نطاق العمل التفصيلي

اسم المشروع	تطوير المنصة والتطبيق الذكي لزوار اجتماع المنظمة العالمية للسياحة
اسم المبادرة	
التاريخ	**8/11/2025**

جدول المحتويات

المقدمة 2

التعريف بالمشروع 3

الشروط الخاصة ومتطلبات العمل 4

معايير تقييم العروض 12

التقديمات المطلوب ارفاقها من قبل مقدم العرض 17

الملحقات 18

المقدمة

وزارة السياحة، هي الجهة الرسمية الأولى المعنية بإدارة القطاع السياحي في المملكة العربية السعودية ودورها الرئيسي هو الاهتمام بقطاع السياحة وتنميته وتطويره، وتذليل معوقات نموه باعتباره رافداً مهماً من روافد الاقتصاد الوطني. ويضطلع القطاع الخاص بالدور الرئيس في إنشاء المنشآت السياحية الاستثمارية، بما يحقق رؤية الدولة وطموحات المواطنين في هذا القطاع الاقتصادي الهام. هذا وتطبق الوزارة نظام المنافسات والمشتريات الحكومية ولائحته التنفيذية، ولائحة تفضيل المحتوى المحلي والمنشآت الصغيرة والمتوسطة والشركات المدرجة بالسوق المالية، ولائحة تنظيم تعارض المصالح ولائحة سلوكيات وأخلاقيات القائمين على تطبيق النظام في تنفيذ أعمالها ومشاريعها.

دعوة

يسر وزارة السياحة أن ترحب بجميع المؤسسات والشركات والأفراد الذين يرغبون في تقديم عروضهم لتنفيذ أعمالها أو تأمين مشترياتها.

يجب على المتنافسين قراءة هذه الشروط وفهمها جيداً، فهي تُعد جزءاً لا يتجزأ من العقد الذي سيتم إبرامه بعد إتمام اجراءات الترسية. وعلى جميع الراغبين في تقديم عروضهم لتنفيذ أعمال الوزارة أو تأمين مشترياتها التقيد بما يلي:

مراعاة تطبيق الشروط بدقة عند إعداد العرض، والتأكيد على ذلك بالتوقيع على جميع صفحات هذه الشروط من قبل صاحب المؤسسة أو من يفوضه، مع ضرورة ختم كل صفحة منها بالختم المعتمد الخاص بالمؤسسة أو الشركة.

(تعتبر هذه الوثيقة جزء لا يتجزأ من كراسة الشروط والمواصفات المرجعية المعتمدة والمرفقة في منصة اعتماد)

التعريف بالمشروع

1. نبذة عن المشروع

ترغب وزارة السياحة في المملكة العربية السعودية من خلال هذه الوثيقة دعوة الشركات والمؤسسات المتخصصة في مجال تقنية المعلومات لتقديم عروضها في مجال الأعمال التطويرية لتطبيقات الويب والأجهزة الذكية والخدمات الالكترونية المصاحبة لها وتقديم خدمات الدعم الفني وذلك لتقديم أفضل تجربة رقمية للمدعوين لاجتماع منظمة السياحة العالمية بما يتناسب مع متطلبات الوزارة.

2. الهدف العام للمشروع

- توفير قناة موحدة تمكن المدعوين من التفاعل مع كافة الخدمات الالكترونية الموجهة لهم عبر الويب وتطبيق للأجهزة الذكية
- تطوير العديد من الخدمات التي تساعد المدعوين في انجاز المهام والوصول للمعلومات المتعلقة بالاجتماع.
- تطوير العديد من الخدمات التي تساعد المدعوين للوصول الى خدمات لتقديم أفضل تجربة سياحية في المملكة.
- تطوير تطبيق لأجهزة الجوال الذكية والويب لتسهيل اعمال فرق العمليات.
- تطوير واجهة ويب لمدير النظام.
- تطوير واجهة لفريق إدارة الضيوف

3. موقع المشروع

وزارة السياحة – الرياض – المقر الرئيسي

الشروط الخاصة ومتطلبات العمل

1. نطاق عمل المشروع:

مرحلة التصميم:

- تصميم كافة واجهات التطبيق.
- تصميم كافة الخصائص المتضمنة في التطبيق.
- تصميم رحلة المستخدمين للتطبيق.

مرحلة التحليل:

أعمال التحليل والتوثيق لكافة الخدمات الالكترونية والتطبيقات التي يتم القيام بها خلال العقد.

مرحلة التطوير:

- التهيئة باستخدام الذكاء الاصطناعي (AI Onboarding): تطوير ما يمكن المدعوين من جمع تفضيلاتهم عبر أسئلة سريعة، أو إتاحة مزامنة تفضيلات البريد بموافقتهم.
- وحدة اتفاقية الموافقة (Consent Agreement Module): تطوير ما يمكن المدعوين من الموافقة على استخدام البيانات (ميزات الذكاء الاصطناعي، التوصيات، إدارة خط سير الرحلة).
- حقيبة الترحيب الرقمية (قبل الوصول) ((Digital Welcome Kit (Pre-Arrival): تطوير ما يمكن المدعوين من الحصول على معلومات تشمل قواعد اللباس، والبروتوكولات، و "ما يجب معرفته عن السعودية"، وتصاريح الدخول.
- تفاصيل الاتصال بالمساعد الشخصي (Personal Assistant Contact Details): تطوير ما يمكن المدعوين من تعيين نقطة اتصال بشرية حقيقية مع خيارات الدردشة/البريد الإلكتروني/الهاتف.
- ملف تعريف المفوض (Delegate Profile): تطوير ما يمكن المدعوين من تضمين معلومات مثل الدور، والجنسية، والاهتمامات، ومعلومات الحمية الغذائية، واحتياجات الوصول.
- حجز الفعاليات (Event Booking): تطوير ما يمكن المدعوين من تصفح الفعاليات الرسمية والثقافية وتلك المخصصة بالدعوات، والرد على الدعوات بناءً على دور المستخدم ومستوى الوصول.
- حجز الرحلات الجوية (Flight Booking): تطوير ما يمكن المدعوين من حجز رحلات الطيران عن طريق التكامل المباشر أو الربط مع شركات الطيران.
- حجز الفنادق (Hotel Booking): تطوير ما يمكن المدعوين من تصفية الفنادق المنسقة القريبة بناءً على موقع الفعالية ونوع الغرفة.
- تأجير سيارة مع سائق (Car Rental With Driver): تطوير ما يمكن المدعوين من حجز سيارة فاخرة مع سائق ثنائي اللغة.
- خدمة السائق الخاص: تطوير ما يمكن المدعوين من التكامل مع واجهات برمجة تطبيقات خدمات النقل الفاخرة.
- خدمة التنقل داخل المدن: تطوير الربط مع مزود خدمات مما يمكن المدعوين من استخدام خيار احتياطي بسيط للنقل العام.
- حجز غرف الاجتماعات (Meeting Room Reservation): تطوير ما يمكن المدعوين من حجز غرف الاجتماعات داخل أماكن الفعاليات أو الفنادق الشريكة.

- الباقات المقترحة (Suggested Bundles): تطوير ما يمكن المدعوين من الحصول على باقات منسقة بالذكاء الاصطناعي تشمل: رحلة طيران + فندق + فعاليات + نقل.
- حجز المطاعم / التجارب + السيارة (Restaurant / Experience Booking + Car): تطوير ما يمكن المدعوين من حجز المطاعم الفاخرة أو التجارب بالإضافة إلى خدمة السائق الفاخرة بنقرة واحدة.
- أولوية الوصول للحجز (Priority Booking Access): تطوير ما يمكن المدعوين من الحصول على فترات زمنية محجوزة أو حجوزات حصرية لكبار الشخصيات.
- مركز المساعدة الشخصية (Personal Concierge Hub): تطوير ما يمكن المدعوين من التفاعل واجهة دردشة أو اتصال للكونسيرج المخصص (مرتبط بلوحة تحكم لفريق العمل).
- الذكاء الاصطناعي السياحي (Norah AI): تطوير الربط مع الذكاء الاصطناعي للسياحة (نورة) مما يمكن المدعوين من استخدام مساعد افتراضي مدرب للإجابة على أسئلة البروتوكول، وجداول الفعاليات، والمساعدة في الحجوزات.
- شخصية الذكاء الاصطناعي التفاعلية (Interactive AI Character): تطوير ما يمكن المدعوين من استخدام مساعد يعتمد على الصور الرمزية (مثل نورة أو "مضيفك في السعودية").
- جدول الأعمال الموصى به (Recommended Agenda): تطوير ما يمكن المدعوين من بناء جدول زمني بواسطة الذكاء الاصطناعي بناءً على التفضيلات وتاريخ الردود على الدعوات.
- الترجمة الصوتية الفورية (Instant Voice Translation): تطوير ما يمكن المدعوين من التحدث والترجمة في الدردشات أثناء الاجتماعات أو في المطاعم أو الجولات.
- تلخيص الذكاء الاصطناعي (AI Summarization): تطوير ما يمكن المدعوين من الحصول على ملخص يومي للفعاليات والاجتماعات والمهام بلغة واضحة.
- ملخص أخبار الذكاء الاصطناعي اليومي (AI Daily Digest News): تطوير ما يمكن المدعوين من الحصول على موجزات منسقة (أخبار سعودية، دولية، خاصة بالبروتوكول).
- طلب مرشد سياحي (Tour Guide Request): تطوير ما يمكن المدعوين من طلب مرشدين محليين معتمدين حسب اللغة أو الموضوع أو الموقع السياحي.
- تحديد المسار (Wayfinding Beacons): تطوير ما يمكن المدعوين من استخدام نظام الملاحة الداخلي/الخارجي باستخدام اجهزة البلوتوث لتحديد الموقع الحالي والاستدلال الى الوجهة.
- إشعارات بالقرب من المعالم (Push Notifications Near Landmarks): تطوير ما يمكن المدعوين من تلقي إشعارات عندما يكونون بالقرب من معلم مدينة أو مواقع ثقافية أو تاريخية.
- تحميل خط سير الرحلة من الواجهة الخلفية (Load Itinerary from Backend): تطوير ما يمكن للمدعوين من تلقي خط سير الرحلة الذي يتم تعيينه من قبل فريق العمل من لوحة تحكم الإدارة بواسطة فريق البروتوكول لكل مستخدم.
- تكامل البث المباشر (Live Stream Integration): تطوير ما يمكن للمدعوين من الوصول إلى الفعاليات القابلة للبث.
- الإشعارات المخصصة (Personalized Notifications): تطوير ما يمكن المدعوين من تلقي تذكيرات تعتمد على الموقع والاهتمامات والوقت.
- الدردشة الآمنة بين المدعوين (Delegate-to-Delegate Secure Chat): تطوير ما يمكن المدعوين المعتمدين من مراسلة بعضهم البعض بشكل آمن.
- الرد على دعوات الفعاليات والحجز (Event RSVP & Booking): تطوير ما يمكن المدعوين من الوصول إلى الفعاليات بناءً على نوعها.
- الاستبيانات والملاحظات الفورية (Push-Based Surveying & Feedback): تطوير ما يمكن المدعوين من تقديم تقييمات في الوقت الفعلي للفنادق، والنقل، والفعاليات.
- البطاقة الرقمية (Digital Card): تطوير ما يمكن للمدعوين من استخدام رمز QR للمسح الضوئي في الفعالية، وتسجيل الدخول.
- مدير خط سير الضيوف في الواجهة الخلفية (Backend Guest Itinerary Manager): تطوير ما يمكن لفريق الإدارة من تعيين، أو تعديل، أو مزامنة، أو تحميل خطط وجداول الضيوف.

