



DETAILED COMPANY & SERVICES PROFILE

Technology that moves your business forward.

Managed IT & AMC. Cybersecurity. Installations.
Websites & mobile apps. Marketing. AI.
CRM, ERP & POS.

A PRACTICAL GUIDE TO OUR SERVICES & DELIVERY

SERVING BUSINESSES ACROSS THE UAE

Business technology, working together.

From maintaining the office network to connecting your website, sales process and business systems.

Who we are

Techvenation brings together IT support, infrastructure, cybersecurity, digital services and business applications. With 10 years of UAE market experience, we help organisations translate day-to-day needs into practical technology decisions.

What we help you achieve

Keep staff productive, organise systems, strengthen your online presence and reduce repetitive work. Our services support new setups, growing teams, existing environments that need improvement and businesses seeking an ongoing technology partner.

How we work

We begin with your requirement, review the current setup and define a clear scope. Delivery can include assessment, procurement coordination, installation, configuration, development, testing, training and ongoing support, depending on the engagement.

Our service principles

Understand first

Match the recommendation to your workflow, budget and operating priorities.

Make ownership clear

Agree access, responsibilities, deliverables and support arrangements.

Build for continuity

Document the solution and plan its maintenance and future improvement.

UAE coverage: Abu Dhabi, Dubai, Sharjah, Ajman, Ras Al Khaimah, Fujairah and Umm Al Quwain. On-site arrangements are agreed by location.

OUR TECHNOLOGY RELATIONSHIPS

Our partners & leading brands.

Technology relationships supporting our IT, security, cloud and communication services.

AUTHORISED PARTNERS



SELECTED PARTNERS & BRANDS



Product and brand names are trademarks of their respective owners.

Your guide to the profile.

A detailed overview of support, delivery workflows and the systems we can help you put in place.

05 - 17

IT AMC, SOC & reporting

Support, maintenance, recovery, security monitoring, vulnerability review and service reporting.

18 - 24

Infrastructure & protection

Office installation, networks, servers, cloud, cyber threats, security controls and CCTV.

25 - 31

Websites & mobile apps

Web development, ecommerce, business portals, Android/iOS apps, launch and maintenance.

32 - 33

Digital marketing

Search visibility, content, advertising, social campaigns and meaningful measurement.

34 - 35

AI & automation

Customer assistants, workflow design, integrations, testing and human oversight.

36 - 43

Business systems & contact

CRM, ERP and POS features, integrations, implementation, training and contact.

An ongoing plan for your IT.

An annual maintenance contract brings agreed support and maintenance into one managed arrangement.

What an AMC does

Instead of treating each issue as an isolated repair, an AMC defines which users, devices and systems are supported, how requests are handled and what preventive work is scheduled. It creates a clearer process for everyday support and recurring technical needs.

Who it is suited to

Businesses without an internal IT department, teams needing additional expertise and organisations with several sites can all benefit from a defined support arrangement. The right scope depends on your equipment, applications, working hours and operational dependencies.

How Techvenation structures it

We assess the environment, identify priorities and propose a covered asset list, service activities, communication routes and commercial terms. Support is then delivered against that agreed scope and reviewed as your business changes.

Three parts of the service

Support

Resolve user issues and investigate faults affecting covered systems.

Maintenance

Carry out scheduled checks and approved improvements.

Review

Report recurring problems, open risks and recommended next actions.

AMC scope is defined in your agreement. Hardware, licences, major upgrades and specialist recovery are priced separately unless expressly included.

Know exactly what is covered.

A useful AMC starts with a clear inventory and a shared understanding of the work included.

Users and workplace devices

Coverage can include desktops, laptops, printers and business applications used by named teams. We record supported equipment and software, investigate common errors, assist with configuration and coordinate vendor support when the issue depends on a third party.

Shared business infrastructure

Servers, storage, switches, Wi-Fi, firewalls and backup systems can be included in the asset schedule. Support boundaries matter: maintaining a firewall is different from running a continuously staffed security monitoring service.

Changes and additional work

New branches, office moves, large migrations and new system installations are scoped as planned changes. Replacements, spare parts, subscriptions and out-of-scope work are identified before approval so that operational support and new delivery remain clear.

Your coverage schedule

Assets & locations

Record device counts, serial numbers, site details and key dependencies.

Support boundaries

Identify covered applications, vendor responsibilities and exclusions.

Commercial clarity

Agree visits, remote support, additional work and renewal terms.

Optional coverage can extend to CCTV, access control, telephony or websites when those systems are specifically listed in the agreement.

How your AMC begins.

A structured handover helps us support your business with context from the first request.

01 / Discover and document

Meet the business contact, understand critical activities and review the current IT environment. Create an inventory of equipment, applications, service providers and existing contracts. Identify systems with limited support, expired licences or missing documentation.

02 / Establish access and a baseline

Arrange authorised administrative access through a secure handover. Review accounts, device health, backup status and network configuration. Record existing issues and distinguish urgent remedial work from improvements that can be scheduled later.

03 / Agree priorities and activate support

Confirm escalation contacts, maintenance windows, request channels and the asset scope. Share the support process with your staff. An initial action plan records priorities, dependencies, approvals and the next review date.

What we need from you

Business context

Users, locations, operating hours and the systems you depend on most.

