العرض الفني والمالي لتطوير سياسات إدارة البيانات

الإصدار 1.0

التاريخ: 24-أغسطس-2025

الموافق: 1-ربيع الأول-1447

معلومات التواصل

للاستفسار حول هذا المستند والمعلومات الواردة، بإمكانكم التواصل مع الأشخاص الوارد ذكرهم في الجدول أدناه:

الاسم	**هاشم العزيزي**
رقم الهاتف	**+966-53-122-1580**
البريد إلكتروني	**Hashem.azizi@trustedvision.biz**
العنوان	**حي قرطبة، شارع سعيد بن زيد،** **مبنى مجموعة إنجاز، رقم 6482، الدور الأول،** **صندوق البريد: 13247،الرياض، المملكة العربية السعودية.**

جدول المحتويات

1. ملخص تنفيذي لمتطلبات العميل

يسر شركة الرؤيا الموثوقة تقديم خدمات مُدارة في الأمن السيبراني وإدارة البيانات للهيئة

يغطي نطاق عمل الخدمات المُدارة المهام التالية الموضحة في الجدول أدناه:

الخدمة المُدارة الأولى	خدمات الحوكمة والمخاطر والالتزام بالأمن السيبراني وتشمل
1	تطوير سياسات وإجراءات ومعايير الأمن السيبراني.
2	تطوير ومراجعة وتحديث نماذج وسجل إدارة مخاطر الأمن السيبراني.
3	تقييم مخاطر الأمن السيبراني بناء على الأصول التقنية (Asset-based).
4	تقييم مخاطر الأمن السيبراني بناء على الأحداث / إدارات الهيئة (Event-based/Function-based).
5	تقييم التدقيق الداخلي للالتزام بمعايير الآيزو 27001:2022 على مستوى إدارة الأمن السيبراني بالمقر الرئيسي للهيئة والإعداد للحصول على الاعتماد لشهادة الآيزو.
6	خدمات مدارة لتقييم حالة الالتزام بسياسات الأمن السيبراني الداخلية المعتمدة بالهيئة.
7	تطوير عمليات الحوكمة والمخاطر والالتزام باستخدام أدوات معتمدة.
8	الخدمات المدارة للتقارير التنفيذية الدورية المطلوبة لإدارة الأمن السيبراني.
9	الخدمات المدارة لتقييم الوضع الراهن للتوعية والتدريب بالأمن السيبراني
10	تطوير برنامج توعوي وتدريبي بالأمن السيبراني

11	الخدمات المدارة لإجراءات وتقييمات دورية لمخاطر أمن البيانات وتطوير واتخاذ الإجراءات التصحيحية بناءً على نتائج التقييم.
12	تقارير مستوى الامتثال لضوابط حماية البيانات.
الخدمة المُدارة الثانية	خدمات الحوكمة والمخاطر والالتزام بالأمن السيبراني وتشمل
1	تطبيق نظام ولائحة حماية البيانات الشخصية (PDPL) وتشمل:
2	تنفيذ خطة حماية البيانات الشخصية.
3	تنفيذ عمليات المراجعة والتطوير لسياسات وإجراءات الخصوصية، إجراءات
4	التعامل مع حوادث تسريب البيانات، إجراءات إدارة الموافقات.
5	خدمات متابعة حالة الامتثال لنظام حماية البيانات الشخصية.
الخدمة المُدارة الثالثة	حوكمة البيانات (DG) وتشمل
1	متابعة أداء تنفيذ الخطة والاستراتيجية بناءً على مؤشرات أداء محددة وتطوير تقارير دورية بها.
2	خدمات مراجعة وتحديث مؤشرات الأداء لقياس نجاح إدارة البيانات بما يتوافق مع المؤشر الوطني للبيانات (نضيء).
3	تشغيل أنشطة حوكمة وإدارة البيانات.
الخدمة المُدارة الرابعة	تطبيق مجال تصنيف البيانات وتشمل
1	تنفيذ خطة تصنيف البيانات.
2	تنفيذ عمليات جرد وتصنيف البيانات والسجلات مع ضمان وجود آلية مراجعة وتحسين مستمر..

3	خدمات مدارة لتصنيف البيانات
4	تنفيذ خطة تصنيف البيانات.

نعتقد أن خبرتنا في تنفيذ مشاريع مماثلة تضعنا بين نخبة الشركات الاستشارية بالإضافة إلى:

1. مزيج متوازن من الخبرات الدولية والمحلية في إدارة البيانات والأمن السيبراني
2. نهج فعال لتنفيذ المشروع لتلبية متطلبات المشروع في الوقت المناسب وبطريقة مهنية وجودة
3. معرفة وخبرة واسعة في تنفيذ وتصميم الحلول بناءً على المعايير الدولية وأفضل الممارسات.
4. أفضل الخبرات الاستشارية في إدارة وحوكمة البيانات

نأمل أن تحقق خدماتنا الاستشارية بنود المنافسة ونتطلع إلى علاقة عمل متبادلة.