- التحليلات والرؤى (Analytics & Insights): تطوير ما يمكن لفريق الإدارة من الحصول على بيانات حول الفعالية، وتقييمات الخدمات، واستخدام الذكاء الاصطناعي، ومقاييس الرضا.
- مدير مهام الكونسيرج (Concierge Task Manager): تطوير ما يمكن لفريق الكونسيرج من تعيين، ومتابعة، وتصعيد طلبات الكونسيرج.
- أدوات تجاوز الطوارئ (Emergency Override Tools): تطوير ما يمكن لفريق البروتوكول من إرسال تنبيهات لتنبيه أو إعادة توجيه الضيوف في الوقت الفعلي.
- خط سير الرحلة الموحد (Unified itinerary): تطوير ما يمكن المدعوين من عرض جميع الفعاليات المحجوزة، والخدمات اللوجستية، وبرنامج الفعالية في تقويم واحد مع المعلومات التفصيلية لكل منها.
- تفاصيل المرافقين (Companion details): تطوير ما يمكن المدعوين من عرض تفاصيل المرافقين لكل دولة.
- تطبيق فريق العمليات (Operation team app): تطوير ما يمكن فريق الخدمات اللوجستية والبروتوكول والعمليات من عرض وتحديث المهام المعينة في الموقع عن طريق تطبيق لأجهزة الجوال الذكية.
- التنبيهات والإشعارات الاستباقية (Proactive Alerts & Notifications): تطوير ما يمكن للمدعوين من تلقي تذكيرات وتغييرات وإرشادات استباقية وذكية تعتمد على السياق.
- برنامج الفعاليات (Event Program): تطوير ما يمكن المدعوين من عرض تفاصيل برنامج الفعالية.
- الذكاء الاصطناعي للمطابقة (Ai Networking & Matchmaking): تطوير ما يمكن المدعوين من عرض قائمة الحضور، والمطابقة مع الأقران، والدردشة معهم، وجدولة الاجتماعات، والاقتراحات الذكية.
- إدارة المقاعد (Seating mgmt.): تطوير ما يمكن المدعوين من عرض خطة المقاعد أثناء الفعالية لكل مدعو.
- الوثائق (documentation): تطوير ما يمكن المدعوين من الوصول إلى جميع المستندات المشتركة.
- نظام حجز (Delegate Booking System): تطوير ما يمكن المدعوين من السماح بالحجوزات الفردية والجماعية للعشاء وما يصل إلى أربع تجارب مع مراقبة السعة في الوقت الفعلي، والتأكيدات الآلية، وإدارة قوائم الانتظار، وجمع تفضيلات الحمية الغذائية، وخطط طوارئ للحجوزات المتأخرة.
- تطوير واجهة مستخدم ويب وتطبيق ذكي بما يسمح لفرق العمل داخل الوزارة من التعامل مع طلبات المدعوين من خلالها.
- تطوير لوحة تحكم بما يسمح لمدير النظام بالتحكم بكافة الخدمات التي تم تطويرها لتطبيق الأجهزة الذكية بحيث تمكنه منه:
  - تفعيل وإلغاء تفعيل الخدمات.
  - تفعيل المستخدمين للتعامل مع واجهات إدارة الضيوف.
  - الوصول الى التقارير ولوحة المؤشرات عن الحدث وتصديرها في ملفات Excel و PDF.
  - إدارة إمكانية الدخول للتطبيق او الخدمات في حال وجود صيانة في التطبيق او في احدى الخدمات
  - إدارة ترتيب ايقونات الخدمات في تطبيق الضيوف للهواتف الذكية.
  - الوصول الى سجل المستخدمين لتطبيق الضيوف وواجهة إدارة الضيوف.
  - الوصول الى سجل استخدام الخدمات لتطبيق الضيوف وواجهة إدارة الضيوف.
  - إدارة الصلاحيات لكافة المستخدمين لكل الواجهات والتطبيقات.
- تطوير واجهة للمستخدمين من فريق إدارة الضيوف لتمكينهم من كل من :
  - الإدارة الكاملة لكافة المحتويات والخدمات التي تقدم للضيوف من خلال تطبيق الهواتف الذكية.
  - إدارة الاشعارات للتطبيق من حيث (اشعارات الخدمات ، الاشعارات الأخرى)
  - إدارة صورة بدء التطبيق ، وصور الخلفيات داخل التطبيق
  - إدارة الاستبيانات والتصويتات.
  - إمكانية تصدير التقارير والاطلاع على لوح المؤشرات ذات العلاقة بالضيوف وتفاعلهم.
- الربط والتكامل مع كافة الأنظمة والتطبيقات الداخلية والخارجية ذات العلاقة وفقًا لآليات الربط التي يحددها فريق الربط في الوزارة.

مرحلة الدعم:

الدعم الفني لجميع المنصات المطلوبة (تطبيق الويب ، الأجهزة الذكية للمدعوين) بالإضافة الى (تطبيق فريق العمليات وموقع الويب الخاص بهم) بالإضافة الى (لوحة التحكم لمدير النظام).

- يجب ألا تقل جودة الخدمة القدمة في سرعة الرد على المشاكل وحلها عن القيم التالية:

خطورة/أهمية الشكلة	التعريف	تأثير الخطر
حرج	خسارة كاملة للنظام وحيث يتعطل النظام ويكون المستخدم غير قادر على العمل والقيام بأجزاء هامه جدا من الهام النوط بها	هذا التعطل في النظام يؤثر على جميع المستخدمين
عالي	توقف لإجراء أو عملية أو وظيفة رئيسية حيث يتعطل النظام ويكون المستخدم غير قادر على العمل والقيام ببعض الجزاء الهامة من الهام النوط بها. وينحسب هذا أيضا على ضياع جزء من البيانات.	تعطل النظام يؤثر على عدد كبير من المستخدمين
متوسط	توقف كامل بإجراء او عملية أو وظيفة غير رئيسية لينطوي عليها توقف كامل بالنظام، حيث يتعطل النظام ويكون المستخدم غير قادر على العمل والقيام ببعض الجزاء الصغير من الهام النوط بها , ولكنه ل يزال قادر على أداء بعض الهام الخرى النوط بها. وقد يتضمن ذلك الأسئلة الطلبات الخاصة بالمعلومات	تعطل النظام يؤثر على عدد صغير من المستخدمين
منخفض	خلل غير رئيسي لن يؤثر على الوظائف والعمليات والإجراءات الرئيسية حيث يتعطل النظام ويكون المستخدمة غير قادر على العمل و القيام ببعض الجزاء البسيط من الهام النوط بها, ولكن ل يزال قادر على إتمام معظم الهام الخرى	عطل النظام قد يؤثر على واحد اواثنان من المستخدمين

ويجب اتباع ساعات العمل والمعايير التالية بحسب خطورة وأهمية أعمال الدعم:

ساعات العمل الرسمية:

كل أيام الأسبوع من الاحد الى الخميس بمعدل 8 ساعات يومية.

يجب أن تكون سرعة الرد على المشاكل والعمل على حلها متناسبة مع خطورة المشكلة وأهميتها، يجب ألا تقل جودة الخدمة المقدمة في سرعة الرد خلال ساعات العمل وخارجها على المشاكل وحلها عن القيم التالية:

	خطورة وأهمية المشكلة (Severity)*			
	حرج	عالي	متوسط	منخفض
الرد المبدئي من الدعم/الاستجابة	30دقائق	60دقائق	3ساعة	6ساعة
تحديد المشكلة	60دقائق	خلال 3 ساعة	خلال 12 ساعة	خلال 12 ساعة
خطة عمل حل المشكلة	2-3ساعات	خلال 12 ساعة	خلال 24 ساعة	خلال 24 ساعة
حل المشكلة	الحد الأقصى المقبول لحل المشكلة هو 4 ساعة متصلة، بعد وقت الاستجابة الأولية	الحد الأقصى المقبول لحل المشكلة هو 24 ساعة متصلة من وقت الاستجابة	الحد الأقصى المقبول لحل المشكلة هو ٣ أيام متصلة من وقت الإبلاغ عن المشكلة	الحد الأقصى المقبول لحل المشكلة هو ٦ أيام متصلة من وقت الإبلاغ عن المشكلة

- يجب أن تقدم الشركة آلية ومنهجية للدعم الفني تحقق المعايير الفنية العالية (مثل ITIL) .
- يجب أن تستخدم الشركة أدوات متقدمة مخصصة لتتبع المشاكل والاختبار وحالة المشاكل عنها ومعرفة حالتها وإصدار تقارير أسبوعية و تفصيلية عنها.
- يجب أن تحصل الوزارة على إمكانية الدخول على هذه الأدوات في أي لحظة لقياس أداء العمل ومراقبته ومعرفة حالة المشاكل المختلفة.
- إجراء اختبارات الأداء وعمل تحسين للأداء لأجزاء النظام بشكل دوري OPTIMIZATION (AND TUNING PERFORMANCE) واصدار التقارير بذلك.
- تحسين أداء النظام مع زيادة حجم البيانات والمستندات المتعلقة بذلك.
- توفير النسخ الاحتياطية (Plans Backup) وسياسات الاحتفاظ للأنظمة التي يتم العمل عليها في المشروع وتوفير المستندات المتعلقة بذلك.

