built for businesses that need IT to just work.

Migration specialists

We've lots of experience with data migration, O365 & Workspace.

Security-first

Lola stack, 24/7 SOC and MFA-everywhere as the default — not an upsell.

Senior engineers

You speak to people who can fix it, not a triage layer.

Transparent service

Live ticket dashboards, real SLAs, monthly reviews — no black box.

MORE THAN AN MSP

Solutions, Lean thinking, AI & Automation — built in.

Alongside the managed service, you get direct access to our Solutions team and Lean, AI and Automation specialists. We sit with your people to refine technology processes — making them flow — then automate the work that shouldn't need a human in the loop.

From contact centres to finance, operations to back-office: agentic AI agents, automated workflows and integrations across your stack. The same partner that keeps the lights on also helps you compound productivity, quarter on quarter.

- Lean process design
- Agentic AI agents
- Workflow automation

A clear commercial framework.

Indicative structure for discussion. Final figures confirmed in the commercial schedule alongside this proposal.

PHASE 1 — ONE-OFF

Migration project

€12,800

Once-off, payable upfront

- Fixed fee
- Covers 96 users / 100 devices
- 5-week delivery window
- Includes Google Workspace setup

PHASE 2 — MONTHLY

Managed services

CORE MSP — CHOOSE ONE TERM:

€65	€71
PER USER / MONTH	PER USER / MONTH
36-month term	12-month term

REQUIRED ADD-ON

€28 per user / month

LOLA CYBER

EDR, email & phishing protection, SaaS backup, anti-virus, ransomware protection, cyber incident response, RMM

Total per user / month (36-month)	€93
Total per user / month (12-month)	€99

- Unlimited helpdesk & 24/7 SOC monitoring
- Additional devices priced separately
- Assumes 1:1 user to device relationship; additional devices charged separately for device licence

EXCLUDED Google Workspace licence cost — procured directly from Google by Walks Devour. All pricing excludes VAT.

NOTE The two phases are interdependent. The migration cost assumes Walks Devour onboards as a Sensys managed services client, with the MSP tool set deployed remotely via RMM. Both phases are costed together and contracted under a single Master Services Agreement, supplied for review on acceptance of this proposal.

Next steps.

THIS WEEK	NEXT	THEN	THEN
Review proposal	MSA & SoW counter-signed	Project plan	Software licence ordered, user onboarding & kick off migration

YOUR SENSYS LEADS

Ben Killeen & Alan Hogan

Directors

Supported by our team of technical engineers.