الهيئة العامة لعقارات الدولة
STATE PROPERTIES GENERAL AUTHORITY

الشروط الخاصة

1- على مقدم الخدمة زيارة الموقع الرئيسي للهيئة والتأكد من الاحتياجات المطلوبة والاستفسار عن أي معلومات من شأنها تحسين العرض المقدم والتأكد من فاعلية الأنظمة وتحقيقها للاحتياج، بالأضافة الى توقيع محضر زيارة الموقع وارفاقه مع العرض الفني.

2- يجب على مقدم الخدمة إعداد خطة عمل شاملة وتفصيلية للمشروع يتم اعتمادها من قبل إدارة المشروع وتشمل ما يلي:

a. خطة عمل وإدارة المشروع
b. الخطة الزمنية للمشروع.
c. خطة تواصل واضحة للمشروع.
d. خطة إدارة مخاطر المشروع.

3- يجب ان يلتزم مقدم الخدمة بتقديم الدعم حسب اتفاقية مستوى الخدمة لجميع وحدات النظام.

4- يجب ان يلتزم مقدم الخدمة بتقديم أفضل الحلول والمقترحات لتنفيذ المتطلبات الجديدة على جميع وحدات النظام.

5- يجب ان يلتزم مقدم الخدمة بجمع وتحليل المتطلبات من الإدارات ذات العلاقة وتوثيقها واخذ الموافقة عليها قبل تنفيذها.

6- يجب على مقدم الخدمة اختبار النظام والتأكد من عدم وجود أي مشاكل فنية كل شهر

7- يجب على مقدم الخدمة تقديم خطة لنقل المعرفة للمستخدمين ومسؤولين الدعم.

8- يلتزم مقدم الخدمة بتعين مدير مشروع خلال (10- 15) يوم من تاريخ توقيع العقد، ويكون مؤهل ولدية شهادة PMP ولديه خبرة في إدارة مشاريع Scrum Master، ويفضل أن يكون سعودي الجنسية وخبرة عملية لا تقل عن 10 سنوات في نفس المجال.

9- للهيئة الحق في استبعاد الموارد البشرية التي لا تحقق الشروط المطلوبة أو التي يثبت عدم الحاجة لها ويتحمل مقدم الخدمة التكاليف المترتبة على ذلك.

10- تعتبر هذه الكراسة هي الأساس التي يتم الاستناد إلية لحسم أي خلافات فنية وتعتبر جزءاً لا يتجزأ من شروط التعاقد مع عدم الإخلال بأي شروط ترد في مستندات أخرى.

11- يجب على المتقدم قراءة كراسة الشروط والمواصفات وفهمها جيداً حيث إن المعلومات المطلوبة وجميع الشروط التي تتضمنها الكراسة وكذلك الالتزامات والبنود التي يتفق عليها في حالة ترسية العملية وتوقيع العقد تعتبر جزءاً لا يتجزأ من العقد.

12- أي وثيقة تقدم بعد ترسية العطاء يجب أن تكون مراجعة لغوياً وتسلم بصيغة رقمية وورقية.

13- أي أعمال تسلم للهيئة تصبح ملكيتها للهيئة ولا يحق لمقدم العرض التصرف أو استخدامها إلا بأذن مسبق ومكتوب من الهيئة.

إدارة المشتريات

14- تعيين مدير مشروع مؤهل طوال فترة تنفيذ المشروع يجيد المنهجية المتبعة في إدارة المشاريع ويكون مدير المشروع هو نقطة التواصل الرسمية بما يخص تنفيذ المشروع.

15- على مقدم الخدمة توضيح مهام ومسؤوليات مدير المشروع ومستوى المساندة من قبل الهيئة خلال فترة المشروع.

16- على مدير المشروع القيام بمهامه وواجباته للتأكد من تطبيق وتنفيذ جميع بنود العقد، علماً بأنه سيكون مسئولاً مسؤولية كاملة عن مراقبة ومتابعة وتنسيق جميع الأعمال والأمور الإدارية والمالية والفنية وغيرها التي سيتم تنفيذها ضمن المشروع.

17- لا يحق للجهة المنفذة استبدال مدير المشروع دون أخذ الموافقة المسبقة من الهيئة بعد توضيح المبررات المؤيدة لقرار الاستبدال.