2. منهجية تنفيذ المشروع

تهدف هذه المنهجية إلى استعراض كيفية تقديم الخدمات المُدارة في مجالي الأمن السيبراني والبيانات ، بما يضمن الامتثال الكامل للضوابط والمعايير الوطنية والعالمية ذات الصلة، وعلى رأسها:

- نظام حماية البيانات الشخصية(PDPL)
- ضوابط إطار حوكمة البيانات NDMO Framework
- مؤشر البيانات الوطنية (نُضيء)
- ضوابط الأمن السيبراني للبيانات – NCA-DCC-1:2022
- معيار الآيزو ISO/IEC 27001

تم تصميم المنهجية لتُنفذ على مدى 12شهرًا، وفقًا لهيكل مرحلي يضمن تحقيق:

- تقييم للوضع الراهن
- تطوير السياسات والإجراءات والنماذج،
- تشغيل الأدوات التقنية وتفعيل التصنيف،
- رفع جاهزية الفرق من خلال التوعية والتدريب،
- تحقيق الامتثال الكامل لمتطلبات مؤشر نُضئ للوصول للهيئة لمرحلة التفعيل.

تراعي المنهجية خصوصية البيئة التشغيلية للجهة، وتعتمد على نهج تشاركي بين فريق الاستشاري وفِرق العمل داخل الجهة، مع التركيز على بناء قدرات داخلية وضمان الاستدامة بعد انتهاء فترة التشغيل

ملاحظة: يعتمد نجاح الخدمة المُدارة المُقدمة من شركة الرؤيا الموثوقة على الأدوات والحلول التقنية المتعلقة بتصنيف البيانات والتي يجب على الهيئة اقتناؤها.

فيما يلي وصف تفصيلي للأنشطة الرئيسية والمخرجات المتوقعة:

الرقم	الأنشطة التي يجب أن تقوم بها شركة الرؤيا الموثوقة	الأنشطة التي يجب أن تقوم بها الجهة	الأنشطة المنجزة والمخرجات
.1	تنفيذ دراسة تحليلية شاملة للوضع الراهن للأمن السيبراني وحوكمة البيانات وتصنيفها بحيث تشتمل على مراجعة السياسات والإجراءات، تقييم البنية التحتية الحالية، حصر الأصول التقنية، وجرد أولي للبيانات.	توفير نسخ محدثة من السياسات والإجراءات المعتمدة، ترتيب اجتماعات مع الفرق الفنية والإدارية، تسهيل الوصول إلى قواعد البيانات والبنية التحتية.	تقرير تقييم الوضع الراهن، تحليل فجوات مفصل مقابل ISO 27001 و NCAو PDPL وNDMO، قائمة أولية بالبيانات الحرجة والأصول التقنية.
.2	إجراء تقييم أولي لمدى الامتثال لمؤشر نُضج البيانات (نُضيء) وضوابط حماية البيانات الشخصية، وتحليل الفجوات الفنية والتنظيمية.	تقديم تقارير الأداء السابقة، تحديد ممثلين من إدارة البيانات لدعم التقييم.	تقرير جاهزية مؤشر نُضيء، تحديد درجة النضج، توصيات لسد الفجوات.
.3	تحديث سياسات وإجراءات وعمليات وأطر الأمن السيبراني والبيانات بما يتماشى مع متطلبات الهيئة الوطنية للأمن السيبراني والهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)	مراجعة السياسات المقترحة واعتمادها، التنسيق مع الشؤون القانونية.	• سياسات وإجراءات وعمليات وأطر محدثة بالأمن السيبراني • سياسات وإجراءات وعمليات وأطر محدثة بالبيانات
.4	إعداد نماذج وسجلات الأمن السيبراني والبيانات مثل: سجل المخاطر السيبرانية، سجل التصنيف، ونماذج مشاركة البيانات.	مراجعة النماذج وتحديد المسؤولين عنها.	نماذج وسجلات الأمن السيبراني والبيانات مثل: سجل المخاطر السيبرانية، سجل التصنيف، ونماذج مشاركة البيانات.
.5	متابعة تنفيذ السياسات والإجراءات وعمليات الأمن السيبراني والبيانات	تنسيق الاجتماعات مع أصحاب المصلحة (إدارات وأقسام الهيئة) عند الحاجة	تقرير دوري بنتائج حالة الالتزام بكافة السياسات والإجراءات والعمليات المتعلقة بالأمن السيبراني والبيانات (داش بورد)
.6	إجراء تقييمات مخاطر أمن سيبراني على:	تنسيق الاجتماعات مع أصحاب المصلحة	تقارير إدارة مخاطر الأمن السيبراني

الرقم	الأنشطة التي يجب أن تقوم بها شركة الرؤيا الموثوقة	الأنشطة التي يجب أن تقوم بها الجهة	الأنشطة المنجزة والمخرجات
	• مستوى الأصول أو التقييمات خلال العمليات اليومية والإجراءات التشغيلية المعتادة، عند اللزوم. • استثناءات الالتزام واستثناءات السياسات والمخالفات ضد تطبيق ضوابط الأمن السيبراني التي يتسبب بها العاملون، عند اللزوم. • أنظمة العمل عن بعد، مرة واحدة سنوياً، على الأقل. • عند التخطيط وقبل السماح بالعمل عن بعد لأي خدمة أو نظام. • لحسابات التواصل الاجتماعي، مرة واحدة سنوياً، على الأقل. • قبل وأثناء استخدام حسابات التواصل الاجتماعي عالية الحساسية، كل ستة أشهر. • عند إنشاء أو استخدام حسابات للتواصل الاجتماعي، عند اللزوم. • عند ربط الشبكات اللاسلكية بشبكات "الجهة"، عند اللزوم. • عند إعطاء صلاحية وصول أو ربط الأجهزة المحمولة للأنظمة الحساسة أو للأنظمة التي تعد أنظمة وطنية حرجة، عند اللزوم. • عند تطوير خدمات أو تطبيقات تقنية جديدة أو خدمات للعمل عن بعد، عند اللزوم.		