Authorised access

A designated approver and controlled access to relevant platforms.

Existing information

Asset lists, network diagrams, licence records and vendor contacts.

Onboarding output: an agreed environment record, known-issue list, support procedure and prioritised action plan.

From request to resolution.

A consistent support process makes progress, ownership and next steps easier to follow.

Log and assess the request

Report the affected system, what changed, the error message and how many people are affected. We assess business impact and urgency, identify a contact and establish whether the issue is local to one device or part of a wider service disruption.

Investigate and restore service

Begin with authorised remote checks where suitable. If physical inspection is necessary, arrange an on-site visit within the agreed coverage. Escalate to a specialist or vendor when required, and record any workaround that helps staff continue working.

Validate and close

Confirm the affected workflow is usable again with the relevant person. Record the action taken, note remaining work and flag repeated incidents for deeper review. Where a permanent fix needs additional parts or a change, provide the next step for approval.

The support journey

1 / Report & prioritise

Give the team enough detail to assess the issue correctly.

2 / Diagnose & coordinate

Investigate, communicate progress and involve the right people.

3 / Confirm & record

Validate the result and retain useful resolution information.

Example: for a shared printer failure, assess users affected, check connectivity and the print queue, restore access and verify a test print.

Maintain before problems multiply.

Planned checks help identify avoidable issues and keep supported systems in a manageable condition.

Workstations and user devices

Review storage capacity, device health, update status and endpoint protection. Investigate recurring application errors and unnecessary startup load. Schedule approved changes around business needs and check that essential applications still work afterwards.

Infrastructure and shared services

Review server alerts, storage utilisation, network health and backup job status. Check hardware warnings and supported firmware where applicable. Keep a record of configuration changes, equipment approaching end of support and capacity issues requiring investment.

Maintenance windows and reporting

Agree when changes can safely take place and how users will be informed. Document checks completed, exceptions and follow-up actions. Maintenance frequency is selected according to system importance, risk and the contracted scope.

A maintenance visit can cover

Health

Device condition, storage, service errors and recurring issues.

Protection

Update status, endpoint alerts and access concerns.

Follow-through

Completed actions, outstanding recommendations and approvals.

Preventive maintenance reduces avoidable risk; it does not make equipment failure or business interruption impossible.

Backups need a recovery plan.

The objective is to recover usable information and essential services when something goes wrong.

Decide what must be recoverable

Identify business files, databases, applications and configuration records. Agree how much recent data loss could be tolerated and how quickly critical services should return. These recovery objectives guide backup frequency, storage and the recovery approach.

Protect and check backup copies

Select suitable local, cloud or hybrid backup arrangements. Keep protected copies separated from production access where practical. Review failed jobs and retention settings, and test sample restores rather than assuming a successful backup notification proves recovery.

Prepare for disruption

Record who can authorise recovery, where credentials are securely held and which systems should be restored first. Recovery may depend on replacement hardware, usable backup copies, cloud access and specialist assistance, so these dependencies should be planned in advance.

Questions to answer

What data?

Which files, databases and systems are essential to operations?

How much loss?

What is the acceptable gap since the last recoverable copy?

How much downtime?

Which services come back first, and what resources are required?

Planning principle: separate backup copies and tested restoration are central to recovery readiness. Reference: CISA StopRansomware Guide.

Set realistic support expectations.

Service levels connect technical urgency with the business impact of a problem.

Agree priority definitions

A complete loss of a critical business service should be treated differently from a minor issue affecting one person. Priority categories can consider users affected, business interruption, security concerns and whether a workaround is available.

Separate response from resolution

Response means the request has been acknowledged and assessment has started. Resolution means service has been restored or an agreed outcome reached. Fixing an issue may depend on vendors, access, spare parts or an approved change, so the two measures should not be confused.

Define hours, escalation and updates

Set contracted support hours, emergency arrangements, on-site coverage and communication expectations. Identify the authorised customer contacts and how unresolved matters are escalated. Any after-hours support or special coverage must be part of the written agreement.

Illustrative priority model

Critical

A key business service is unavailable or a serious security issue is suspected.

High

Several users or an important process are affected.

Standard

An individual issue, routine request or planned change.

Response targets, resolution objectives and support availability are agreed per contract. This profile does not promise a universal response time.

Support that stays accountable.

Regular reviews keep the service aligned with your changing users, equipment and business needs.

Review useful information

A service review can cover request volumes, repeat incidents, maintenance completion, open actions and ageing equipment. Discuss the causes of repeated disruption and whether the issue needs training, configuration changes, replacement or a different business process.

Plan improvements and renewals

Maintain a list of upcoming licence renewals, capacity concerns and equipment nearing the end of useful life. Prioritise work according to business impact and budget. Update the coverage schedule when staff numbers, systems or locations change.

Share responsibilities clearly

Techvenation performs the agreed support work; your designated contact approves changes and helps coordinate access and staff availability. Business owners retain decisions about spending, data access and acceptable interruption. Third-party providers remain responsible for their contracted services.

Choosing the right arrangement

Remote support

Suitable where most covered issues can be resolved remotely.

Remote + scheduled visits

Adds planned on-site checks for equipment and local requirements.

Tailored coverage

Designed for multiple sites, critical workflows or additional systems.