18- يلتزم مقدم الخدمة بنقل الخبرة إلى الفريق الموجود بالهيئة.

19- يلتزم مقدم الخدمة بعمل التوثيقات الخاصة بمراحل المشروع.

20- يجب أن يراعى أي متطلب تطلبه الهيئة العامة لعقارات الدولة خلال مدة التعاقد ومتعلق بنطاق عمل المشروع.

21- إتاحة أدوات للتقييم والفحص لتمكن فريق العمل من القيام بعملية الفحص بطريقة واضحة وسلسة.

22- للهيئة الحق في طلب إعادة الفحص لأي سبب تراه، حتى لو تم استلامه.

23- للهيئة الحق في اختيار واختبار أعضاء الفريق أو طلب تغييرهم.

24- يجب أن يكون فريق تنفيذ المشروع متفرغ تماماً للعمل في مشروع الهيئة ولا يكون مرتبط بأي من مزاولة أي أعمال أخرى تخل بسير عمل المشروع.

25- الالتزام بتوفير جميع الموارد بحالتها الأصلية وضمان جودتها.

26- يجب أن تكون جميع مخرجات المشروع متاحة باللغتين العربية والإنجليزية.

27- يلتزم مقدم الخدمة بإعداد منهجية لتنفيذ المشروع مع مراعاة خصوصية بيئة العمل.

28- يلتزم مقدم الخدمة بالتوثيق الورقي والإلكتروني لجميع أعمال المشروع.

29- يلتزم مقدم الخدمة بتطبيق المعايير المعتمدة في تسليم واستلام مخرجات المشروع والتي سيتم تحديدها من قبل الهيئة عند اعداد خطة العمل.

30- انتقال واستلام الأعمال والمهام:

i- يلتزم المتعاقد – عند ترسية المنافسة عليه – باستلام جميع الأعمال والمهام والمسؤوليات المتعلقة بالنظام الإلكتروني محل العقد من المورد/المشغل الحالي، وذلك خلال مدة أقصاها ثلاثون (30) يومًا من تاريخ توقيع العقد أو من تاريخ تسلمه إشعار المباشرة، أيهما أسبق.

ii- يشمل الاستلام – على سبيل المثال لا الحصر – ما يلي:

- الشفرة المصدرية (Source Code) وجميع مكونات النظام البرمجية.
- قواعد البيانات بكامل بياناتها ونسخها الاحتياطية.
- بيانات الدخول والصلاحيات للخوادم وبيئات التشغيل والاستضافة.
- وثائق التحليل والتصميم الفني والمعماري وأدلة الاستخدام والتشغيل.
- التراخيص البرمجية، شهادات الأمان، النطاقات، وأي ارتباطات بطرف ثالث.
- خطط وإجراءات النسخ الاحتياطي والتعافي من الكوارث.
- أي أصول تقنية أو معلومات أو التزامات تعاقدية مرتبطة بتشغيل المنصة.

iii- يلتزم المتعاقد بالتنسيق الكامل مع المشغل الحالي والهيئة العامة لعقارات الدولة لضمان انتقال الأعمال بصورة سلسة ودون انقطاع في الخدمة، ويتحمل مسؤولية التحقق من سلامة وكفاية ما يتم استلامه خلال مدة الانتقال.

iv- توثق عملية الاستلام بمحضر استلام وانتقال موقع من الأطراف ذات العلاقة، وتنتقل بموجبه المسؤولية التشغيلية والفنية الكاملة إلى المتعاقد. وفي حال عدم إتمام الاستلام خلال المدة المحددة، دون سبب تقبله الهيئة العامة لعقارات الدولة، يحق للهيئة تطبيق ما تراه مناسبًا من إجراءات وفقًا لأحكام العقد والنظام.

v- لا يترتب على عدم تعاون المشغل الحالي – إن وجد – إعفاء المتعاقد من التزاماته التعاقدية، ويجب عليه إشعار الهيئة بأي معوقات فور حدوثها.

31- يلتزم مقدم الخدمة بإعداد نموذج حوكمة للمشروع قبل بداية العمل.