- أعمال الصيانة الوقائية الدورية:
  - عمل الصيانة الوقائية بشكل دوري اسبوعياً وشهرياً للنظام وتقديم تقارير بالنتائج.

يلتزم المتعاقد بتوفير وضبط بيئات لعمل التالي لجميع الأنظمة/ لكل نظام أو خدمة يجب توفير التالي:

- توفير بيئة عمل تطويرية (environment Development)
- توفير بيئة عمل تجريبية (Environment Staging)
- توفير بيئة عمل تشغيلية(Environment Production)

- ضمان استمرارية العمال عند الكوارث مما يضمن هذا الحل استمرارية العمال عند حدوث ما يسبب ايقاف بدون انذار مسبق .

مرحلة التوثيق:

- توثيق وتسليم كافة الأعمال التي تم تطويرها بما يشمل تسليم الكود الخاص بالخدمات والتطبيق، ووثيقة الإصدارات القادمة في Devops الخاص بالوزارة.

2. المسؤوليات الواجب الالتزام بها خلال تنفيذ المشروع:

- أي تغيير في نطاق العمل يجب أن يتم عبر نظام التغيير المعتمد إذا تم الموافقة علية من قبل الوزارة.
- الالتزام بجميع الأعمال من خلال نطاق العمل المذكور في الكراسة.
- الالتزام بخطة اتصال ومدة زمنية واضحة لتحقيق أهداف المشروع.
- الالتزام بجميع الخصائص والمواصفات التقنية المذكورة من خلال الكراسة.
- استخدام الأدوات المناسبة لتحقيق الجودة العالية من خلال عناصر المشروع.
- التزام المتعاقد بالسياسات والإجراءات والمعايير المذكورة في الملحقات.
- نقل المعرفة إلى فريق الوزارة فيما يتعلق بجميع المكونات في التطبيق حسب الطلب.
- يلتزم المتعاقد بتطبيق جميع ماورد في نظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم م/19 في تاريخ 9/2/1443هـ، ولوائحه التنفيذية والسياسات الوطنية، وسياسات وزارة السياحة ذات العلاقة، كما يلتزم بتوضيح ما إذا كان يخضع لأي أنظمة في دول أخرى وأثر ذلك على الالتزام بنظام حماية البيانات الشخصية، وتحديد ما إذا كانت هناك جهات فرعية أخرى متعاقدة مع الجهة التي ستشارك البيانات الشخصية ذات الصلة. كما يلتزم المتعاقد بتحديد فئات البيانات الشخصية المعالجة والغرض من المعالجة والالتزام بالمعالجة وفق الغرض المحدد، وتزويد الوزارة بنسخة من جميع البيانات بصيغة شاملة وواضحة ومقروءة، بما يتناسب مع ما تراه الوزارة. ويلتزم المتعاقد بتحديد المدة الزمنية للمعالجة وحذف جميع البيانات، بما في ذلك البيانات الشخصية والمعلومات والوثائق الأخرى التي تم الحصول عليها من وزارة السياحة أو تولدت لخدمة المشروع بمجرد الانتهاء من الغرض المتفق عليه، أو إنهاء العقد، أو بناءً على طلب صاحب البيانات أو الوزارة، مع التنسيق المسبق وتزويد الوزارة بنسخة مقروءة قبل الحذف.
- يلتزم المتعاقد باتخاذ كافة التدابير اللازمة لضمان الحفاظ على أمن وحماية البيانات الشخصية ذات الصلة، ويشعر الوزارة خلال 24 ساعة في حال حدوث تسرب أو اختراق ، يتعلق بالبيانات الشخصية، ويتحمل المتعاقد المسؤولية عن الإجراءات والعواقب الناشئة في حال حدوث تسرب أو خرق أو حادث للبيانات أو البيانات الشخصية، كما يلتزم بأي مهام توكل له فيما يتعلق بالوزارة وفقاً لنظام حماية البيانات الشخصية ولوائحه التنفيذية والتعاون مع الوزارة عند إجراء التحقق من الالتزام بالنظام، ويتحمل المتعاقد مسؤولية ما ينتج عن معالجة البيانات الشخصية التي تم الحصول عليها أو توليدها بناءً على العقد.
- الالتزام التام بتطبيق كافة الضوابط والمعايير والتشريعات المتعلقة بالأمن السيبراني وحماية البيانات، وفقًا لما يصدر من الهيئة الوطنية للأمن السيبراني والهيئة السعودية للبيانات والذكاء الاصطناعي، بالإضافة إلى أي متطلبات تصدر من وزارة السياحة.

3. جدول مراحل ومخرجات المشروع:

المرحلة	المخرج	مدة التنفيذ/موعد التسليم
مرحلة التصميم	تقديم تقرير التصور المبدئي للتطبيق	خلال أسبوعين من توقيع العقد
مرحلة التحليل	تقرير بجميع الأعمال المنجزة المشار إليها بنطاق العمل واعتمادها من قبل مدير المشروع بالوزارة	خلال شهر من توقيع العقد
مرحلة التطوير	تقرير كل شهرين بإطلاق التطبيقات والخدمات وجميع الأعمال المنجزة المشار إليها بنطاق العمل واعتمادها من قبل مدير المشروع بالوزارة	طوال مدة المشروع
مرحلة الدعم	تقرير كل ثلاثة أشهر بجميع الأعمال المنجزة المشار إليها بنطاق العمل واعتمادها من قبل مدير المشروع بالوزارة	طوال مدة المشروع
مرحلة التوثيق	تقرير بجميع الأعمال المنجزة المشار إليها بنطاق العمل واعتمادها من قبل مدير المشروع بالوزارة	خلال الشهر الأخير من المشروع

4. الفترة الزمنية لتنفيذ المشروع:

مدة تنفيذ المشروع 6 شهر وتبدأ من تاريخ توقيع العقد.

وينبغي على مقدم العرض إعطاء خطة تفصيلية عن كيفية إنجاز الأعمال وفق جدول زمني يوضح كيفية إنجاز الأعمال ونطاق العمل خلال هذه الفترة.

5. آلية الاشراف والمتابعة:

آلية الاشراف والمتابعة على المشروع من قبل الإدارة المالكة للعقد "الإدارة العامة لحلول تقنية المعلومات".

6. الدفعات المالية للمشروع:

المرحلة	المخرج	نسبة الدفعة %
مرحلة التصميم	بعد الانتهاء من تسليم تقرير التصور المبدئي للتطبيق وجميع الأعمال المشار اليها بنطاق العمل واعتمادها من قبل مدير المشروع بالوزارة	%20
مرحلة التحليل	بعد الانتهاء من تسليم تقرير بوثيقة المواصفات ومتطلبات العمل بشكل كامل وجميع الأعمال المشار اليها بنطاق العمل واعتمادها من قبل مدير المشروع بالوزارة	%20
مرحلة التطوير	بعد الانتهاء من تسليم تقرير كل شهرين يشمل إطلاق التطبيقات والخدمات وجميع الأعمال المشار اليها بنطاق العمل واعتمادها من قبل مدير المشروع بالوزارة	%30 (مقسمة الى 3 دفعات بواقع 10% لكل دفعه)
مرحلة الدعم	بعد الانتهاء من تسليم تقرير كل 3 أشهر بالدعم التقني للخدمات والتطبيقات لضمان عملها بشكل سليم وجميع الأعمال المشار اليها بنطاق العمل واعتمادها من قبل مدير المشروع بالوزارة	20% (مقسمة الى دفعتين بواقع 10% لكل دفعه)
مرحلة التوثيق	بعد الانتهاء من تسليم تقرير توثيق وتسليم كافة الأعمال التي تم تطويرها بما يشمل تسليم الكود الخاص بالخدمات والتطبيق وجميع الأعمال المشار اليها بنطاق العمل واعتمادها من قبل مدير المشروع بالوزارة	10%

معايير تقييم العروض

ستخضع العروض المقدمة للوزارة للتقييم من خلال مرحلتين:

- أولاً: مرحلة التقييم الفني
- ثانياً: مرحلة التقييم المالي

تخضع العروض الفنية للتقييم من خلال تطبيق الضوابط الفنية والمعتمدة في وثيقة الشروط والمواصفات، وفي هذه المرحلة يتم استبعاد العروض التي لا تحقق الحد الادنى من الدرجات المطلوبة ويتم تأهيل العروض الفنية التي تلبي احتياجات الوزارة لمرحلة التقييم المالي.

تتم ترسية العقد على مقدم العطاء صاحب العرض المالي الأقل والأفضل فنيا.

وتشترط الوزارة في مقدم العرض أن يكون متخصصًا في مجال هذه المنافسة وذو موقف مالي مستقر ولديه خبرة وكفاءة في مشاريع مماثلة.

يجب أن تتضمن العروض الفنية، على سبيل المثال لا الحصر، ما يلي:

- المنهجية المقترحة والإطار الزمني
- قائمة بالفريق المقترح توضح تخصصات ومدة عمل ومدخلات كل منهم
- بيانات مؤهلات وخبرات أعضاء الفريق الأساسي وتأكيد بتوفرهم والتزامهم بالعمل.
- الحد المتوقع للاستعانة بالمصادر الخارجية ومؤهلات هذه المصادر المقترحة
- تفاصيل عن مشاريع مماثلة مع نسخ للاطلاع عليها من قبل الوزارة.