These are engagement options, not fixed package promises. Final inclusions and pricing follow an assessment of your environment.

See the work behind the support.

Structured records connect daily technical work with the information management needs to review.

Timestamped activity records

A service register can record the date, request reference, affected user or location, system, reported issue, action taken, status and follow-up owner. Record work as it happens during the agreed service window, distinguishing technician effort from the total time a request remains open.

Daily tracking and weekly summaries

Track open, closed and pending requests, including items waiting for access, parts, approval or a vendor. Weekly summaries can highlight recurring problems, completed maintenance and decisions needed from the customer. Hourly reporting, where required, is agreed as part of the service scope.

An asset health view

Bring together the status of covered servers, endpoints, network equipment, printers, CCTV, attendance devices and websites. Identify the source and time of each check, the exceptions found and the next action. A green status should be supported by defined checks, not assumed from the absence of complaints.

Example record structure

Request

Time, reference, affected asset, issue and business impact.

Work performed

Diagnosis, authorised action, technician and supporting notes.

Follow-up

Status, unresolved dependency, owner and target date.

Agree the reporting frequency, asset coverage and required fields during onboarding so the records remain useful to your team.

Turn security alerts into reviewed actions.

A scoped Security Operations Centre (SOC) service connects monitoring, assessment and escalation.

Define monitoring coverage

Identify which endpoints, servers, accounts, firewalls and website events can supply useful security information. Available coverage depends on the installed tools, licences, log integrations and retention settings. Confirm monitoring hours and responsibility for responding to each type of alert.

Review and prioritise alerts

Assess suspicious authentication, malware detections, privilege changes and network anomalies in context. Establish which events are expected, which need investigation and which require escalation. An alert is a signal to assess; it is not automatically proof of a successful compromise.

Track response and closure

Create an incident record where further action is needed, document the investigation and coordinate approved response steps. Report alert categories, reviewed cases, unresolved risks and recommended improvements. Keep operational support tickets linked to security incidents when both relate to the same problem.

Tools and their roles

SIEM

Collects and correlates security logs from connected sources.

EDR

Provides endpoint detection and response capabilities.

XDR

Connects detections across supported security tools and data sources.

Managed SOC is a separately agreed service. Tool deployment alone does not establish continuous human monitoring or 24/7 response coverage.

A clear path from alert to closure.

Agree the people, authorisations and evidence needed before an urgent security event occurs.

Assess and escalate

Record the detection time, affected assets, source of the alert and initial business impact. Determine who needs to be contacted and whether the incident meets an urgent escalation threshold. Critical events are escalated through the agreed route rather than waiting for the next scheduled report.

Coordinate authorised containment

Select actions according to the incident and the business impact. These may include isolating an endpoint, suspending a compromised account or blocking an identified source. Preserve useful records, document decisions and coordinate with customer contacts and relevant providers before disruptive changes.

Validate recovery and learn

Check whether the cause has been addressed and whether the affected workflow can safely return to use. Record the recovery checks, remaining risks and closure decision. Follow-up recommendations can include access changes, improved detection, patching, training or changes to the incident procedure.

Incident register fields

Identity & impact

Reference, severity, detection time, affected assets and owner.

Response history

Evidence, investigation notes, approvals and containment actions.

Closure

Recovery validation, final status and follow-up work.

Support windows, on-call availability, escalation contacts and priority response targets are defined in the service agreement.

Find weaknesses. Track the fixes.

Vulnerability management connects assessment findings with accountable remediation and retesting.

Agree scope and authorisation

Identify the systems, applications and addresses to be assessed, the permitted methods and the testing window. Confirm ownership and written authorisation before testing. Vulnerability assessment identifies weaknesses; penetration testing examines exploitability within a specifically approved scope.

Document useful findings

A report should describe the affected asset, evidence, severity, likely business impact and recommended action. Use severity scoring where appropriate, while considering business context. Typical review areas include outdated software, excessive permissions, weak configurations and unnecessary external access.

Assign, remediate and retest

Give each finding an owner, target date and status. Schedule approved changes and check that business services still function afterwards. Retest to establish whether the issue is resolved. If action is deferred, record the reason and the authorised risk owner rather than silently closing the finding.

Assessment deliverables

Executive view

Scope, limitations, major risks and prioritised actions.

Technical register

Findings, evidence, affected assets and recommended remediation.

Follow-through

Owners, deadlines, retest results and accepted exceptions.

VAPT means vulnerability assessment and penetration testing. Testing scope, written authorisation, reporting and retesting are agreed before delivery.

Make performance and risks visible.

Bring support, security, website maintenance and improvement priorities into one management review.

Monthly service overview

Summarise covered assets, support activity, unresolved requests, maintenance and security events. Include a health view of key systems and website care: updates, backup checks, availability events and security review. Highlight decisions, dependencies and actions proposed for the next reporting period.

Explain metrics and exceptions

Show how acknowledgement and resolution measures are calculated, including support hours and valid exclusions. Define the source and measurement period for availability figures. If no priority incidents occurred, report that clearly rather than claiming a tested response performance for events that did not happen.

Maintain evidence for assurance

Activity logs, incident records, asset lists, access-change records, backup checks and remediation registers can support an organisation's information security management evidence. Agree the retention period and access permissions. The customer remains responsible for its management system, policies and certification process.