32- يلتزم مقدم الخدمة بإجراء تقييم لمخاطر الأمن السيبراني، والتأكد من أن المخاطر ستكون تحت السيطرة قبل توقيع العقود والاتفاقيات أو عند تغيير المتطلبات التشريعية والتنظيمية ذات الصلة.

33- يجب توفير وتطوير إجراءات الاتصال في حالة وقوع حادث للأمن السيبراني.

34- يجب ان يكون مقدم الخدمة في المملكة العربية السعودية وأن يتم تقديم الخدمة منه وليس من خارج المملكة.

35- يجب على مقدم الخدمة استيفاء الشروط التالية عند قيامه بتنفيذ المشروع:

i. يجب أن يكون لمقدم الخدمة خبرة سابقة في تطبيق مشاريع مشابهه مع إرفاق ما يثبت ذلك وستأخذ الهيئة هذا من ضمن نقاط التقييم لاختيار مقدم الخدمة.

36- يجب على مقدم الخدمة توثيق جميع الزيارات ومحاضر الاجتماعات وتسليمها الى فريق عمل الهيئة.

37- يلتزم بتوفير فريق العمل الكافي والمؤهل لإنجاح كافة أعمال المشروع، على أن تتوفر فيهم المؤهلات المناسبة لطبيعة العمل. وللهيئة الحق بمقابلة أعضاء فريق العمل وطلب تغيير من لا تثبت جدارته وأهليته للقيام بالدور المنوط به في المشروع وعلى مقدم الخدمة إيجاد البديل ضمن الوقت المتفق عليه مع الهيئة.

38- يلتزم مقدم الخدمة بتوافق الخدمة مع الضوابط الأساسية والتشريعية للهيئة الوطنية للأمن السيبراني.

39- يلتزم مقدم الخدمة بإرفاق نموذج التصعيد حسب الهيكل التنظيمي لدى مقدم الخدمة حتى الرئيس التنفيذي لشركة.

40- الالتزام بوجود وثيقة اتفاقية مستوى الخدمة Service Level Agreement (SLA) تحدد فيها نسبة توفر الخدمة وسرعة التجاوب مع البلاغات.

41- في حال انقطاع الخدمة لأي سبب كان، يجب على مزود الخدمة ارسال تقرير يوضح فيه السبب الرئيسي RCA Report خلال 24 ساعة من عودة الخدمة.

42- وجود فريق دعم فني يتحدث اللغتين (عربي – انجليزي) داخل المملكة على مدار الساعة.

43- على المتنافس المتقدم للمشروع تقديم عرض فني شامل ومتكامل يتضمن التصاميم ومميزات الحلول الفنية، ومنهجية العمل لجميع مراحل المشروع .

44- يجب أن تكون جميع التراخيص الموردة ضمن المشروع مشمولة بضمان الشركة الصانعة حسب مدة العقد ويجب أن تكون اتفاقية الدعم من الشركة المصنعة مع دعم وعمل التحديثات والترقيات اللازمة خلال فترة المشروع.

45- سوف تعمل الهيئة العامة لعقارات الدولة على تخصيص بعض الموظفين المناسبين للمشاركة في أعمال تنفيذ هذا المشروع بغية نقل المعرفة بشكل عملي. وفي هذه الحالة، على مقدم الخدمة أن يتأكد من إشراك موظفي الهيئة في جميع المراحل المتعلقة بتنفيذ المشروع، ويوفر لهم جميع البيانات والمعلومات الفنية اللازمة لحصولهم على الخبرة الكافية في الأنظمة المقدمة في المشروع.

46- يجب على الشركة المتقدمة أن تكون شركة سعودية متخصصة وسعودية المنشأ وان يكون لديها مقر دائم داخل المملكة العربية السعودية مع وجود مهندسين وفنيين مقيمين داخل المملكة العربية السعودية.

47- عدة جهات حكومية تم تنفيذها خلال الثلاث سنوات الماضية.

48- يلتزم مقدم الخدمة بتوفير السير الذاتية من ذوي الخبرات لفريق العمل المرشح لتنفيذ المشروع.

49- يلتزم مقدم الخدمة بتطبيق متطلبات وسياسات الأمن السيبراني للهيئة العامة لعقارات الدولة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

50- يجب أن يتم إجراء المسح الأمني (Screening or Vetting) لشركات خدمات الإسناد، ولموظفي خدمات الإسناد، والخدمات المدارة العاملين على الأنظمة الحساسة .