الرقم	الأنشطة التي يجب أن تقوم بها شركة الرؤيا الموثوقة	الأنشطة التي يجب أن تقوم بها الجهة	الأنشطة المنجزة والمخرجات
	• عند إجراء تغييرات جوهرية على الخدمات والتطبيقات والأصول المعلوماتية الحالية، عند اللزوم. • عند الحاجة لتخزين أو استخدام بيانات مصنفة وغير عامة في بيئات تقنية غير بيئة الإنتاج مثل بيئات الاختبار والتجارب والتطوير، عند اللزوم. • عند الحاجة لوصول مطوري الأنظمة ومدراء قواعد البيانات لبيئات الإنتاج، أو عند الحاجة لوصولهم لبيانات بيئة الإنتاج، عند اللزوم. • عند التعاقد مع الأطراف الخارجية مثل مزودي الخدمات التقنية المدارة، أو مزودي خدمات توفير الكوادر البشرية، أو شركات الخدمات الاستشارية، عند اللزوم. • عند الحاجة لتغيير تقني في بيئات الحوسبة السحابية أو إنشاء اشتراكات جديدة عليها، عند اللزوم. • عند تطوير أنظمة حساسة أو التغيير عليها، عند اللزوم. • في مرحلة جمع المعلومات في جميع المشاريع التقنية، عند اللزوم..		
7.	إصدار تقارير شهرية بمستوى الامتثال لضوابط حماية البيانات.	مراجعة واعتماد التقارير	تقارير شهرية بمستوى الامتثال لضوابط حماية البيانات.
8.	تقديم الدعم في تطبيق نظام ولائحة حماية البيانات الشخصية (PDPL) وتشمل:	مراجعة واعتماد • خطة حماية البيانات الشخصية.	• خطة حماية البيانات الشخصية.

الرقم	الأنشطة التي يجب أن تقوم بها شركة الرؤيا الموثوقة	الأنشطة التي يجب أن تقوم بها الجهة	الأنشطة المنجزة والمخرجات
	• خطة حماية البيانات الشخصية. • تنفيذ عمليات المراجعة والتطوير لسياسات وإجراءات الخصوصية، إجراءات • التعامل مع حوادث تسريب البيانات، إجراءات إدارة الموافقات. • تنفيذ خطة حماية البيانات الشخصية. • تنفيذ عمليات المراجعة والتطوير لسياسات وإجراءات الخصوصية • إجراءات التعامل مع حوادث تسريب البيانات. • إجراءات إدارة الموافقات. • متابعة حالة الامتثال لنظام حماية البيانات الشخصية.	• تنفيذ عمليات المراجعة والتطوير لسياسات وإجراءات الخصوصية، إجراءات • التعامل مع حوادث تسريب البيانات، إجراءات إدارة الموافقات. • تنفيذ خطة حماية البيانات الشخصية. • تنفيذ عمليات المراجعة والتطوير لسياسات وإجراءات الخصوصية • إجراءات التعامل مع حوادث تسريب البيانات. • إجراءات إدارة الموافقات. • متابعة حالة الامتثال لنظام حماية البيانات الشخصية.	• تنفيذ عمليات المراجعة والتطوير لسياسات وإجراءات الخصوصية، إجراءات • التعامل مع حوادث تسريب البيانات، إجراءات إدارة الموافقات. • تنفيذ خطة حماية البيانات الشخصية. • تنفيذ عمليات المراجعة والتطوير لسياسات وإجراءات الخصوصية • إجراءات التعامل مع حوادث تسريب البيانات. • إجراءات إدارة الموافقات. • متابعة حالة الامتثال لنظام حماية البيانات الشخصية.
.9	تنفيذ خطة تصنيف البيانات الشاملة تشمل: جرد البيانات، التصنيف الفعلي، آلية المراجعة المستمرة.	تعيين مسؤولين عن التصنيف في الإدارات، دعم التنفيذ الميداني.	خارطة تصنيف، بيانات مصنفة، تقرير تغطية التصنيف المؤسسي.
.10	تفعيل أدوات مشاركة البيانات داخليًا وخارجيًا بشكل آمن ومؤتمت وفق السياسات.	تحديد الجهات المشاركة وتقديم قائمة الأدوات الحالية.	نموذج مشاركة مؤتمت، سجل الجهات المشاركة، تقارير الاستخدام.
.11	مراجعة وتحديث مؤشرات الأداء لقياس نجاح إدارة البيانات بما يتوافق مع المؤشر الوطني للبيانات (نضيء).	مراجعة مؤشرات قياس الأداء	مؤشرات قياس الأداء مُحدّثة