AMC and SOC records can support ISO/IEC 27001 evidence. They do not, by themselves, establish conformity or provide certification.

Management review agenda

Service performance

Work completed, unresolved requests and agreed service measures.

Risk & maintenance

Security findings, asset health, updates and recovery readiness.

Next actions

Named owners, approvals, priorities and target dates.

Set up the workplace properly.

Coordinate the technology required for a new office, expansion or move before staff arrive.

Survey and prepare

Review the layout, staff count, work areas, communications needs and available internet services. Identify data points, equipment locations, rack space and power requirements. Coordinate with the fit-out contractor and service providers so dependencies are visible early.

Install and configure

Install agreed network equipment, cabling, Wi-Fi, workstations and peripherals. Configure user access, shared resources and approved business applications. Where included, coordinate telephony, CCTV and access control as part of the wider site setup.

Test and hand over

Check connectivity, internet access, printing and key business workflows. Label network points, record the equipment and document essential settings. For relocations, plan the cutover, data protection and a fallback arrangement before disconnecting the existing environment.

Typical installation outputs

Site readiness

Confirmed layout, dependencies and installation schedule.

Working systems

Configured devices, connectivity and agreed business services.

Handover

Asset details, configuration records and user guidance.

Internet activation, civil works, electrical work and landlord approvals are coordinated dependencies and are included only where expressly scoped.

Connect people, devices and locations.

A network should reflect how your business actually uses applications, data and communication tools.

Structured cabling and switching

Plan labelled data outlets, patch panels and switching capacity around work areas and equipment. Keep installation records so faults and future changes are easier to trace. Test agreed connections and review the capacity needed for shared systems and connected devices.

Business Wi-Fi

Assess coverage areas, walls, user density and application needs. Position access points and configure staff and guest access appropriately. Review coverage and performance after installation; adding access points without planning can create interference rather than improve service.

Secure connectivity

Separate appropriate device groups, restrict administrative access and configure remote connectivity according to approved requirements. Document network settings and maintain supported equipment. Branch connections and remote access are designed around security and application needs.

Common use cases

Offices

Staff access, meeting rooms, printers and shared applications.

Retail & hospitality

POS connectivity, staff devices and separate guest access.

Warehouses

Coverage for scanners, workstations and operational devices.

Wireless performance depends on the site, interference, equipment and user load. A survey helps define an achievable design.

Organise your shared business systems.

Server and storage choices should balance application requirements, capacity, access and recoverability.

Assess the workload

Identify the applications, files, users and existing data that the environment must support. Review storage growth, vendor requirements and whether a local server, NAS or hosted solution is appropriate. Confirm licensing and equipment requirements before procurement.

Configure and migrate

Set up the agreed storage structure, accounts, permissions and network access. Plan data migration, test copies and arrange a cutover window. Check that users can access the right resources and that business applications function in the new environment.

Maintain and protect

Monitor agreed health indicators, capacity and service errors. Document configuration, manage approved updates and maintain a recovery approach. Storage redundancy can help with some hardware failures, but it does not replace a separate backup.

Delivery considerations

Capacity

Allow for current information and realistic growth.

Permissions

Give staff the access required for their responsibilities.

Continuity

Plan backup, restoration and support for the chosen setup.

Potential scope includes file services, NAS, directory services and virtual environments, subject to application compatibility and licensing.

Make everyday collaboration easier.

Business email and shared tools need careful setup, controlled access and a practical migration plan.

Plan the environment

Review your domain, current mailboxes, user count and collaboration requirements. Select appropriate subscriptions and confirm who owns billing and administration. Identify shared mailboxes, distribution groups, shared files and any integrations that need to remain operational.

Migrate with coordination

Prepare accounts, test the migration approach and schedule the transition. Coordinate DNS changes, mail flow, device configuration and staff communication. Validate messages, calendars and relevant data after migration, with a plan for addressing missing items or access problems.

Manage users and access

Support account creation, role changes and staff departures. Configure appropriate sign-in protection, permissions and collaboration settings. Review backup and retention needs separately from the productivity subscription so that recoverability matches business expectations.

Typical scope

Business email

Microsoft 365 setup, mailbox migration and device configuration.

Shared working

Team files, calendars, shared mailboxes and collaboration tools.

Administration

User changes, access review and subscription coordination.

Cloud subscriptions, migration volume, retention requirements and ongoing administration are confirmed in the proposal.

Cyber threats affect daily operations.

Recognising common attack patterns helps staff and management make better protection decisions.

Phishing and account compromise

Fraudulent messages may imitate a supplier, manager or familiar service to request credentials, payment or sensitive information. Stolen passwords can expose email and business applications. Staff awareness, independent verification and stronger sign-in protection help reduce this risk.

Ransomware and malicious software

Malicious software can disrupt systems, restrict access to files or expose business information. Recovery may require clean systems and usable backups. Keeping software maintained, limiting access and planning recovery helps reduce the impact of a successful attack.

Weak access and exposed systems

Old accounts, excessive permissions and neglected software create avoidable exposure. Accidental sharing and lost devices can also disclose information. Security therefore involves staff behaviour and routine administration as well as specialist tools.

Warning signs to report

Unexpected requests

Urgent payment changes, unusual attachments or sign-in prompts.