أولاً: المعايير الفنية لتقييم العروض:

يتم حساب النتيجة الإجمالية للعرض الفني على أساس الاستجابة لنطاق العمل ومن خلال تطبيق المعايير التالية:

رقم	المعيار الرئيسي	المعيار الفرعي	آلية احتساب الدرجة	الوزن
1	الخبرات السابقة	عدد سنوات الخبرة في مجال المنافسة	➢ 10-7 سنوات فأكثر – (كامل الدرجة) ➢ 6-4 سنوات – (نصف الدرجة) ➢ 3-1 سنوات (ربع الدرجة) ➢ عدم وجود سنوات خبرة في المجال (تحسم كامل الدرجة)	45
2	الكفاءة الفنية	التقنيات المستخدمة في تنفيذ الأعمال المطلوبة	➢ التقنيات المستخدمة في التنفيذ حسب الأنظمة معتمدة عالمياً - غير المتعارف عليها ولا يوجد لها مراجع وقصص نجاح لها- (منخفض) (ربع الدرجة) ➢ التقنيات المستخدمة في التنفيذ حسب الأنظمة معتمدة عالميا - غير المتعارف عليها، ولكن هناك مراجع وقصص نجاح لها (متوسط) - (نصف الدرجة) ➢ التقنيات المستخدمة في التنفيذ حسب الأنظمة المتعارف عليها وسهلة الاستخدام (عالي) - (كامل الدرجة)	20
3	منهجية العمل	تقييم مدى وضوح منهجية العمل على أن تشتمل على سبيل المثال ليس الحصر كل من: (تحديد الأهداف والأدوار والمسؤوليات، خطة عمل والجدول الزمني، أدوات التنظيم والإدارة، آليات التواصل، المتابعة والتقييم الدوري)	➢ كفاءة وتقييم مدى وضوح منهجية تشتمل على عنصرين فقط فأقل – (ربع الدرجة) ➢ كفاءة وتقييم مدى وضوح منهجية تشتمل على ثلاثة عناصر الى خمسة عناصر أساسية – (نصف الدرجة) ➢ كفاءة وتقييم مدى وضوح منهجية تشتمل على ستة عناصر أساسية فأكثر – (كامل الدرجة)	20
4	فريق عمل المشروع	تقييم كفاءة وتخصص الفريق العمل للمشروع، بما في ذلك مؤهلات الموظفين وخبراتهم حسب جدول المواصفات لفريق العمل	➢ كفاءة وتخصص الفريق المقترح متوافق الى حد ما وتم الالتزام بشروط التوطين - (نصف الدرجة) ➢ كفاءة وتخصص الفريق المقترح متوافق وتم الالتزام بشروط التوطين - (كامل الدرجة)	15

درجة القبول للتأهل لفتح العرض المالي هي الحصول على75 نقطة كحد أدنى في تقييم العرض الفني، ويتم استبعاد العرض الفني في الحالات التالية:

- إذا فشل في تحقيق الحد الأدنى للتقييم.
- إذا اشتمل على معلومات مالية عن العرض المقدم.
- عدم تلبيته لمتطلبات الوزارة.
- عدم مراعاته لنطاق العمل بالمشروع.
- عدم إرفاق السير الذاتية للكوادر الإدارية والفنية.

وفيما يلي وصف تفصيلي لضوابط التقييم الفني:

1 الخبرات السابقة: (45 نقطة)

يتم تقييم هذا المعيار استنادًا إلى معيار واحد فرعي وهو: عدد سنوات الخبرة في مجال المنافسة.. أما فيما يخص الوثائق المطلوبة للتحقق فهي قد تكون:

- قائمة المشاريع السابقة مع تفاصيل النجاح
- الشهادات من العملاء السابقين
- خطابات انتهاء الأعمال

2 الكفاءة الفنية: (20 نقطة)

يتم تقييم الكفاءة الفنية بداية في المجال المحدد ويتعين على مقدم العرض تقديم الوثائق أدناه حيث ينطبق:

- تقارير مفصلة عن التقنيات المستخدمة وشهادات اعتماد من جهات معترف بها
- خطة ضبط الجودة
- شهادات إدارة الجودة مثل الأيزو ISO 9001
- دليل الجودة ونماذج إجراءات الجودة
- اتفاقية مستوي الخدمة

وأخيراً يتم التقييم بناء على تقييم مدى توافق المعدات أو التقنيات الجديدة أو التطبيقات الجديدة مع ما تملكه الوزارة حالياً ويتم التحقق من خلال:

- تقارير التوافق الفني
- شهادات الاعتماد

3 منهجية العمل: (20 نقطة)

تقييم شمولية ووضوح منهجية العمل والبرنامج الزمني المقترح من خلال تقديم عرض مفصل للمنهجية المقترحة لتنفيذ المشروع توضح المهام الرئيسية وترابطها والبرنامج الزمني لكافة مراحل الشروع، وشمولية قائمة المخرجات النهائية للمشروع.

ويتعين على مقدم العرض تقديم ما يلي مع الوصف ما أمكن: إدراك مقدم العرض للأهداف المطلوبة، أسلوب العمل ومنهجية تنفيذ المشروع، آلية إدارة

المشروع، الأنشطة والمهام الرئيسية، البرنامج الزمني مراحل المشروع، المخرجات، مواعيد التسليم، فريق عمل المشروع، أدوار ومسئوليات فريق العمل،

طرق تحديد المخاطر المحتملة وخطة التعامل معها ومعالجتها، القيمة المضافة لمقدم العرض، التناغم في تقديم العرض وتناسق المحتويات والأسلوب والمنهجية مع خطة العمل.

4 فريق عمل المشروع:(15 نقطة)

تقييم كفاءة وتخصص فريق عمل المشروع المخصصة للمشروع، بما في ذلك مؤهلاتم وخبراتهم حسب جدول المواصفات لفريق العمل، ويمكن التحقق من خلال:

- السير الذاتية لفريق العمل
- شهادات الخبرة والتدريب

5 للاستفسار:

يمكنكم تقديم الاستفسارات باللغة العربية عبر منصة اعتماد.

ثانياً: المعايير المالية لتقييم العروض:

يتعين على مقدم العرض أن يقدم العرض المالي داخل مظروف مغلق ومستقل عن بقية مستندات العرض الأخرى ومحتوياته. ويلتزم مقدم العرض بالتقيد بما يلي: -

- استخدام جداول الأسعار المبينة في قسم جداول الأسعار علماً ان التكلفة الاجمالية للمشروع يجب أن تكون شاملة ضريبة القيمة المضافة مع ايضاح الاسعار الافرادية والاجمالية رقماً وكتابة.
- عدم إيراد أي بيانات مالية في أي جزء من أجزاء العرض الفني، أو أن تكون واضحة الدلالة من المعلومات الواردة في الأجزاء الأخرى من العرض، باستثناء العرض المالي.
- تشتمل البيانات المالية، على سبيل المثال لا الحصر، على التكاليف والأتعاب والرسوم والأسعار والأجور وأي مصاريف أخرى.
- تقديم جميع الأسعار بالريال السعودي.

جدول الأسعار							
الرقم	الأعمال	الوحدة	الكمية	السعر الافرادي		السعر الاجمالي	
				رقماً	كتابةً	رقماً	كتابةً
1	مرحلة التصميم	تقرير	1				
2	مرحلة التحليل	تقرير	1				
3	مرحلة التطوير	تقرير	3				
4	مرحلة الدعم	تقرير	2				
5	مرحلة التوثيق	تقرير	1				
التكلفة الإجمالية للمشروع شاملة ضريبة القيمة المضافة بالأرقام:							
التكلفة الإجمالية للمشروع شاملة ضريبة القيمة المضافة كتابة:							

ملاحظات مهمة: -

- **يلتزم مقدم العرض بتعبئة جدول الأسعار وختم كامل صفحات الكراسة وإرفاقه مع العرض.**
- **تعتبر هذه الوثيقة جزء لا يتجزأ من كراسة الشروط والمواصفات المرجعية المعتمدة والمرفقة في منصة إعتماد.**

التقديمات المطلوب ارفاقها من قبل مقدم العرض

- يلتزم مقدم العرض بتعبئة جدول الأسعار وختم كامل صفحات الكراسة وإرفاقه مع العرض
- تعتبر هذه الوثيقة (الكراسة) جزء لا يتجزأ من كراسة الشروط والمواصفات المرجعية المعتمدة والمرفقة في منصة اعتماد.
- يجب أن تشتمل الأسعار على جميع التكاليف بما في ذلك تكاليف الشحن، والجمارك، ورسوم التخليص، والتوريد.
- ملف الشركة (Company profile)
- نموذج الموائمة مع نطاق العمل (Project compliance template).
- شهادات الخبرة للكوادر (CV).
- الخبرات السابقة للمتعاقد
  - ذكر الاعمال السابقة في نفس المجال
  - أهم المستفيدين من اعمال المتعاقد
- خطة إدارة عمل المشروع، على أن تشمل ما يلي:
  - خطة العمل
  - إدارة نطاق العمل
  - الجدول الزمني (ينبغي على مقدم العرض إعطاء خطة تفصيلية عن كيفية إنجاز الأعمال وفق جدول زمني يوضح كيفية إنجاز الأعمال ونطاق العمل خلال هذه الفترة).
  - إدارة الموارد
  - إدارة المخاطر
  - إدارة المشكلات
  - إدارة الاتصال
  - إدارة الجودة
  - نماذج التقارير الدورية

الملحقات

1. متطلبات مكتب البنية المؤسسية:

إذا كان المشروع يحتوي على تطوير تطبيقات أو توريد أجهزة فإنه يجب على المقاول تلبية متطلبات البنية المؤسسية التالية عند تنفيذ المشروع:

- يجب المو ائمة مع إدارة البنية المؤسسية في تصميم الحل التقني .
- أن في حال توفير الاجهزة ان تكون ملك للمتعاقد.
- على المقاول اتباع منهجية معتمدة في التخطيط والتطوير وخطط التحويل والتنفيذ طوال مدة المشروع وأخذ المو افقات
- يجب على المقاول خلال فترة عمل المشروع إدارة وتحديث الهيكل الخاص بالمشروع وذلك باستخدام الأدوات والإجراءات والنماذج المتاحة في إدارة البنية المؤسسية داخل الوزارة، سيتم توفير الإجراءات والنماذج من قبل الوزارة للمقاول الفائز بالعقد .
- يجب أن تتو افق تفاصيل هيكل الحلول المقدمة مع إطار عمل البنية المؤسسية في الوزارة حيث يشمل إطار عمل البنية المؤسسية على سبيل المثال لا الحصر مبادئ ومعايير البنية المؤسسية .
- يجب أن يتم توثيق كامل تفاصيل هيكل الحلول المقدمة باستخدام أدوات التوثيق المستخدمة في الوزارة من قبل المقاول الفائز بالعقد حيث يشمل هيكل الحلول على:
  - تفاصيل هيكل الأعمال ويتضمن على سبيل المثال لا الحصر الاستر اتيجية والإجراءات والاهداف والخدمات التي تدعم الحلول المقدمة
  - تفاصيل هيكل الأنظمة والتطبيقات ويتضمن ذلك على سبيل المثال لا الحصر مكونات التطبيقات والواجهات والتقنيات المستخدمة .
  - تفاصيل هيكل التكامل بين الأنظمة والتطبيقات ويتضمن ذلك على سبيل المثال لا الحصر التكامل مع الجهات الداخلية والخارجية.
  - تفاصيل هيكل البيانات ويتضمن ذلك على سبيل المثال لا الحصر المعلومات والبيانات المستخدمة في الحلول المقدمة
  - تفاصيل هيكل التقنيات ويتضمن ذلك على سبيل المثال لا الحصر الأجهزة والتقنيات والانظمة التي تخدم الحلول المقدمة
  - تفاصيل الهيكل الأمني ويتضمن ذلك على سبيل المثال ال الحصر التصميم الأمني، التقنيات والسياسات الأمنية المستخدمة .
- وثائق هيكل وتصميم الحلول يجب أن تتو افق مع وثائق إطار عمل البنية المؤسسية وأن يتم مراجعتها والمو افقة عليها من قبل إدارة البنية المؤسسية .
- يجب أن تتو افق البرامج والتقنيات المقدمة مع مواصفات و أفضل ممارسات البنية المؤسسية .
- يجب الحصول على مو افقة إدارة البنية المؤسسية لإجراء أي تغيير على الهيكل المؤسسي .
- في حالة عدم التو افق مع المبادئ والمعايير ومواصفات الهيكلة المؤسسية، على المقاول أن يتقدم بطلب استثناء من إدارة البنية المؤسسية على أن يقوم بطلب مو افقة أخرى في وقت لاحق .

2. متطلبات الأمن السيبراني ضمن المشاريع المعلوماتية والتقنية:

*** قد يطلب فريق إدارة الأمن السيبراني في الوزارة من مقدم العرض تقديم الأدلة على بعض أو كل المتطلبات المنصوص عليها في هذه الكراسة.**

*** يحق للفريق المختص من إدارة الأمن السيبراني في الوزارة إجراء عمليات المراجعة والتدقيق السيبراني Assessment & Audit والمراقبة الأمنية لجميع الأعمال والأنشطة المتعلقة بأصول الوزارة.**

*** ستخضع العروض الفنية المقدمة للوزارة للتقييم من قبل إدارة الأمن السيبراني للتأكد من تطبيق الضوابط الفنية والمعتمدة والمعايير الأمنية الصادرة من الجهات المعنية -على سبيل المثال لا الحصر- مثل: وجود محلي للنظام أو التطبيق المقدم On-premises software، التزام مقدم العرض بضوابط الهيئة الوطنية للأمن السيبراني ، اجتياز مقدم العرض للاختبارات والتقييمات السيبرانية.**

*** يتم استبعاد مقدم العرض في حال عدم اجتيازه التقييم الفني للجوانب الأمنية للمشروع من قبل إدارة الأمن السيبراني.**

- بعض معايير أو متطلبات الأمن السيبراني التي يجب على مقدم العرض أخذها بعين الاعتبار في أي مشروع أو أي تغيير على الأصول التقنية أو قبل إطلاق وتدشين تطبيقات الوزارة. ومن هذه المعايير أو المتطلبات، على سبيل المثال لا الحصر:
  - تقييم المخاطر.
  - تقييم الثغرات.
  - اختبار الاختراق قبل إطلاق أي تطبيقات جديدة.
  - مراجعة الكود المصدري.
  - مراجعة الإعدادات والتحصين (Secure Configuration and Hardening)
  - مراجعة حزم التحديثات قبل إطلاق، وتدشين التطبيقات، والمشاريع، والتغييرات.
  - التأكد من استخدام البرامج والحزم المرخصة.
  - التأكد من أن أي تصميم للتطبيق يجب أن يدعم المعمارية متعددة المستويات.
  - التأكد من استخدام معايير التطوير الآمن للتطبيقات (Secure Coding Standards).
  - التأكد من استخدام مصادر مرخصة وموثوقة لأدوات تطوير التطبيقات والمكتبات الخاصة بها (Libraries).
  - إجراء اختبار للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمنية السيبرانية للوزارة.
  - مراجعة أمن التكامل (Integration) بين التطبيقات.

- يتم إجراء الاختبارات السيبرانية من قبل فريق إدارة الأمن السيبراني في الوزارة أو تحت إشرافهم، وعلى المتعاقد إصلاح الملاحظات الناتجة من هذه الاختبارات ودمجها في تصميم الحل وتطويره. إذا كان إصلاح هذه الملاحظات يتطلب تكلفة إضافية، فيجب أن يتحملها المتعاقد.
- يجب فحص مصدر الكود للبرنامج المقدم إلى الوزارة والتأكد من خلوه من الثغرات أو نقاط الضعف البرمجية باستخدام المعايير الآمنة وأدوات الفحص لأمان مصدر الكود، وذلك من قبل المتعاقد وبإشراف إدارة الامن السيبراني في الوزارة والتنسيق معهم وفقا لاشتراطات الوزارة.
- يجب على المتعاقد تقديم تقرير مراجعة الكود (أو ما يعادله، مثل بيان ضمان مستقل) وفقًا لطلب إدارة الامن السيبراني بالوزارة في حالة تعذر تقديم مصدر الكود.
- يجب على المتعاقد التأكد من أن يدعم النظام / التطبيق مبدأ المعمارية متعددة المستويات، الويب والتطبيقات وقاعدة البيانات المنفصلة.
- يجب على المتعاقد التأكد من أن يدعم النظام / التطبيق الاحتفاظ بسجلات الأحداث وتخزينها.
- يجب على المتعاقد التأكد من أن يتمتع النظام / التطبيق بالقدرة على تصدير السجلات إلى نظام إدارة الأحداث والسجلات للوزارةSIEM .
- يجب على المتعاقد تشفير البيانات الحساسة أثناء التخزين والنقل باستخدام معايير بروتوكولات التشفير المعمول بها في الوزارة.
- يجب على المتعاقد تطوير تطبيقات الويب والجوال للنظام (حسب ما تقتضيه الحاجة) باتباع أفضل ممارسات الأمان والمعايير القياسية في المجال، على سبيل المثال OWASP
- يجب على المتعاقد التأكد من أن يتمتع النظام بالقدرة على إدارة الجلسات على سبيل المثال التعامل الآمن مع الطلبات المتعددة لتطبيق أو خدمة مستندة إلى الويب، أو مهلة الجلسة الخاملة، إلخ
- يجب على المتعاقد التأكد من أن يستخدم النظام طرقًا آمنة للاتصال بأنظمة أخرى مثل اتصالات API الآمنة واتصالات MQ الآمنة وما إلى ذلك.
- يجب أن تغطي متطلبات الأمن السيبراني، لإدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية للأنظمة الحساسة في الوزارة، بحد أدنى؛ ما يلي:
  - إجراء اختبار التحمل (Stress Testing) للتأكد من سعة المكونات المختلفة.
  - التأكد من تطبيق متطلبات استمرارية الأعمال.

- يجب أن تغطي متطلبات الأمن السيبراني، لمشاريع تطوير التطبيقات، والبرمجيات الخاصة بالأنظمة الحساسة للوزارة، بحد أدنى؛ ما يلي:
  - إجراء مراجعة أمنية للشفرة المصدرية، قبل إطلاقها (Security Source Code Review).
  - تأمين الوصول، والتخزين، والتوثيق للشفرة المصدرية (Source Code) وإصداراتها.
  - تأمين واجهة برمجة التطبيقات (Authenticated API).
  - النقل الآمن والموثوق للتطبيقات من بيئات الاختبار (Testing Environment) إلى بيئات الإنتاج (Production Environment) مع حذف أي بيانات، أو هويات، أو كلمات مرور، متعلقة ببيئات الاختبار، قبل النقل.

- يجب تقييم الثغرات من قبل إدارة عمليات الأمن السيبراني أو تحت إشرافهم، ومعالجتها من قبل المتعاقد وفقا للأولوية والإطار الزمني والمضمن في اتفاقية مستوى الخدمة كالآتي:

تصنيف المخاطر Risk Rating	☐ None لاشيء	☐ Low منخفض	☐ Medium متوسط	☐ High عالي	☐ Critical حرج
الإطار Mitigated Timeframe الزمني للمعالجة	No Action بلا إجراء	30 يوما	12 يوما	8 أيام	5-0 أيام
تقديم Risk Rating Presented by تصنيف المخاطر من خلال	☐ Vulnerability Assessment تقييم الثغرات		☐ Penetration Testing اختبار الاختراق		☐ Risk Assessment تقييم المخاطر

*** يجب على المتعاقد الالتزام بما ورد في اتفاقية مستوى الخدمة SLA المتعلقة بالمشروع، وفي حال عدم قيام المتعاقد بمعالجة الثغرات والملاحظات حسب تصنيفها خلال الإطار الزمني المتفق عليه لمعالجتها فسيتم تطبيق غرامة التأخير المنصوص عليها في العقد .**

- التزام المتعاقد بمتطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات بالتنسيق مع إدارة عمليات الامن السيبراني وتقنية المعلومات في الوزارة.
- يجب أن تتضمن متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات بحد أدنى ما يلي:
  - وحدة إدارة المستخدم التي تدعم التكامل مع خادم الدليل النشط User Admin module supports integration with Microsoft Active directory server (LDAP).
  - يجب أن يوفر النظام القوى العاملة لإنشاء الأدوار (مثل مسؤول النظام والمشرف والمدقق والمشغل).
  - تقديم تقرير بجميع الأدوار والوظائف المسموح بها.
  - تقديم تقرير بجميع معرفات/هويات المستخدم مع دورها وملفها الشخصي وحالتها.
  - يجب أن يوفر النظام إمكانية إلغاء تنشيط المستخدم وإعادة تنشيطه مؤقتًا (أثناء فترة الإجازة).
  - التحكم في الوصول إلى النظام بواسطة معرفات المستخدم وكلمات المرور.
  - يجب أن يوفر النظام قفل الشاشة بعد X دقيقة (قابلة للتكوين) من وقت عدم النشاط.
  - يجب أن يكون الحل المقترح قادرًا على دعم آليات التحقق من الهوية متعدد العناصر Multi Factor Authentication للمستخدمين المتميزين على سبيل المثال مدير نظام تقنية المعلومات.
  - يجب أن يتمتع الحل المقترح بالقدرة على دعم إمكانية الدخول الموحد Single Sign on أثناء التعامل مع تطبيقات متعددة داخليًا داخل الوزارة.
  - تعيين كل مستخدم إلى مجموعة معينة، حيث سيكون لكل مجموعة مستويات وصول خاصة بها access levelsعند استخدام التطبيق. يجب أن يتم تغيير مجموعات المستخدمين عبر إعدادات التكوين configuration
  - يجب أن يكون الحل المقترح قادرًا على توفير فصل واضح للواجبات segregation of duties (على سبيل المثال، صانع ومدقق)
  - يجب أن يتمتع النظام بالقدرة على إنشاء تقارير الأحداث الأمنيةsecurity events reports .