51- خدمات الاسناد والتشغيل لهذا المشروع يجب ان تكون عن طريق شركات وجهات وطنية وفقا للمتطلبات والتنظيمات التشريعية ذات العلاقة.

52- يجب تضمين مسؤوليات الامن السيبراني وبنود المحافظة على سرية المعلومات في عقود موظفي الأطراف الخارجية لتشمل خلال وبعد انتهاء/ انهاء العلاقة الوظيفية مع الهيئة بالإضافة الى الحذف المن من قِبل الطرف الخارجي لبيانات الجهة عند انتهاء الخدمة

53- يجب الالتزام بمتطلبات الامن السيبراني للتغيير كالتالي:

i. يلتزم مقدم الخدمة بتتبع عملية التغيير الرسمية والمناسبة وفقا لسياسات وإجراءات الهيئة العامة لعقارات الدولة وبما يتوافق مع متطلبات الأمن السيبراني
ii. يجب مراجعة واختبار التغيير التي أجريت على الأصول المعلوماتية والتقنية الخاصة بالهيئة قبل تطبيقها على بيئة الإنتاج.

54- متطلبات حماية البيانات والمعلومات:

i. يجب عدم نقل بيانات ومعلومات خاصة بالهيئة خارج البيئة الإنتاجية
ii. يجب عدم معالجة أو تخزين أو استخدام بيانات ومعلومات الهيئة العامة لعقارات الدولة الموجودة في الأنظمة الجيومكانية في بيئة الاختبار الا بعد أخذ موافقة داخلية من إدارة الامن السيبراني

55- يلتزم مقدم الخدمة بإبلاغ إدارة الامن السيبراني عن أي حوادث أمن سيبراني يتعرض لها مقدم الخدمة والتي من شأنها أن توثر على الأصول التقنية والمعلوماتية للهيئة

56- يلتزم مقدم الخدمة وموظفيه بالتعاون مع أنشطة مراجعة سجل الاحداث والتدقيق التي تقوم بها الهيئة العامة لعقارات الدولة

57- يلتزم مقدم الخدمة بتصنيف البيانات والمعلومات وفقا لسياسة تصنيف البيانات والمعلومات الصادرة من مكتب إدارة البيانات الوطنية.

58- يلتزم مقدم الخدمة او مزود الخدمة بربط الأصول التقنية بالحلول السيبرانية على سبيل المثال لا الحصر مركز عمليات الامن السيبراني.

59- الالتزام بما ورد في قواعد وإجراءات المستودعات الحكومية بالمادة (38)وما يطرأ عليها من تعديل من الجهات ذات الاختصاص .

60- يلتزم مقدم الخدمة بحذف بيانات الهيئة العامة لعقارات الدولة (مقيد و سري و سري للغاية) من على أجهزة و خوادم مقدم الخدمة عند انتهاء العلاقة التعاقدية

61- يلتزم مقدم الخدمة بتوافق الخدمة مع كافة الضوابط الصادرة من الهيئة الوطنية للأمن السيبراني و مكتب إدارة البينات الوطنية.

62- توفر خطة لتعافي من الكوارث التقنية وفق معاير الأمانة العامة لمجلس المخاطر الوطني وهيئة الحكومة الرقمية واختبارها ومشاركتها مع إدارة استمرارية الاعمال لضمان وجود خطة عند تعطل النظام.

63- توفر خطط لاستمرارية الاعمال وفق معاير الأمانة العامة لمجلس المخاطر الوطني وهيئة الحكومة الرقمية واختبارها ومشاركتها مع إدارة استمرارية الاعمال لضمان وجود خطة عند تعطل النظام.

64- في حال لم يتم الالتزام باتفاقية مستوى الخدمة سيتم تطبيق الغرامة حسب جدول الغرامات الذي سيتم اعتماده في بداية المشروع.

65- يجب على المقاول تقديم شهادة تصنيف فني للمقاولين معتمده (قطاع الاتصالات وتقنية المعلومات).