Account anomalies

Unfamiliar sign-ins or unexpected authentication requests.

System disruption

Unexplained file changes, security alerts or unusual device behaviour.

Awareness reference: CISA Secure Our World resources. If you suspect an incident, use a known support contact and follow your incident procedure.

Use several layers of protection.

Security controls should work together and fit the systems, information and people in your business.

Reduce opportunities for attack

Enable multifactor authentication (MFA), maintain supported software and restrict access to what each role needs. Review endpoint protection, firewall rules and remote access. Check that departed staff and unused accounts no longer retain unnecessary access.

Prepare staff and operations

Explain how to report suspicious activity and verify unusual requests through a trusted channel. Assign decision makers for an incident and keep important contacts available outside a potentially affected system. Define which events require specialist investigation.

Respond and recover carefully

When a suspected incident is reported, assess the impact, coordinate authorised containment and preserve relevant records. Recovery should address the cause before normal access is restored. Specialist forensics, legal advice or notification support may require a separately scoped provider.

A practical security review

Accounts

Who has access, and how is that access protected?

Systems

Are devices maintained and protection tools operating?

Readiness

Who takes action, and can important services be recovered?

Security work reduces risk but cannot guarantee prevention of every attack. Continuous monitoring or a staffed SOC is a separate service scope.

Control access. Improve visibility.

Site systems work best when coverage, user access and ongoing maintenance are planned together.

CCTV installation

Survey the areas to be monitored, lighting conditions, cable routes and recorder location. Select cameras and recording capacity around the agreed requirement. Configure viewing permissions, test playback and document the installed equipment and authorised access arrangements.

Access control and attendance

Review doors, staff groups, attendance workflows and the way the premises are used. Configure authorised users and access schedules, test operation and provide administrator guidance.

Integration with other systems is assessed before implementation.

PABX and business communication

Plan extensions, call routing, greetings and required business features. Configure the selected telephony solution and test internal and external call flows. Coordinate provider dependencies and document routine administration and support needs.

Installation sequence

Survey

Confirm coverage, equipment locations and site dependencies.

Install & configure

Complete the agreed physical and system setup.

Test & explain

Validate operation and train the nominated administrator.

Any authority approvals, project-specific standards or specialist certification requirements must be assessed for the site before commitment.

Start with the purpose of the website.

A website needs clear content and customer journeys before development begins.

Define the audience and action

Identify who the website is for and what a visitor should do: request a quotation, call, book, buy or learn about a service. Review the business offering and agree which information helps a potential customer make that decision.

Plan pages and content

Create a sitemap covering the main services, company information, contact routes and supporting content. For UAE location pages, explain genuine service coverage and local relevance. Gather approved text, logos, images and business details before final layout and build.

Design the experience

Develop a visual direction consistent with the brand, then design responsive layouts and navigation. Review the content hierarchy, calls to action and usability on smaller screens. Confirm the design and functional scope before development.

Discovery deliverables

Page plan

A sitemap and purpose for each key page.

Content requirements

Text, imagery, business details and customer questions.

Functional scope

Forms, languages, integrations and editing requirements.

Typical workflow: discovery and content planning -> design -> development -> testing -> launch -> ongoing care.

Install, configure and build.

WordPress delivery includes the environment, website functionality and a manageable editing experience.

Prepare hosting and the domain

Confirm domain ownership, DNS access, hosting suitability and the people responsible for renewals. Set up the development environment and encrypted HTTPS access. Plan backups and separate staging from the public website while the build is in progress.

Build the WordPress website

Install and configure WordPress, the agreed theme and necessary plugins. Create page templates, navigation, forms and content structures. Use appropriate access roles and avoid unnecessary plugins. Connect approved services such as analytics and business enquiry delivery.

Configure search and handover

Set up the agreed SEO plugin, page metadata, sitemap settings and indexing controls. Explain how to edit content and manage common tasks. Provide a clear record of installed components, subscriptions and ongoing maintenance responsibilities.

Setup checklist

Environment

Domain, hosting, HTTPS, staging and backups.

Website

Theme, pages, plugins, forms and user roles.

Operations

Updates, licence ownership and administrator guidance.

A theme or SEO plugin is one component of the website. Hosting, content, delivery testing and ongoing maintenance also need to be planned.

Connect the online customer journey.

An online store or integrated website must work beyond the page the customer sees.

Products and checkout

Plan categories, product details, variations and the checkout flow. Configure suitable delivery, tax and payment settings using your approved business rules. Payment providers and merchant approval are external dependencies that must be confirmed early.

Business integrations

Connect appropriate forms, booking tools, CRM records, inventory or other applications through supported interfaces. Define which system owns each field, how updates flow and what happens when an integration fails or receives incomplete information.

Test real operating scenarios

Check successful and failed payments, order notifications, product availability and relevant administrative workflows. Confirm how staff handle cancellations, refunds and enquiries. Test integrations with sample data before allowing them to affect live records.

Questions before development

Commercial rules

Products, pricing, delivery areas and approved policies.

System ownership

Where are customers, stock and orders maintained?

Daily operations

Who manages orders, exceptions and customer communication?

Gateway fees, paid extensions, shipping providers and third-party API access are confirmed separately in the agreed scope.

Launch with checks. Maintain with care.

The website should be tested as a working business tool before it becomes your public presence.