الرقم	الأنشطة التي يجب أن تقوم بها شركة الرؤيا الموثوقة	الأنشطة التي يجب أن تقوم بها الجهة	الأنشطة المنجزة والمخرجات
.12	تنفيذ مراجعات التزام دورية لسياسات الأمن السيبراني والتصنيف والخصوصية.	تسهيل مراجعة السجلات وتوفير بيانات الأداء.	تقارير امتثال، تحديثات سياسات، توصيات تصحيحية.
.13	إجراء تدقيق داخلي على معيار الآيزو 27001:2022 على مستوى إدارة الأمن السيبراني	تنسيق الاجتماعات والتزويد بكافة الوثائق المطلوبة ذات الصلة بمعيار الآيزو 27001:2022	تقرير التدقيق الداخلي والخطة التصحيحية
.14	إجراء تقييم حالة الالتزام بسياسات الأمن السيبراني الداخلية المعتمدة بالهيئة	تنسيق الاجتماعات والتزويد بكافة الوثائق المطلوبة ذات الصلة بمعايير الهيئة الوطنية للأمن السيبراني	تقرير حالة الالتزام بسياسات الأمن السيبراني
.15	تصميم وتنفيذ برنامج توعوي وتدريبي بالأمن السيبراني والبيانات	تحديد الفئات المستهدفة وتنسيق الجداول مع الموارد البشرية.	توعوي وتدريبي بالأمن السيبراني والبيانات
.16	متابعة أداء تنفيذ الخطة والاستراتيجية بناءً على مؤشرات أداء محددة وتطوير تقارير دورية.	مراجعة أداء تنفيذ الخطة والاستراتيجية	تقارير متابعة أداء تنفيذ الخطة والاستراتيجية
.17	إعداد أدلة تشغيل ودليل استخدام للأنظمة والسياسات والأدوات التقنية.	مراجعة واعتماد الأدلة وتعميمها داخليًا.	دليل تشغيل السياسات، دليل استخدام أدوات التصنيف والمشاركة.
.18	تفعيل مؤشرات الأداء الخاصة بمؤشر نُضج وربطها بلوحات التقارير الدورية.	اعتماد مؤشرات الأداء، وتفعيلها ضمن أنظمة التقارير.	لوحات أداء ديناميكية، تقارير شهرية وربع سنوية، دعم اتخاذ القرار.
.19	قياس الأثر المؤسسي الناتج عن تنفيذ التصنيف والحوكمة.	تقديم ملاحظات المستخدمين والإدارات حول التغيير والتحسن.	تقرير قياس الأثر، دراسة حالة، توصيات للتحسين.

الرقم	الأنشطة التي يجب أن تقوم بها شركة الرؤيا الموثوقة	الأنشطة التي يجب أن تقوم بها الجهة	الأنشطة المنجزة والمخرجات
.20	إعداد التقرير النهائي للامتثال الكامل لمؤشر نُضج مدعومًا بالأدلة.	مراجعة التقرير واعتماده وتقديمه للجهات الرقابية.	تقرير امتثال نهائي شامل، مرفقات الإثبات، وثائق دعم القرار.
.21	تقديم خطة التحسين المستمر والمجالات المستقبلية للتطوير المؤسسي.	مراجعة التوصيات، مناقشتها مع الشركاء الداخليين.	وثيقة خطة التحسين، جدول متابعة، خارطة طريق مستقبلية.
.22	تسليم المشروع رسميًا بجميع مخرجاته ومستنداته التشغيلية والتدريبية.	التحقق من جاهزية فرق العمل الداخلية للاستلام والتشغيل.	مستندات التسليم، النسخ النهائية من الأدلة، خطة الاستدامة الداخلية.

3. مدة ومكان تنفيذ الخدمات

- تكون مدة تقديم الخدمات المُدارة اثنا عشر شهرا (12) تحسب بالتقويم الميلادي وتبدأ من تاريخ محضر بدء الاعمال.
- سيتم تنفيذ الخدمات المذكورة في مقرات للهيئة.

4. نموذج التصعيد

مستوى الأولوية	زمن الاستجابة	زمن الحل	التصعيد الأول	زمن التصعيد	التصعيد النهائي	زمن التصعيد النهائي
P1-حرج	30دقيقة	60دقيقة	مدير المشروع	بعد 30 دقيقة من عدم الحل	المدير التنفيذي	بعد 60 دقيقة إضافية
P2-عالي	60دقيقة	60دقيقة	مدير المشروع	بعد 60 دقيقة من عدم الحل	المدير التنفيذي	بعد 60 دقيقة إضافية
P3-متوسط	ساعتين	12ساعة	مدير المشروع	بعد 4 ساعات	المدير التنفيذي	بعد 8 ساعات
P4-منخفض	4ساعات	24ساعة	مدير المشروع	بعد 6 ساعات	المدير التنفيذي	بعد 18 ساعة