- تقديم جلسات تدريبية Training sessions .
- تحديد عدد المستخدمين الذين يتم ترخيصهم لهذا النظام.
- يجب تسليم بيانات مسؤول النظام المحلي local admin credentials .
- تزويد جميع الأدلة المتوفرة وأدلة المستخدم user manualsلكل دور مستخدم في النظام ومدير النظام.

إدارة التغيير CHANGE MANAGEMENT

- يجب أن يتم إشراك الإدارة العامة للأمن السيبراني من بداية المرحلة الأولية لأي تغييرات وذلك للقيام بتقييم التغييرات.
- في حالة وجود تغييرات تحتاج إلى التطبيق على البيئة التشغيلية Operating Environment فإنه يجب أن يتم تطبيقها من قبل موظفي الوزارة وإذا كانت التغييرات بحاجة إلى تطبيق من قبل المتعاقد فهم بحاجة إلى تقديم خطة تغيير وخطة الرجوع إلى الوضع الحالي والخطوات الموثقة لتطبيق جميع تفاصيل التغيير ويجب على موظفي الوزارة تطبيق التغييرات بمساعدة المتعاقد دون تعاملهم مع النظام أو الخوادم في البيئة التشغيلية، وإذا اقتضى الأمر فإنه يجب اعتماد موافقة الإدارة العامة للأمن السيبراني أولاً.
- يجب على إدارة التغيير التأكد من أن يتضمن إجراء إدارة التغيير ما يلي:
  - وصف وسبب التغيير.
  - معلومات تشير إلى تنفيذ التغيير على البيئة الاختبارية.
  - تقييم الأثر من الناحية الأمنية والتشغيلية، وما إلى ذلك.
  - الموافقة الرسمية ومنح الصلاحيات قبل الشروع في إجراء التغييرات التي قد يكون لها تأثير كبير على بيئة العمل.
  - التواصل مع جميع الموظفين المعنيين بخصوص التغييرات والتي تشمل:
  - الاتصال المسبق للتحذير من التغييرات.
  - المواعيد المقترحة.
  - إجراءات الإيقاف والرجوع إلى الوضع الحالي في حالة حدوث أي مشاكل.
  - عمليات التخطيط واختبار التغييرات بما يشمل معايير الرجوع إلى الوضع الحالي في حالة إيقاف التغيير.
  - توثيق التغييرات التي تم إجراؤها وجميع الخطوات المتخذة في عملية إدارة التغيير.
  - تحديد التغييرات الجوهرية وتقييم المخاطر التي قد تنتج عن تطبيق هذه التغييرات بما في ذلك تحليل أي تأثير محتمل وكذلك تحديد وتعريف الضوابط والتدابير اللازمة لتقليل المخاطر وتأثير حدوثها.
  - تسجيل وتوثيق جميع التغييرات في سجل التغييرات.
- يجب على الإدارات المعنية بالوزارة تغيير أي خدمات مقدمة من الأطراف الخارجية عند الحاجة وفقًا لسياسة وإجراء إدارة التغيير الخاصة بالوزارة.

متطلبات الأمن السيبراني المتعلق بالأطراف الخارجية

- يجب على المتعاقد ضمان الامتثال لسياسات الأمن السيبراني في الوزارة بالإضافة لمتطلبات الأمن السيبراني الصادرة من الجهات التشريعية في المملكة العربية السعودية، مثل الهيئة الوطنية للأمن السيبراني ومكتب إدارة البيانات الوطنية وغيرها من الجهات ذات العلاقة.
- يجب أن يتضمن أي عقد أو اتفاق مع أي طرف خارجي بندًا بعدم الإفصاح، لحماية المعلومات والبيانات، والأصول المعلوماتية والتقنية الخاصة بالوزارة، لضمان الوصول إليها بطريقة آمنة.
- يلتزم المتعاقد بإبلاغ الوزارة مباشرةً عند حدوث حادثة أمن سيبراني قد تؤثر على البيانات التي تمت مشاركتها أو إنشائها.
- يجب على المتعاقد تحديد ممثل للمشروع أو نقطة اتصال من إدارة الأمن السيبراني الخاصة بهم لإخطار الوزارة على الفور بأي حادثة أمن سيبراني (مثل اختراق البيانات، وما إلى ذلك) لبيئة المتعاقد و / أو أي من منتجاته المقدمة إلى الوزارة، والتي تشكل خطرًا على الوزارة و / أو أعمال الجهات التابعة لها، عن طريق البريد الإلكتروني incident@mt.gov.sa
- يجب على المتعاقد تمكين و / أو تقديم المعلومات ذات الصلة للإدارة المعنية بالأمن السيبراني في الوزارة أثناء التحقيق في مثل هذه الحوادث.
- يجب إجراء المسح الأمني (Screening or Vetting) لشركات خدمات الإسناد، ولموظفي خدمات الإسناد، والخدمات المدارة والعاملين على الأنظمة الحساسة، ولموظفي الأطراف الخارجية، وموظفي شركات الخدمات الاستشارية الذين لديهم صلاحيات الاطلاع على البيانات.
- يجب على المتعاقد التوقيع على اتفاقية عدم الإفشاء والسرية وسياسة الاستخدام المقبول لموظفي الأطراف الخارجية للسماح لهم بالوصول إلى المعلومات السرية أو المعلومات ذات الاستعمال الداخلي، وبعد الحصول على الموافقات المطلوبة التي تشمل قيوداً على الوصول والاستخدام لبيانات ومعلومات الوزارة.
- يجب على المتعاقد التوقيع على سياسة الأجهزة المحمولة والخاصة بالجهات الخارجية قبل المشاركة في المشاريع التي تتطلب الوصول إلى شبكة الوزارة بواسطة جهاز خارجي.
- يجب أن يضمن المتعاقد تلقي جميع موظفيه العاملين في الوزارة، جلسات توعية، لزيادة الوعي بالأمن السيبراني والتهديدات والمخاطر السيبرانية وضرورة الالتزام بسياسات الأمن السيبراني.
- يجب عند إبرام العقود واتفاقيات مستوى الخدمة (SLA)، توثيق ما يتعلق بالتزامات كلا الطرفين للوفاء بمتطلبات الأمن السيبراني ذات العلاقة.
    - يجب تضمين البنود التالية داخل الاتفاقيات من أجل الوفاء بمتطلبات الأمن السيبراني المحددة، على سبيل المثال لا الحصر:
        - تصنيف المعلومات حسب نظام تصنيف الوزارة.
        - الالتزام بجميع سياسات الأمن السيبراني بالوزارة والمتطلبات القانونية والتنظيمية والتشريعية ذات العلاقة وحقوق الملكية الفكرية وحقوق النشر.
        - مراجعة الأداء، والمراقبة، ورفع التقارير والتدقيق.
        - الالتزام بتطبيق إجراءات التواصل الخاصة بحوادث الأمن السيبراني، وخاصة التنبيهات والتصعيد أثناء حوادث الأمن السيبراني وخلال عمليات معالجة تلك الحوادث.

- بنود عدم الإفشاء والإزالة الآمنة للبيانات والمعلومات والأصول المعلوماتية والتقنية للوزارة من قبل أطراف خارجية عقب انتهاء الخدمات.
- يجب أن تكون خدمات الإسناد، والخدمات المدارة على الأنظمة الحساسة؛ عن طريق شركات، وجهات وطنية؛ وفقًا للمتطلبات التشريعية، والتنظيمية ذات العلاقة.
- يجب أن تتواجد أي مراكز للخدمات المدارة للأمن السيبراني للمراقبة والعمليات بالكامل داخل المملكة العربية السعودية.
- للوزارة الحق في التدقيق على أي عمليات أو ضوابط خاصة بالأمن السيبراني للأطراف الخارجية تتعلق بالاتفاقيات الموقعة.

- لن يتم إتاحة الوصول لموظفي أي أطراف خارجية لبيانات ومعلومات الوزارة حتى يتم الحصول على الموافقة بذلك، وبعد أن يتم تطبيق ضوابط الأمن السيبراني المناسبة.
- يجب على الإدارات المعنية بالوزارة القيام بإعادة تصنيف البيانات إلى أقل مستوى يحقق الهدف، قبل مشاركتها مع الأطراف الخارجية ومع شركات الخدمات الاستشارية وذلك باستخدام تقنيات تعتيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling).
- يجب على المتعاقد عدم تخزين معلومات الوزارة على وسائط محمولة حيثما أمكن ذلك مع أخذ الموافقات اللازمة.
- يجب على المتعاقد عدم استخدام معلومات الوزارة أو المعاملات الخاصة بالوزارة لأي غرض آخر غير ما هو محدد في نطاق العمل و / أو نسخها إلى أقراص أخرى أو نقلها إلى مكان آخر دون إذن كتابي وموافقة خطية من الوزارة.
- يجب على المتعاقد مراعاة ضمان عدم استخدام الاتصال بالشبكة (في حال توفير ذلك للدعم عن بُعد ؛ إذا لزم الأمر) لأغراض الاختراق أو المساس بأمان أنظمة الوزارة.
- فصل البيئة الخاصة بالوزارة (خصوصا الخوادم الافتراضية) عن غيرها من البيئات الأخرى التي يستضيفها مزود الخدمة السحابية من قبل المتعاقد.
- يجب على المتعاقد إعادة معلومات أعمال الوزارة بصيغة قابلة للاستخدام ، وحذف بيانات الوزارة بطرق آمنة عند الانتهاء/إنهاء العلاقة التعاقدية مع تقديم الأدلة على ذلك.