Validate the website

Review key pages on mobile and desktop, navigation, links, content and basic accessibility. Submit forms and confirm they reach the right recipient. Test agreed integrations and review image size, caching and third-party scripts that affect performance.

Plan the production switch

Back up the relevant environment, confirm the domain changes and agree the launch window. For a replacement website, map old URLs to suitable new pages and implement redirects. Recheck HTTPS, indexing settings, analytics and enquiry delivery after release.

Maintain after launch

Keep the platform and supported extensions updated through an agreed process. Review backup health, security alerts and important user journeys. Content updates and feature development can be scheduled separately from technical maintenance.

Handover essentials

Access

Document administrative roles and account ownership.

Knowledge

Explain editing, forms, backups and support contacts.

Continuity

Confirm renewals, maintenance and recovery responsibilities.

Website maintenance can be included in a separate care agreement or listed explicitly within a wider AMC.

Build around your business needs.

Techvenation develops websites and web applications around your customers, staff and daily workflows.

Business websites and service platforms

Present your company, services and enquiry routes through responsive pages that work across desktop and mobile. Scope can include multilingual content, quotation forms, booking requests, searchable information and a content management system your team can maintain.

Portals and custom web applications

Create authenticated experiences for customers, staff, suppliers or members. Depending on the requirement, a portal can provide document access, request tracking, approvals, dashboards or self-service functions. Define user roles and the information each person is permitted to view or change.

Connect the website to operations

Integrate suitable CRM, ERP, booking, payment or inventory systems through supported interfaces. Agree the source of truth for each record, error handling and administrator controls. We plan, design, develop and test the agreed solution, then provide handover and a maintenance arrangement.

Examples of business needs

Generate enquiries

Service pages, quotation forms and lead capture.

Serve customers

Bookings, order visibility and account-based information.

Support your team

Internal forms, approval flows and operational dashboards.

Choose the build around the workflow: a WordPress website, ecommerce platform or custom web application, according to the agreed requirements.

Your business, in your customer's hand.

Android and iOS app development for customer services, staff workflows and connected business operations.

Customer-facing mobile applications

Scope an app around a useful repeat activity: bookings, ordering, service requests, account access or customer communication. Potential features include sign-in, profiles, notifications, payment integration and order or request status. Each feature is selected for the business need and intended audience.

Staff and field-service applications

Support employees working beyond the office with assigned jobs, visit records, stock lookups, checklists or proof of service. Camera capture, location access and offline workflows can be considered where relevant. Permissions and data collection should be limited to the agreed operational purpose.

Android, iOS and shared development

Choose native or cross-platform development according to device features, performance needs, budget and maintenance requirements. Connect the app to suitable backend services and business systems. Provide an administration interface where your team needs to manage users, content or transactions.

App features, device support, backend hosting, third-party services and ongoing maintenance are defined in the development proposal.

App opportunities

Service businesses

Booking, requests, job updates and customer communication.

Retail & hospitality

Ordering, loyalty and relevant customer account features.

Internal operations

Field tasks, approvals and mobile access to business data.

From app idea to a working release.

A staged delivery process makes the application easier to review, test and maintain.

Discover, prototype and define

Identify the users, priority workflows and success criteria. Map screens and navigation, then review a prototype before full development. Agree the first-release feature set, supported devices, backend requirements and account ownership so the team has a clear delivery baseline.

Develop, integrate and test

Build the interface, application logic and agreed integrations. Test critical journeys on representative Android and iOS devices, including weak connectivity, expired sessions and failed requests. Review permissions, accessibility and notification behaviour alongside functional testing.

Prepare release and ongoing care

Assist with agreed store assets, build submission and release preparation using the business's developer accounts. Platform review remains external to the project. After launch, plan defect handling, crash review, operating-system compatibility and future improvements under the maintenance scope.

What delivery can include

Design & build

Screen designs, app development and agreed backend functions.

Testing & release

Test records, release preparation and submission support.

Handover

Administration guidance, ownership records and support arrangements.

Developer accounts, source-code handover, intellectual-property terms, store fees and post-launch support are agreed in the contract.

Build visibility around real services.

Help potential customers find useful information and understand why your business fits their needs.

Research and prioritise

Identify the services, locations and customer questions that matter commercially. Group related searches by intent and map them to suitable pages. Prioritise topics using available demand data, competition, business value and the content already on the website.

Improve the website and content

Review technical issues affecting discovery and usability. Develop clear service pages, useful supporting articles and accurate business information. Explain actual UAE coverage with original location content rather than repeating identical pages with different city names.

Measure and refine

Review search visibility, relevant landing pages and qualified enquiries. Use performance evidence to improve page content and internal navigation. Search work develops over time and depends on the website, competition and the usefulness of the information provided.

Potential SEO scope

Technical review

Crawlability, indexing, links and page structure.

Content work

Service pages, local information and customer questions.

Performance review

Relevant searches, landing pages and enquiry outcomes.

SEO aims to improve relevant visibility and business enquiries. Specific positions, traffic volumes or revenue cannot be guaranteed.

Connect campaigns to business outcomes.

Advertising and content should support a clear offer, audience and next step.

Plan the campaign

Agree the customer segment, geographic coverage, offer and desired action. Select appropriate channels and landing pages, then define a working budget and approval process. Separate media spending from management, creative production and website development.