5. تقرير سير عمل المشروع الأسبوعي

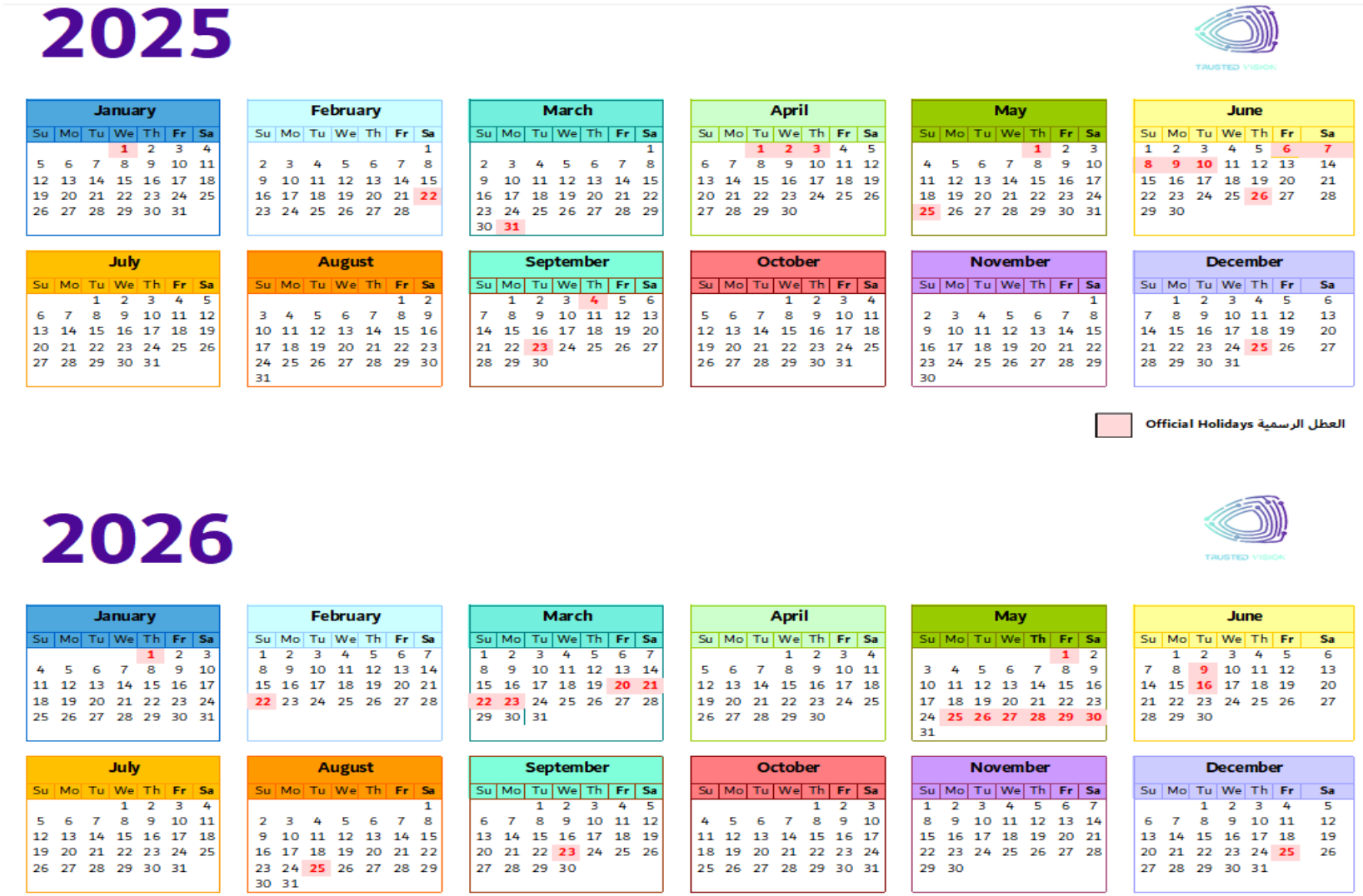
يوضح الجدول أدناه تقدم المشروع بشكل أسبوعي لضمان تحقيق الأهداف وفقًا للجدول الزمني المخطط. يتم تقسيم التقرير إلى أربعة محاور رئيسية:

1. منجزات الأسبوع الحالي: تشمل جميع الأنشطة والمهام المكتملة خلال الأسبوع.
2. منجزات الأسبوع القادم: تحديد المهام والأنشطة المخطط تنفيذها لضمان الاستمرارية.
3. التحديات: استعراض العقبات التي قد تؤثر على سير العمل، مع تحديد الجوانب التي تحتاج إلى حلول.
4. التوصيات: تقديم اقتراحات لتحسين الأداء، وتقليل التحديات المحتملة، وضمان كفاءة العمليات.

اسم المشروع مدير المشروع (من طرفكم)		مدير المشروع (الرؤيا الموثوقة)
منجزات الأسبوع الحالي	1	
منجزات الأسبوع القادم	1	
التحديات	1	
التوصيات	1	

6. تقويم الشركة

يوضح التقويم أدناه أيام الدوام والإجازات لموظفي شركة الرؤيا الموثوقة



7. نقل المعرفة

يتضمن نقل المعرفة، نقل المعارف من الاستشاري الى منسوبي الجهة والتدريب بهدف القيام بالأعمال التي كان يقوم بها الاستشاريون وتمكين موظفي الهيئة من القدرة على القيام بكافة أعمال الاستشاريون بثقة وتمكن.

سيتم نقل المعرفة لمنسوبي الجهة عن طريق الجدول التالي:

ماذا (المحتوى)	متى	من (الإدارة المستهدفة)	كيف (قنوات التواصل)
نقل المعرفة لفريق الأمن السيبراني جميع الوثائق والخطط المتعلقة بالمشروع 1. مشاركة وتوزيع الوثائق والسياسات 2. تبادل المعلومات حول التهديدات والهجمات والتقنيات الجديدة 3. بث المعلومات عبر منصات تبادل المعلومات 4. تطبيق أفضل الممارسات.	بشكل يومي خلال جميع مراجل المشروع	1. محاضرات ودورات وورش عمل تدريبية 2. تقارير تهديدات	1. الاجتماعات المرئية 2. الاجتماعات الحضورية

8. إدارة المشروع

خلال فترة المشروع، سيقوم الاستشاريون بتقديم مستندات إدارة المشروع الأساسية. تتضمن هذه المستندات ما يلي:

- الجداول ومحاضر اجتماعات
- خطة إدارة المخاطر
- سجل المخاطر/المشكلات
- تقارير حالة
- استراتيجية وخطة الاتصال
- استراتيجية وخطة المشاركة
- مقاييس المشروع

من المتوقع أن تقوم الجهة بإكمال الأنشطة الإدارية للمشروع التي يقدمها الاستشاريون على الدوام

9. نطاق المشروع والافتراضات

9.1 خارج نطاق العمل

- تنفيذ أو شراء أدوات وحلول التقنية المتعلقة بإدارة البيانات
- أي خدمة أخرى لم يتم ذكرها بوضوح في الأقسام السابقة سيتم اعتبارها خارج نطاق العمل.