3.متطلبات المعايير التقنية:

1. INTRODUCTION

This document discusses the technical standards which will be used to develop or maintain web/mobile applications either in in-house development or by vendors.

1.1 REQUIREMENT LEVEL

In this document, certain wording conventions are followed. There are precise requirements and obligations associated with the following terms:

Must	*This requirement is not optional*
May	*The implementer may choose to take one or more of a selection of options but must make a choice of one or more, as dictated within the context of the item*
Should	*The implementer must choose this action unless business functionality dictates otherwise. Exceptions must be approved by management as modifications to the standard practice*

2. DEVELOPMENT

In this section, we will be listing the technologies and architecture of the web applications, including mobile apps:

2.1 DEVELOPMENT METHODOLOGY:

As MT we don't enforce any development methodology, development teams may use any iterative SDLC suitable for their needs.

2.2 TECHNOLOGIES

1. Development of components and mechanisms should be in the programming languages: Microsoft **.NET**/ .**Net Core / MVC .NET** Framework with **C#**, **Latest LTS** version covering the support duration of the project, and if the site will be under MT main site, it should go with **Angular 12+ (using Micro-Frontends)** or please check the current version with Solutions design and development team.

   a) Solution should use following for Identity solution, technologies/tools such as Microsoft Membership, Microsoft Identity Core, Identity Server, Entity Framework Core, Ready API for API Testing, Redis cache, Redis Search, MS SQL Server and approved logging, health check and monitoring solution.

2. The solution should be developed bases on Service Oriented Architecture or Micro-services to be used across the board and serving multiple applications or integrations.
3. Should use Unit Testing framework, such as **MSUnit** Test, **NUnit**, **XUnit** etc. and target code and the test results must be shared by the vendor (development team) for each release and the document must be checked in to MT DevOps.

   a) Live Unit Testing should be used, with 100% code coverage, if possible, if it is less than that, a solid reason should be presented to MT IT and MT IT reserve the right to take any decision on it.

4. Must avoid using Silver Light and Adobe Flash player-based solutions and use the development of dynamic and interactive effects via HTML 5 or better if available at time and latest secure JavaScript libraries.
5. Solution may use technologies such as **containers**, orchestration tools such as **Kubernetes**, given that such capability and capacity is available at MT's system/operation teams end. Prior approval is required from MT Infra & Development Teams.
6. Any **third-party** framework/technology or **off the shelf** software or any such requirement not covered in this document, should be discussed, and approved by MT Director of solutions design and development before inducting in the solution.

2.3 DESIGN AND ARCHITECTURE:

1. A top-level architecture of the system must be established. The architecture should identify items of hardware, application/software, databases, and manual operations. It should be ensured that all the system requirements are allocated among the items. Hardware configuration items, application/software configuration items, database configuration items, and manual operations should be subsequently identified

from these items. The system architecture and the system requirements allocated to the items must be documented.

2. The system architecture and the requirements for the application must be evaluated considering the criteria listed below. The results of the evaluations must be documented. Below requirement are directly related to CMMI Audit:
    a) ***Traceability*** *to the system requirements, this is important for* ***CMMI*** *audit.*
    b) *Consistency with the system requirements.*
    c) *Appropriateness of design standards and methods used.*

d) Feasibility of the application module/component/services fulfilling requirements.

e) Feasibility of operations and maintenance.

3. **Bilingual** so that the system is fully capable of handling all the required procedures in both Arabic and English comprehensively. It is highly appreciated to design the system to add more languages flexibly if required in future.
4. A dynamic reporting mechanism should be developed for all fields of the system and its stages and extraction in multiple electronic formats (PDF, Excel, HTML, etc.) If required PowerBi or Tableau can be used with the prior approval of Tourism Intelligence center.
5. Detailed reports - analysis of procedures and recording of all events (reports and statistics), including fees and graphs.
6. Easy management and updating of the system -the possibility of applying the special criteria and special cases (Administrative System User -Friendly).
7. **Windows Server 2019** or higher must be approved by the system team.
8. The solution must be capable of supporting **CICD** using MT's **Azure DevOps On Premises Platform,** if third party tools are to be used, check the capabilities of the tools so that these tools fit in Azure DevOps on Premises Server ecosystem.
9. Any source code is to be deployed on any environment in MT/DR site/Azure or any other cloud must be scanned and have zero issues reported in the MT source code scanning through DevSecOps https://devSecOps.mt.gov.sa/ .
10. All the components of the solution should be designed to be Highly Available and must be validated with failover testing.
11. Extensive logging (for User actions, errors etc.) should be implemented which must be stored in databases like SQL or Redis. These logs must be visualized using sophisticated tools when required.
12. All public facing portals (G2B, G2C) should be developed as Micro-frontend (Angular) on MT's Unified service delivery platform (USDP) a.k.a MT Portal. *See related point (Integrations 3.5.18).* More details about USDP architecture can be obtained from MTs Solutions Engineering Team.

2.4 MT SKY ARCHITECTURE

These guidelines are for MT SKY System, MT SKY have many components, we are listing few in a new service is to be onboarded:

1. Front end
2. Middleware API
3. Identity Platform
4. Shared Services

2.4.1 Front End

Micro-Frontend architecture on Angular using Module Federation. MT have ready made template for the front end.

2.4.2 Middleware API

Middleware API is built dot.net core 6.x or latest LTS version. MT have a ready-made template for the Middleware API as well.

2.4.3 Identity Platform

Identity platform is SSO solution, which is used to authenticate the users on MT Sky platform.

2.4.4 Shared Services

MT sky have a lot of services available as a wrapper layer through our back end ESB, these include file scan, email, SMS, and push notification services to name a few.

2.5 DOCUMENTATION

The project must produce the following minimum set of documentation:

1. Software Requirement Specification
    a) Functional specification Document
    b) Solution Design Document
    c) Wire frames
2. Use-Case Model
3. User Interface Prototype
4. Logical Data model
5. Physical Data Model
6. Physical Design Document
7. System Architecture Document
8. Logical Design Document
9. Infrastructure Component Placement Diagram
10. Logical Application Deployment Model
11. User manual

Source code should also be properly documented, and IDE's built-in support for source code documentation could be used.

2.6 INTEGRATIONS

1. MT's all integrations are running on SoftwareAG's Enterprise Service Bus (webMethods).
2. With Regards of Economies of scale, any existing application, platform, or hardware must be reused wherever applicable and integrable.
3. Integrations must be developed using webMethods integrations server (minimum ver 10.3) by leveraging Universal Messaging (if applicable).

   Or

   must be used developed in **WCF**, Microsoft .NET/ .Net Core Based **WebAPI.**

   gRPC .Net Ported version or original **gRPC** may be used if appropriate.
4. APIs and web services must be consumed using internal/external API Gateway (SoftwareAG). Therefore, Swagger must be provided.
5. Any uploading document feature requires to use MT's File scanning APIs which works in Async way. So, the upload function should be designed accordingly.
6. APIs and web services must provide authentication mechanisms such as Basic Auth and cannot be published anonymously unless exempted by Development & Security Teams.
7. APIs and web services must be developed using security best practices to avoid attacks just to list a few, CSRF attacks, XSS attacks, SQL injection attacks, and JSON injection attacks.
8. APIs and web services must be tested for functional, performance, and network latency issues.
9. Integration and documentation of all services with history using **MT DevOps** as source code management (Git Repository), including any integration with third-party tool for **CICD**.
10. Should Support for Internet technologies, especially Data Definition Technology (**XML**) or **JSON** (Preferred) or **YAML**, either one of them or all as per project requirements.
11. The possibility of integration with applications and databases based on the scope covered in the RFP.
12. Ability to integrate with the Government Service Bus (GSB) if required.
13. Integrate MT's SMS, MT's Email, File Scanning & Payment gateway (Including Tahseel, Credit & Debit cards, Apple Pay etc..) solutions where-ever required. All these platforms are based on open APIs.
14. Single Sign on for MT Employees by Authenticating from Active Directory/ADFS or Microsoft Intune (MDM) for (Internal) Mobile Apps.
15. For **business process management** and **workflows**, you are encouraged to use **K2**, check availability and capacity with Director of solutions and design and development.
16. If you have such requirement which are not fulfilled by K2 and want to bring your own solution, please contact Director of solutions design and development to take approval.
17. For all integrations, please contact with integrations team integrations.team@mt.gov.sa
18. For all external authentications, MT's Identity platform id.mt.gov.sa must be used. Which is providing two types of authentication providers. IAM (by NIC based on Absher for Saudi Citizens and Residents) & Custom Authentication which covers both GCC nationals & Investors in general.

19. For internal authentications, MT's ADFS (Active directory federation services) or MT's Azure AD authentication should be used (based on the business requirements & getting approval from MT Infra & Solutions Engineering teams).

3. MOBILE APPLICATIONS STANDARDS

3.1 NATIVE

3.1.1 IOS

- Programming language: Swift 5
- Minimum iOS support: iOS 10+
- App store app size: Less than 50mb

3.1.2 ANDROID

- Programming language: Kotlin
- Minimum OS support: Android M and above
- Play store app size: Less than 40 mb

3.1.3 GENERAL

- MVVM design pattern
- S.O.L.I.D Principle
- Unit test
- Analytics
- Offline data support with online sync (if applicable)

3.1.4 HANDOVER

- Source code (At the time of delivery all libraries/SDK should be latest stable version and should support the latest OS versions for iOS and Android)
- XD or Sketch file with all assets and fonts
- Feature Document
- Technical specification document
- Webservice API document
- Test case document
- Handover sessions

3.1.5 DOCUMENTS: (ENGLISH VERSION)

- System Architecture i.e Outline of the application architecture (description of all modules and their correlations).
- Project specification
- Development documents
- Business Requirements files (BRS) latest version
- Functional Specification Document (FSD)
- Project scope and Guidelines

- Use case documents
- Test case documents
- Description of the database structure
- Key Source Code Sections
- Share RCA if any
- Share Existing critical issues and resolution steps
- Application's configuration information (timer Jobs etc. if any)

- Extract data for all change Request if any
- Extract data from task tracking systems as in bugs tracking system if any (like TFS, Jira etc.)
- Staging and Production Environment Build Guide
- Project roadmap and past progress are documented. High-level diagrams are explained.
- Wireframe documents if any
- Code optimization with Third
- Integration documents if any

Note: Once the above documents are available, we can complete the handover.