Create and deliver

Prepare campaign messaging, graphics and approved content. Configure advertising or publishing schedules and connect enquiries to the right team. Social media planning can cover recurring themes, promotions and useful business information appropriate to each channel.

Review meaningful results

Assess enquiries, conversion paths and lead quality alongside reach and engagement. Test creative messages and landing pages, then refine the campaign using available evidence. A call or WhatsApp click is a signal of interest, not automatically a confirmed sale.

Campaign building blocks

Offer & audience

A specific reason to respond and a relevant customer group.

Creative & destination

Consistent messaging from advert to landing page.

Follow-up

A clear owner for enquiries and a way to review lead quality.

Scope can include Google Ads, social advertising, content planning and branded creative. Ad spend and platform charges are agreed separately.

Help customers reach the right answer.

AI assistants can support common enquiries while keeping staff available for judgement and exceptions.

Choose a useful starting point

Begin with repetitive questions or a clearly defined enquiry journey. A website or WhatsApp assistant can explain approved services, collect initial information and route a request. Identify what the assistant is allowed to answer and what should always move to a person.

Connect approved information

Prepare a reliable source of service details, FAQs and operating information. Define required enquiry fields and connect appropriate CRM or notification workflows. Access to customer information should follow the minimum permissions needed for the task.

Test and supervise

Test typical questions, ambiguous requests and incorrect inputs before release. Review the assistant's answers and handover behaviour. Keep an owner responsible for updating information and examining failed conversations as services and customer needs change.

Practical use cases

Enquiry capture

Collect service needs, contact details and location.

FAQ assistance

Answer approved questions from maintained business content.

Staff handover

Pass complex or sensitive requests to an authorised person.

AI can produce incorrect responses. Define review and escalation rules; platform fees and channel access depend on the selected solution.

Automate the repeated steps.

Map the process first, then connect the systems that can reliably carry it out.

Find the workflow and its owner

Document the trigger, required information, decisions and expected result. Suitable starting points include form-to-CRM entry, lead assignment, approval requests and recurring notifications. Remove unnecessary process steps before automating them.

Build with controls

Use supported integrations and appropriate credentials. Define checks for missing data, duplicate records and failed actions. Require human approval for important commitments, external messages or business changes where that approval is part of the process.

Pilot and improve

Run sample cases, including errors and exceptions, before broader use. Review completion, failures and whether staff still need to repeat the work manually. Maintain the integration as connected applications, permissions and business rules change.

Example enquiry workflow

Trigger

A customer submits a website enquiry.

Process

Check required fields, create a CRM entry and assign an owner.

Action

Notify the assigned team and create an agreed follow-up task.

Deliverables can include a workflow map, configured integrations, test results and administrator guidance. Final scope depends on platform access.

Give every enquiry a clear next step.

A customer relationship management system organises the work between first contact and ongoing service.

Design the sales process

Map the lead sources, qualification steps, deal stages and people responsible for follow-up. Agree which information is required and how duplicate contacts should be handled. The system should reflect the actual sales process rather than add unnecessary administration.

Configure and connect

Set up fields, pipelines, permissions, reminders and useful reports. Connect suitable website forms or other enquiry channels. Where information is migrated, review its quality, map the fields and validate sample records before the full transfer.

Train and adopt

Guide staff through creating records, updating stages and recording relevant activity. Give managers a usable view of open work and ownership. Review adoption after rollout and refine fields or reporting when they create friction without adding value.

Common CRM functions

Lead management

Capture, qualify, assign and follow up.

Customer history

Keep relevant contacts, notes and interactions together.

Pipeline visibility

Review active opportunities and next actions.

CRM implementation may use an existing platform or a custom approach. Licensing, integrations and development are confirmed after assessment.

Manage relationships beyond the first lead.

Configure a CRM that helps sales and service teams share useful information and follow through.

Lead capture and sales management

Bring approved enquiry channels into a central pipeline. Configure assignment rules, qualification fields, tasks, reminders and stage changes. Track quotations and next actions where supported, with dashboards showing who owns an opportunity and what needs attention.

Customer service and retention

Organise relevant contact history, service requests, account notes and renewal reminders. Use roles to control access to sensitive records. A shared customer view helps staff respond with context while keeping personal information limited to the people who need it.

Integrations and automation

Connect suitable website forms, approved messaging channels, email or business applications. Define when records should be created or updated and how duplicate information is handled. Begin with a small number of useful automations, then refine them using staff feedback and data quality checks.

A typical enquiry journey

Capture & assign

Create a record, check required information and assign an owner.

Follow up & quote

Record contact, schedule tasks and track the proposed work.

Win & hand over

Pass approved details to delivery, accounts or service teams.

Features are configured or developed for the chosen platform. Channel permissions, integration access and paid modules are assessed during discovery.

Connect the processes behind the business.

ERP planning starts with how information moves between departments and where controls are needed.

Map operations and requirements

Review purchasing, inventory, sales, finance and other relevant workflows. Identify approval rules, reporting needs and manual handovers. Confirm which modules are essential for the first release and which can follow after the team is comfortable with the system.

Configure, migrate and test

Set up agreed roles, master data and business rules. Prepare and validate data from existing systems before migration. Test complete scenarios, such as purchase-to-stock and sale-to-reporting, so that dependencies between departments are visible.