9.2 افتراضات

1. سيتم تنفيذ العمل بشكل هجين (عن بعد وفي مقر الجهة) بما يضمن رضى الجهة عن آلية العمل.
2. لن يتم تقديم أي حلول تقنية خلال فترة تنفيذ المشروع.
3. لن يكون للشركة أي علاقة أو مسؤولية في حال تم شراء أي تقنية بعد انتهاء مدة تنفيذ المشروع.
4. جميع الوثائق (السياسات، والإجراءات، ونماذج البيانات، والخطط، إلخ) ستُسلَّم باللغة العربية وبضوابط الإصدار.
5. **جميع الأنشطة ستتم خلال فترة المشروع فقط وليس للشركة أي علاقة إن كان هنالك أي تأخير أو عدم تعاون من الجهة**
6. **الشركة غير مسؤولة عن أي تأخير يحدث من طرف الجهة**
7. التعاون من اقسام وإدارات الجهة إلزامي لنجاح المشروع
8. ستكون مسؤولية مجال أمن البيانات (المجال رقم 15 في ضوابط ومواصفات حوكمة البيانات وحماية البيانات الشخصية) من مسؤولية إدارة الأمن السيبراني وسيعمل الاستشاريون مع قسم الأمن السيبراني في الجهة على تطبيق الضوابط
9. يتضمن العرض المراجعة مرة واحدة فقط للوثائق المسلمة.
10. يحق للشركة إيقاف المشروع بشكل مؤقت في حال عدم تسديد الدفعة خلال أسبوعين من تاريخ إصدار الفاتورة وإرسالها للجهة

10. خطط الموارد والجودة والتوصل

يقوم مدير المشروع في مرحلة التخطيط بعمل مجموعة من الخطط من أجل تنفيذ المشروع على أفضل وجه ومنها خطة للموارد وخطة للجودة وخطة للتواصل كما يلي:

1. في خطة الموارد يتم حصر الموارد المتوفرة وتحديد المتطلبات ولا أولويات وتوزيع الموارد حسب الأولويات.
2. في خطة الجودة يتم تحديد معايير الجودة من أجل تطبيقها في المشروع مثل طرق سير العمل والوقت اللازم لمراجعة الوثائق وآليات مراجعة الوثائق واعتمادها.
3. في خطة التواصل يتم تحديد أفضل طرق للتواصل حسب احتياجات أصحاب المصلحة ويتم تدوين الخطة ولعمل بها

تعد الخطط المذكورة جزء مهم في إدارة المشاريع، والهدف منها تحديد كيفية تجهيز الموارد وإدارة الجودة وكيفية التواصل خلال حياة المشروع. حيث تشمل كل أدوار أصحاب المصلحة.