66- يفضل أن يكون مقدم الخدمة مؤهل من قبل ايزو 27001 في أمن المعلومات

67- يلتزم المتعاقد بالتقييد بمقتضى الأمر السامي رقم 45462 وتاريخ 1440/8/13هـ

68- يلتزم مقدم الخدمة بتطبيق دليل توطين مهن الاتصالات وتقنية المعلومات والصادر بموجب قرار معالي وزير الموارد البشرية والتنمية الاجتماعية رقم 28889 وتاريخ 1440/05/03هـ.

69- يلتزم مقدم الخدمة بالتقيد بدليل توطين عقود التشغيل والصيانة بالجهات العامة والصادر بموجب قرار معالي وزير الموارد البشرية والتنمية الاجتماعية رقم 73483 وتاريخ 1444/04/30هـ.

70- يلتزم المتعاقد بإعداد وتطبيق خطة استمرارية أعمال شاملة ومحدثة تتوافق مع السياسة المعتمدة لدى الهيئة العامة لعقارات الدولة، وتغطي جميع الأنشطة والخدمات محل التعاقد، بما في ذلك آليات استعادة الأنظمة والبيانات وضمان استمرارية تقديم الخدمات في حالات الطوارئ أو الانقطاع.

71- كما يلتزم المتعاقد بتقديم الخطة للهيئة العامة لعقارات الدولة لاعتمادها قبل بدء التنفيذ، ومراجعتها وتحديثها بشكل دوري أو عند حدوث أي تغيير جوهري في العمليات أو المخاطر. ويُعد عدم الالتزام بأحكام هذا البند إخلالاً جوهرياً يترتب عليه تطبيق الجزاءات النظامية والعقدية ذات الصلة.

72- التزامات المورد:

- يجب على المورد القيام بتقييم شامل للأنظمة الحالية وقواعد البيانات وهيكلية النظام الخاصة بمنصة «انتفاع»، مع تقديم تقرير تفصيلي يتضمن الوضع الحالي، التحديات، والتوصيات الفنية للتحسين.
- يجب على المورد توفير وتطبيق منصة متكاملة لمراقبة وإدارة أعمال التطوير والتشغيل (DevOps)، بما يشمل إدارة الإصدارات، تتبع المهام، التكامل المستمر (CI) والتسليم المستمر (CD)، بالإضافة إلى أدوات المراقبة وقياس الأداء.
- يلتزم المورد بالامتثال التام لكود المنصات الموحد الخاص بمنصة انتفاع، وكافة المعايير والمتطلبات الفنية والتنظيمية ذات العلاقة، بما في ذلك أي تحديثات أو تعديلات تطرأ على كود المنصات الموحد مستقبلاً، ويلتزم بتطبيقها فور صدورها دون أي تكاليف إضافية على الجهة. كما يلتزم بتوفير أداة (منير) وكافة الأدوات والتجهيزات المرتبطة بها، بما يضمن التكامل والتوافق مع متطلبات المنصة وتشغيلها بكفاءة.

1. يلتزم مقدم الخدمة بتوافق الخدمة مع كافة الضوابط الصادرة من الهيئة الوطنية للأمن السيبراني ومكتب إدارة البينات الوطنية.
2. يلتزم مقدم الخدمة بتطبيق متطلبات وسياسات الأمن السيبراني للهيئة العامة لعقارات الدولة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
3. يجب أن يكون مقدم الخدمة في المملكة العربية السعودية وأن يتم تقديم الخدمة منها وليس من خارج المملكة.
4. يجب أن يكون موقع واستضافة وتخزين معلومات الهيئة داخل المملكة العربية السعودية مع مراعاة التنظيمات والجوانب التشريعية بعدم خضوع تلك البيانات لاي قوانين دول أخرى.
5. يجب توفير وتطوير إجراءات الاتصال في حالة وقوع حادث للأمن السيبراني و ابلاغ إدارة الامن السيبراني عن أي حوادث أمن سيبراني يتعرض لها المقاول خلال مده أقصاها 24 ساعة.
6. يلتزم مقدم الخدمة بإجراء تقييم لمخاطر الأمن السيبراني، والتأكد من أن المخاطر ستكون تحت السيطرة قبل توقيع العقود والاتفاقيات أو عند تغيير المتطلبات التشريعية والتنظيمية ذات الصلة.
7. يلتزم مقدم الخدمة وموظفيه بالتعاون مع أنشطة مراجعة سجل الاحداث والتدقيق والاختبارات الأمنية التي تقوم بها الهيئة العامة لعقارات الدولة.
8. يجب أن يتم إجراء المسح الأمني (Screening or Vetting) لشركات خدمات الإسناد، ولموظفي خدمات الإسناد، والخدمات المدارة العاملين على الأنظمة الحساسة.
9. يجب تضمين مسؤوليات الامن السيبراني وبنود المحافظة على سرية المعلومات في عقود موظفي الأطراف الخارجية لتشمل خلال وبعد انتهاء/ انهاء العلاقة الوظيفية مع الهيئة بالإضافة الى الحذف من قِبل الطرف الخارجي لبيانات الجهة عند انتهاء الخدمة.
10. يلتزم مقدم الخدمة بتصنيف البيانات والمعلومات وفقا لسياسة تصنيف البيانات والمعلومات الصادرة من مكتب إدارة البيانات الوطنية.
11. الالتزام بوجود وثيقة اتفاقية مستوى الخدمة Service Level Agreement (SLA) تحدد فيها نسبة توفر الخدمة وسرعة التجاوب مع البلاغات.
12. يلتزم مقدم الخدمة بإرفاق نموذج التصعيد حسب الهيكل التنظيمي لدى مقدم الخدمة حتى الرئيس التنفيذي لشركة.
13. يجب الالتزام بمتطلبات الامن السيبراني للتغيير كالتالي:

    يلتزم مقدم الخدمة بتتبع عملية التغيير الرسمية والمناسبة وفقا لسياسات وإجراءات الهيئة العامة لعقارات الدولة وبما يتوافق مع متطلبات الأمن السيبراني

    يجب مراجعة واختبار التغيير التي أجريت على الأصول المعلوماتية والتقنية الخاصة بالهيئة قبل تطبيقها على بيئة الإنتاج.
14. متطلبات حماية البيانات والمعلومات:

يجب عدم نقل بيانات ومعلومات خاصة بالهيئة خارج البيئة الإنتاجية

يجب عدم معالجة أو تخزين أو استخدام بيانات ومعلومات الهيئة العامة لعقارات الدولة الموجودة في بيئة الاختبار الا بعد أخذ موافقة داخلية من الادارة العامة لحوكمة البيانات والأمن السيبراني.

15. يلتزم مقدم الخدمة بإعادة البيانات بصيغة قابلة للاستخدام وحذفها بشكل غير قابل للاسترجاع عند انهاء/ انتهاء الخدمة.
16. يلتزم مقدم الخدمة بالتأكد من ضمان خصوصية البيانات المستضافة في الحوسبة السحابية.
17. تطوير مخطط معماري للاتصالات يوضح الطبقات الثلاث للتطبيق/الحل/النظام (العرض – التطبيق – قاعدة البيانات)، متضمناً جميع التكاملات والاتصالات الخارجية والمنافذ.
18. تطوير الشيفرة المصدرية يجب أن يتوافق مع أفضل الممارسات الأمنية.
19. يجب أن تكون جميع الحلول والأنظمة المقدمة مطوَّرة باستخدام منصات أو لغات برمجة آمنة من نوع No-Code / Low-Code، مع الالتزام الكامل بأفضل الممارسات والمعايير المعتمدة للأمن السيبراني وحماية البيانات.
20. يجب تشفير البيانات أثناء النقل وأثناء التخزين وربط قواعد البيانات مع حل إدارة مفاتيح التشفير (KMS).
21. يجب أن تتوافق خوارزميات وبروتوكولات التشفير مع المعايير الوطنية للتشفير (NCS-1:2020) الصادرة من الهيئة الوطنية للأمن السيبراني (NCA).
22. إعداد خطة تراجع (Exit Plan) تشمل استراتيجية النسخ الاحتياطي، على أن تتم الموافقة عليها مسبقاً.
23. جميع الحسابات/الصلاحيات ذات الامتيازات يجب إدارتها عبر حل إدارة الوصول المتميز (PAM).
24. يجب أن يستخدم النظام طرق مصادقة آمنة مثل LDAPs.
25. يجب أن يكون النظام متوافقاً ومتكاملاً مع أداة إدارة أصول تقنية المعلومات (IT Asset Management Tool).
26. يجب تكوين النظام بحيث تكون هناك بيئات منفصلة لكل من الإنتاج، ما قبل الإنتاج، الاختبار، التطوير، وبيئة التعافي من الكوارث (DR).
27. يجب أن يتوفر للنظام مستند توثيق كامل (As Built Documentation)ومصفوفة RACI.
28. يجب اعتماد منهجية ال DevSecOps في تخطيط وتصميم وتطوير ونشر التطبيقات.
29. استخدام بيانات النظام يجب أن يكون مقصوراً على بيئة الإنتاج، أما في بيئات التطوير، الاختبار، وما قبل الإنتاج فيجب تطبيق ضوابط صارمة مثل: إخفاء أو تشويش البيانات.
30. يلتزم مقدم الخدمة بتمكين الربط مع الدليل النشط (Active Directory) لضمان إدارة مركزية للهويات والمستخدمين والتحقق من الهوية وفق ضوابط الهيئة.
31. يلتزم مقدم الخدمة بدعم تسجيل الدخول الموحد (Single Sign-On – SSO) وفق المعايير المعتمدة (مثل SAML2.0 أو OAuth2.0 أو OpenID Connect).
32. يجب أن يوفر مقدم الخدمة مصفوفة صلاحيات (Role Matrix) واضحة تشمل الأدوار، المهام، الصلاحيات، وآلية التحكم في الوصول وفق مبادئ أقل صلاحية وفصل المهام.
33. يجب على مقدم الخدمة دعم الأمان متعدد العوامل (Multi-Factor Authentication – MFA) لجميع الحسابات، وخصوصاً الحسابات ذات الصلاحيات الحساسة.