Roll out with ownership

Train process owners and end users, coordinate the transition and provide an agreed support period. Review reports and data quality after go-live. Changes to accounting or regulatory configurations require validation by the business's qualified advisers.

Implementation priorities

Process fit

Make sure the system supports real operational needs.

Reliable data

Clean and validate products, suppliers and opening records.

Team adoption

Define ownership, training and practical support.

ERP scope, modules, integrations, migration effort and commercial terms are established through requirements assessment.

Connect purchasing, stock and delivery.

Select the modules that address your operational needs and introduce them in manageable stages.

Purchasing and inventory

Organise suppliers, purchase requests, approvals and receiving workflows. Maintain product records and relevant stock movements across agreed locations. Reorder information, transfers and stock counts can help teams understand availability and investigate differences between records and physical stock.

Sales, finance and operational workflows

Connect quotations, orders, fulfilment and invoicing where supported. Define handovers between sales, warehouse and finance teams. Additional scope may include service jobs, project costing or selected employee administration, depending on the platform and the processes your business needs.

Reporting and management controls

Provide role-based dashboards and reports built around meaningful business questions. Track approvals and important changes, with clear responsibility for master data. Validate accounting settings and opening balances with your finance team before production use and reconcile key reports after migration.

Example purchase-to-stock flow

Request & approve

Raise a requirement and route it to the authorised approver.

Order & receive

Issue the purchase order and record goods received.

Update & review

Update stock and pass the relevant records to finance.

A phased ERP rollout can start with core modules, then add integrations and further processes once the initial workflows are stable.

Support the point of service.

A POS solution should fit the way staff sell, take payment and manage everyday transactions.

Match the business model

Review the needs of a restaurant, retail shop or laundry operation. Define products or services, price options, user roles and required reports. Restaurant workflows may include tables, kitchen routing or QR menus; retail may focus on variants, stock and barcode scanning.

Install and configure

Set up the chosen POS software and compatible terminals, printers or scanners. Configure approved business rules and assess payment or inventory integration. Check network dependencies and document what functions remain available if connectivity is interrupted.

Test and train the team

Test sample transactions, cancellations, permitted refunds and end-of-day routines. Confirm receipt printing and relevant reporting. Train managers and staff, then agree how device faults, software issues and changes to the catalogue will be supported.

Potential configurations

Restaurants

Menus, tables, order routing and digital menu options.

Retail

Products, barcodes, stock and sales reporting.

Laundry

Service items, order tracking and collection workflows.

Features depend on the selected platform and equipment. Payment integration, offline operation and multi-branch functions must be verified before commitment.

Fit the POS to the way you serve.

Different businesses need different sales screens, equipment and fulfilment workflows.

Restaurant and cafe POS

Configure menus, modifiers, tables and takeaway workflows as required. Kitchen printing or display integration can route orders to preparation teams. QR menus, delivery connections and loyalty features are assessed against the selected platform and the way staff handle orders and payments.

Retail and multi-location operations

Manage products, variants, barcode scanning, price rules and authorised returns. Connect stock and sales reporting where supported. Branch access, transfers and consolidated reporting can support a wider operation, provided the platform and connectivity model meet the requirement.

Laundry and service-counter workflows

Record service items, order references, collection dates and status changes. Where supported, add garment tags, receipts and customer notifications. Define how staff record handover, corrections and collection so that the system follows the actual customer-service process.

Equipment and readiness

Counter devices

Suitable terminals or tablets, scanners and receipt printers.

Operational devices

Kitchen printers, displays or label printers where required.

Connectivity

Network readiness, payment interfaces and backup arrangements.

Offline behaviour, payment reconciliation, branch synchronisation and specialist peripherals must be tested with the selected solution.

A complete path from setup to adoption.

CRM, ERP and POS projects need coordinated data, users and workflows as well as software installation.

Requirements, selection and configuration

Map the current process and agree what needs to improve. Assess suitable existing products or a custom development approach. Define the included modules, user permissions, reports and integration boundaries, then review a configured demonstration against the agreed workflows.

Migration, integration and acceptance

Clean source data and map the fields before transfer. Test sample records, balances or stock information as relevant. Validate end-to-end scenarios between systems and obtain user acceptance for the agreed functions. Plan the cutover, backup and rollback arrangements before live use.

Training, rollout and ongoing support

Train administrators and end users using realistic tasks. Provide operating guidance and identify who maintains products, users and process settings. Support the agreed rollout period, then review adoption, unresolved issues and further improvements through a defined care arrangement.

Connected business example

Website or app

Captures the enquiry, booking or customer order.

CRM and ERP

Coordinate customer ownership, approvals and fulfilment.

POS and reporting

Record counter transactions and feed agreed operational reports.

Licensing, hosting, hardware, data migration, integrations, training and support should be itemised so the complete implementation cost is clear.



LET'S PLAN YOUR NEXT STEP

Tell us what your business needs.

For an AMC proposal, share your locations, user count, main systems, operating hours and current challenges.

For an installation, website or business system, tell us your required outcome, scope and preferred timeline.

+971 55 285 5413

info@techvention.ae

techvention.ae

TECHVENATION FZC LLC | UNITED ARAB EMIRATES