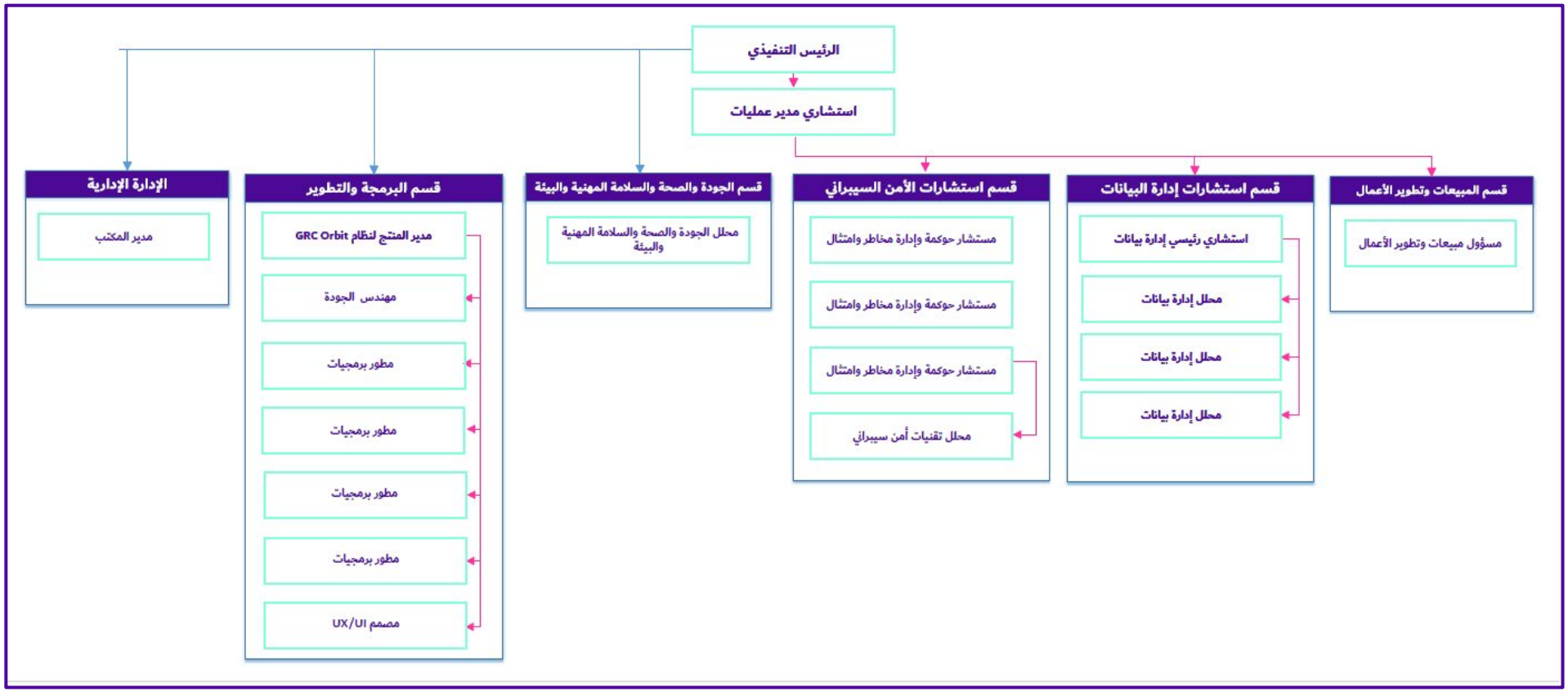
11. المخاطر عالية المستوى

تم تحديد أهم المخاطر عالية المستوى في المشروع كما في الجدول أدناه

رقم الخطر	سيناريو الخطر	المستوى الإجمالي	ضوابط التعامل مع الخطر
1	عدم تعاون منسوبي الجهة وبالتالي حصول تأخير في التسليات	عالي	1- تخصيص مدير للمشروع من الجهة وتفريغه للعمل مع الاستشاريين 2- إعطاء رسالة وأمر من صاحب الصلاحية لجميع الإدارات بضرورة التعاون مع الاستشاريين لضمان إتمام المشروع خلال الوقت المحدد
2	عدم رضى الجهة عن الوثائق المسلّمة	متوسط	تطوير خطة جودة وتفعيلها بين الشركة وبين الجهة
3	استقالة أحد الاستشاريين خلال عمل المشروع	منخفض	توفير استشاريين آخرين للاحتياط من قبل الشركة

12. معلومات عن الشركة

شركة الرؤيا الموثوقة هي شركة استشارية تعمل في مجال إدارة البيانات والأمن السيبراني وتقدم خدمات كاملة في مجال إدارة الحوكمة والمخاطر والامتثال، بالإضافة إلى حلول وتدريبات، لمساعدة الجهات على تلبية متطلبات أعمالهم. ما يميزنا هو القيم الجوهرية التي نتبناها.



الشكل (3) الهيكل التنظيمي

13. الشهادات

يحمل فريقنا مجموعة متنوعة من الشهادات، بما في ذلك ما يلي:


PECB
ISO 9001
LEAD AUDITOR


ITIL
FOUNDATION


CompTIA
CCAP
Cloud Admin
PROFESSIONAL

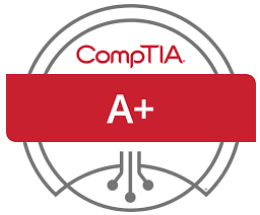

CompTIA
CSCP
Secure Cloud
PROFESSIONAL


CompTIA
Data+


CompTIA
Cloud+


CompTIA
CySA+


CompTIA
Network+


CompTIA
A+


CompTIA
Security+


CNSS


FORTINET
NSE
1
ASSOCIATE


FORTINET
NSE
2
ASSOCIATE


FORTINET
NSE
3
ASSOCIATE


ASSOCIATE
CERTIFIED


C|EH
Certified Ethical Hacker


paloalto
PCCSA


paloalto
PCNSA


paloalto
PCNSE


CISA
CYBER+INFRASTRUCTURE

14. المشاريع السابقة التي تم تنفيذها

تم تنفيذ العديد من المشاريع من خلال التعامل مع جهات متنوعة في دول مختلفة وبيئات متعددة ونسعى دائمًا إلى تنفيذ أفضل الممارسات والمعايير من أجل تحقيق أفضل النتائج المطلوبة

رقم المشروع	اسم المشروع	اسم العميل أو الجهات المستفيدة	الشعار	وصف المشروع
.1	تنفيذ معيار ISO 27001 وضوابط الأمن السيبراني الأساسية (ECC,CCC,DCC,OSMACC,TCC)	شركة التصنيع وخدمات الطاقة (طاقة)	TAQA	• إنشاء نظام إدارة الأمن السيبراني • تطوير استراتيجية الأمن السيبراني والنموذج التشغيلي • تطوير السياسات والإجراءات والمعايير ذات الصلة • ضمان الامتثال لأطر الهيئة الوطنية للأمن السيبراني ECC, CCC, DCC, OSMACC, TCC • ضمان الامتثال لمعيارISO 27001 • إجراء التدقيق الداخلي على أطر الهيئة الوطنية للأمن السيبراني ومعيار الآيزو 27001 • الحصول على شهادة الأيزو 27001

.2	التدقيق والإشراف على تنفيذ الضوابط الأساسية للأمن السيبراني NCA-ECC	جهة حكومية سيادية		• التحسين على وثائق الحوكمة (استراتيجية الأمن السيبراني، الأدوار والمسؤوليات بالأمن السيبراني، سياسات الأمن السيبراني) • التدقيق على الضوابط الأساسية للأمن السيبراني NCA-ECC
.3	تدقيق أنظمة تقنية المعلومات	شركة ليبارا اتصالات	LEBARA ليبارا موبايل	• تدقيق السياسات والإجراءات المتعلقة بتقنية المعلومات (الضوابط التقنية العامة + الضوابط التقنية على التطبيقات)
.4	تدريب معيار أمن المعلومات ISO 27001	شركة التصنيع وخدمات الطاقة (طاقة)	TAQA	• تقديم التدريب في معيار أمن المعلومات ISO 27001
.5	استراتيجية إدارة وحوكمة البيانات	مكتبة الملك عبد العزيز العامة		• إجراء تحليل الفجوات المتعلق بإطار عمل الضوابط الوطنية لإدارة وحوكمة البيانات • دراسة الوضع الراهن • تطوير استراتيجية إدارة البيانات • تطوير خطة البيانات المفتوحة