34. يلتزم مقدم الخدمة بتوفير إجراءات واضحة وموثقة لمنح الصلاحيات تشمل الطلب، الاعتماد، المراجعة، وتحديد مالك الصلاحية، بما يتوافق مع سياسات إدارة الهويات والصلاحيات.
35. يجب على مقدم الخدمة توفير نظام Sandbox في حال الحاجة ليعمل بتوافق مع النظام ويلبي متطلبات الامن السيبراني.
36. تفعيل التسجيل (Logging) بشكل كامل وربطه مع نظام إدارة الأحداث والمعلومات الأمنية (SIEM).
37. ربط قواعد البيانات مع نظام مراقبة نشاط قواعد البيانات (Database Activity Monitoring - DAM).
38. تنفيذ المراجعات والاختبارات (Hardening , Configuration Review , VA , PT) تكون على بيئة الإنتاج قبل الإصدار.
39. صلاحيات الوصول يجب أن تكون قائمة على RBAC.
40. يجب توفير شهادات الوثوق والأمان (SSL) لجميع متطلبات المشروع.
41. يجب توفير نسخة احتياطية لجميع أنظمة التشغيل والتطبيقات حسب سياسات النسخ الاحتياطي الخاص بالهيئة.
42. يلتزم مقدم الخدمة بتوقيع اتفاقية عدم افشاء المعلومات مع الهيئة (NDA).
43. يلتزم مقدم الخدمة او مزود الخدمة بربط الأصول التقنية بالحلول السيبرانية على سبيل المثال لا الحصر مركز عمليات الامن السيبراني.
44. يلتزم مقدم الخدمة او مزود الخدمة بعمل الاختبارات الأمنية والتي تشمل (اختبار الاختراق – اختبار تقييم الثغرات – تقييم مخاطر الامن السيبراني قبل اطلاق الخدمة) عن طريق طرف ثالث مستقل عن مزود الخدمة.
45. الالتزام بنظام حماية البيانات الشخصية وذلك بتطبيق جميع المتطلبات على سبيل المثال:
    a. تجهيز اشعار/سياسة الخصوصية للنظام مع توضيح حالات الاستخدام للبيانات الشخصية.
    b. توثيق سجلات معالجة البيانات الشخصية للنظام بالتفصيل.
    c. توثيق قبول المستخدمين الجدد والحاليين لإشعار الخصوصية للنظام، وإتاحة تغيير قبول اشعار الخصوصية.
    d. إتاحة الوصول إلى حالات قبول إشعار الخصوصية للنظام لمكتب البيانات من خلال جدول بيانات ولوحة بيانات.