3.1.6 DETAILED PLAN FOR THE HANDOVER (BY USE CASES):

- Code Walkthrough in the context of use cases

3.2 REACT NATIVE

3.2.1 GENERAL

- React Native (Latest stable version available)
- Minimum OS version: iOS 10+ & Android M +
- React hooks
- Redux
- Stable and feature supportable node packages
- Unit test
- Analytics
- Offline data support with online sync (if applicable)

3.2.2 HANDOVER

- Source code, local dependencies repos, forked repos. (At the time of delivery all libraries/SDK should be latest stable version and should support the latest OS versions for iOS and Android)
- XD or Sketch file with all assets and fonts
- Feature Document
- Technical specification document
- Webservice API document
- Test case document
- Handover session

Note: Any mobile application intended for internal use (employees services) must be integrated with Microsoft MDM (intune) and/or should be part of MT's Super App architecture. Any mobile app intended for public (G2C, G2B) must be integrated with MT's identity services for authentication & authorization (in some cases).

4. UI STANDARDS

1. Implementing w3c standards and minimum adoption of **WCAG 2.0**.
2. Implementing the **Responsive** Design version of the portal with its most important components and pages in accordance with the portal's design and identity and applying the highest standards for the W3c phone version. Source code must be provided so that the source code for all content in the system, which has been developed for this project, is provided with training and documentation
3. Mobile **Material** design is encouraged, the UI of **Mobile App** and Web App should have same theme and concepts.
4. Web UI should be validated against **GTMatrix** and target a minimum 75% rating.
5. **UI** layout should be following **MT design standards and structure** (ask for the reference)

5. SECURITY

The security is the one aspect which is of highly value to us, below are some points which are to be followed including best security practices in placed by organization:

1. Use latest secure third-party libraries, which are vetted by Approved Security Organizations and allowed by Head of Application Development.
2. Writing Secure source code to avoid **Session Hijacking**, **SQL Injection**, XSS Attacks. This should be done at Source code in Programming Language C# and Database Query Language (SQL Server T-SQL) and validate by performing approved **SAST** tools(https://devsecops.mt.gov.sa/)
3. Target **OWASP 2021** Top security risks and validate that the final published site doesn't have any risks mentioned in OWASAP 2017 by scanning the published site using approved **DAST** tools.
4. Personal data should be **encrypted** inside DB like IQAMA/Saudi ID etc. if you need to store credit card number you need to get approval from IT Development Head.
5. Implement **Anti Forgery** techniques for MVC / WebAPI. If you are using **tokens**, make sure you have access and refresh tokens are implemented.
6. Query parameters should be encrypted and try using Form POST method instead of GET wherever it is possible for system changing behavior with proper tokenization of the requests.
7. Query parameters should not have real IDs instead use GUID and non-predictable query string values.
8. Obtain and apply a gateway protection certificate and all Digital Certificate applications.
9. Default ports of any proposed solutions must not be used.

Use two factor authentications wherever possible

6. INFRASTRUCTURE STANDARDS

1. A high-availability deployment of Infrastructure Management consists of two servers with identical configuration, one designated as primary and the other as secondary. At any point, one of the nodes is active and the other in standby mode. If the active node shuts down or otherwise becomes unavailable, the standby node takes over the active role. When you restore the primary server, failback occurs, and it becomes the active node.
2. Use 2 layer of firewall Using firewalls to separate internal and external networks.
3. Use web application firewall.
4. Do vulnerability assessment on all assets.
5. Communication between servers is via specified ports.
6. Use LAPS for managing Windows computer local Administrator passwords.
7. Use gMSAs for securing group managed service accounts (AppPool Accounts).
8. Use ESG protection by blocking email-based threats before they reach a mail serve.
9. Use secure jump host for accessing MT servers.
10. Create MT Databases based on Always On availability groups: a high-availability and disaster-recovery solution or A Windows Server Failover Cluster (WSFC)
11. Enforce install all security updates on software and hardware.
12. Use MFA for accessing MT applications

Note: You may need to refer to other guidelines to understand full landscape of MT standards. This document is updated regularly, you can obtain the latest by contacting any one of the contacts listed at the start of the document.

4.متطلبات الجودة:

- توفير إجراءات متكاملة وواضحة لإتمام عملية اختبار النظام من قبل المستخدمين UAT بحيث تتضمن ولا تقتصر على ما يلي:

1. سيناريوهات حالات اختبارات مناسبة(Test cases scenarios) يتم حفظها في أنظمة تتبع الأخطاء الخاصة لوزارة السياحة (مثل: DevOps)
2. على المورد تحمل تكاليف الأدوات والأجهزة لأداء الاختبارات بجميع أنواعها .
3. يجب على حالات الاختبار ضمان تغطية كاملة للنظام.
4. تضمين جميع حالات الاختبار المباشرة والغير مباشرة.
5. يجب أن حالات الاختبار تركز أولا على وحدات فردية ثم القيام بتوسع تدريجيا لتغطية النظام بأكمله.
6. خطوات تنفيذ السيناريو لحالات الاختبارات، تضمن تجربة الإجراءات هل هي صالحة وغير صالحة (positive testing and negative testing)، حيث السيناريو المراد اختباره يحتوي على خطوات مفصلة وحالات مرتبطة به لتنفيذه بشكل صحيح.
7. حالات الاختبار تتضمن جميع اللغات المنفذة في النظام.
8. اختبارات المحتوى والتدقيق اللغوي للمحتوى أن لزم الامر.
9. تطبيق الاختبارات لتقنيات المتخصصة في مجال الذكاء الاصطناعي ان وجدت
10. حالات الاختبار تتضمن جميع الحالات في تطبيقات الجوال والمتصفحات في الأجهزة الذكية بأحدث الإصدارات.
11. توثيق كافة المشاكل والمخاطر التي قد تحدث في النظام باستخدام تقارير تفصيلية قياسية ومعتمدة.
12. في حال حصول مشكلة أو خطر يجب توثيقها من حيث خطورتها، تأثيرها، كيفية حلها، كيفية تفاديها، باستخدام النماذج القياسية لتوثيق المخاطر والمشاكل (Standard issue/risk log template).
13. تصميم حالات الاختبارات يتم حفظها في أنظمة تتبع الأخطاء الخاصة لوزارة السياحة (مثل: DevOps)

- تقارير اختبار الأداء والتحمل يتم تنفيذها قبل نقل المشروع على البيئة التشغيلية، باستخدام أحدث التقنيات حيث تتكفل الشركة المنفذة تكلفة الأدوات المستخدمة مثل : AWS , Gravana, Jmeter .
- تقارير اختبار قابلية الاستخدام: لإنشاء نظام سهل الفهم والاستخدام والتصفح مع السرعة في الأداء أخذ بعين الاعتبار تجربة المستخدم عن طريق تسلسل العمليات وسهولة الواجهات.
- تقارير اختبار الأتمتة: تنفيذ اختبارات الأتمتة للعمليات و قواعد البيانات لخاصة بالمشروع أن لزم الامر .
- توظيف تقنيات مراقبة جودة الخدمات (على سبيل المثال لا الحصر: Dynatrace، hotjar ، أو أنظمة إدارة التطبيقات ...) والتي تساعد على معرفة مواطن الخلل من ناحية أداء المنصة او أي مشاكل التقنية .
- استخراج تقارير عن مراقبة جودة الخدمات بشكل دوري بحيث توضح استقراريه المشروع و عدد المستخدمين و غيرها من البيانات في مجال مراقيه جودة الخدمات ..
- تقارير اختبار التكامل والربط: تنفيذ اختبارات التكامل للمشروع و تأكد من أدائها و على شركة تحمل تكلفة جميع الأدوات المستخدمة ...
- معايير ضمان جودة الخدمات

✓ على الموردين الالتزام بمعايير الجودة التي حددها قسم جودة الحلول:

- معدل الأخطاء العالية والحرجة 0 %.
- معدل الأخطاء المتوسطة أقل من 3 %.
- معدل الأخطاء المنخفضة أقل من 5%.
- نسبة جودة المشروع أكثر من 95 % ((معدل الأخطاء مفتوحة / مجموع الأخطاء) * 100)

✓ على المورد تقديم تقرير للاختبارات الربط API and Webservice إن وجدت بحيث معدل الأخطاء 0%.

✓ خدمة الكترونية خالية من الأخطاء واكتمال الخدمة بشكل كامل عند التقديم

✓ خلو النظام من رسائل خطأ 404

✓ خلو النظام من رسائل خطأ 500

✓ خلو النظام من رسائل خطأ 505

- تقارير اختبارات قابلية تحمل النظام:

✓ تجرى غالبا لفهم سلوك النظام في حالة زيادة المستخدمين ومدى استقرار النظام والعمل تحت العبء والضغط

✓ تقرير يفيد بأن النظام لن يستجيب عند الوصول رقم محدد

✓ يجب ان يدعم النظام على الأقل 100,000 طلب متزامن ويمكن للنظام التعامل معها

✓ يجب إعداد سيناريوهات لكل خاصيه يتم تطبيقها على النظام

- ✓ يجب إعداد وتصميم سيناريوهات بحيث ينبغي أن يشمل كل سلوك النظام وكذلك إجراءات متعددة تعمل معا السلوك تزامنا (مثال: اجراء نسخ احتياطيه لقاعده البيانات تزامنا مع تصفح المستخدمين للنظام)
- ✓ التخطيط لسيناريوهات الضغط على وظيفة معينة بصوره متكررة (عدد المستخدمين المتوقع لتنفيذ السيناريو وهم على الأقل 50000) او حسب متطلبات المشروع
- ✓ تنفيذ سيناريوهات اختبار الضغط (تكثف صعودا وهبوطا) ويتم مراقبه ورصد سلوك النظام في نفس الوقت
- ✓ يجب على المورد تضمين التقارير التالية:
  - كم عدد المستخدمين المتزامنين القادرين على التعامل مع النظام لكل سيناريو؟
  - كم عدد المستخدمين المتزامنين يمكن التعامل مع إجراءات متعددة في النظام؟
  - كيف يتصرف النظام في نقطة الانهيار (اختبار الضغط) ؟
  - هل لدى النظام القدرة على التعافي بشكل صحيح من المشاكل المتصلة بالضغط؟