				• نشر ست مجموعات من البيانات المفتوحة على المنصة السعودية للبيانات الوطنية
.6	تنفيذ معيار أمن المعلومات ISO 27001	Genelle		• إنشاء نظام إدارة أمن المعلومات • تطوير السياسات والإجراءات والمعايير ذات الصلة • ضمان الامتثال لمعيارISO 27001 • إجراء أنشطة التصحيح وحل الاستنتاجات • الحصول على شهادة الأيزو 27001
.7	تنفيذ ضوابط أرامكو للأمن السيبراني Saudi Aramco Cybersecurity Implementation	Maham		• تنفيذ معيار أرامكو للأمن السيبراني SACS-002 • تطوير السياسات والإجراءات والمعايير ذات الصلة
.8	تصنيف البيانات Data Classification	Perfect Presentation		• حصر وتصنيف جميع البيانات • تطوير السياسات والإجراءات والمعايير المتعلقة بتصنيف وحماية البيانات

.9	تنفيذ معيار أمن المعلومات ISO 27001 وضوابط الأمن السيبراني الأساسية (ECC,CCC,DCC,OSMACC,TCC)	البرنامج الوطنية للتنمية المجتمعية (تنمية)	تنمية البرنامج الوطني للتنمية المجتمعية في المناطق	• إنشاء نظام إدارة الأمن السيبراني • تطوير استراتيجية الأمن السيبراني والنموذج التشغيلي • تطوير السياسات والإجراءات والمعايير ذات الصلة • ضمان الامتثال لأطر الهيئة الوطنية للأمن السيبراني ECC, CCC, DCC, TCC OSMACC, • ضمان الامتثال لمعيارISO 27001 • إجراء التدقيق الداخلي على أطر الهيئة الوطنية للأمن السيبراني ومعيار الآيزو 27001 • الحصول على شهادة الأيزو 27001
.10	إدارة مخاطر الأمن السيبراني	جهة حكومية سيادية		• تطوير منهجية إدارة مخاطر الأمن السيبراني وموائمتها مع المنهجية العامة لإدارة المخاطر • إجراء تقييم مخاطر الأمن السيبراني على الأصول المعلوماتية + الأطراف الثالثة + التغييرات الجوهرية + المشاريع التقنية + العمليات

.11	NCA-ECC and CCC-P	Nashirnet		• إنشاء نظام إدارة الأمن السيبراني • تطوير السياسات والإجراءات والمعايير الخاصة بضوابط الحوسبة السحابية وبالضوابط الأساسية ECC + CCC لمزودي الخدمة • إجراء تقييمات لمخاطر الأمن السيبراني على المشاريع والمنتجات • إجراء التدقيق الداخلي • تطوير وقياس مؤشرات قياس الأداء
.12	تصنيف ونمذجة البيانات	مكتبة الملك عبد العزيز العامة		• تطوير سجل البيانات • تصنيف البيانات • تطوير خطة نمذجة البيانات والقيام بالنمذجة لأنظمة المكتبة
.13	تنفيذ نظام ولائحة حماية البيانات الشخصية PDPL	Aljaber Finance		• حصر البيانات الشخصية وأنشطة المعالجة • تطوير السياسات والمعايير والإجراءات ذات الصلة بخصوصية البيانات • تطوير عمليات إدارة الموافقات • إجراء التدقيق على عمليات أنشطة معالجة البيانات

				• تنفيذ ورشات توعوية في حماية البيانات الشخصية
.14	تنفيذ نظام ولائحة حماية البيانات الشخصية PDPL	Hala Payment	HALA	• حصر البيانات الشخصية وأنشطة المعالجة • تطوير السياسات والمعايير والإجراءات ذات الصلة بخصوصية البيانات • تطوير عمليات إدارة الموافقات • إجراء التدقيق على عمليات أنشطة معالجة البيانات • تنفيذ ورشات توعوية في حماية البيانات الشخصية

ملاحظة

15. السير الذاتية

#	الاسم	المنصب الوظيفي	المستوى الدراسي	سنوات الخبرة	الخبرات
1	ه. ع	مدير المشروع	بكالوريوس هندسة الحاسوب	12 سنوات	• خبرة أكثر من 10 سنوات في إدارة المشاريع. • خبرة في قيادة وتنفيذ مشاريع البيانات وحوكمة البيانات. • خبرة في التعامل مع الجهات الحكومية والمؤسسات الكبيرة. • قدرة على التنسيق بين الفرق التقنية والإدارية. • الإلمام الكامل بمنهجيات إدارة المشاريع مثل PMP أو Scrum. • خبرة في إدارة التغيير والاتصال المؤسسي.
2	ب. ع	خبير حوكمة بيانات وبيانات شخصية	بكالوريوس علوم البيانات والذكاء الاصطناعي	3 سنة	• خبرة في مجالات حوكمة البيانات وحماية البيانات الشخصية. • خبرة في تطبيق السياسات والإجراءات المرتبطة بإدارة البيانات. • معرفة بأنظمة ولوائح حماية البيانات مثل GDPR أو NDMO. • خبرة في تقييم النضج المؤسسي للبيانات وتحليل الفجوات. • القدرة على العمل مع اللجان وتقديم التوصيات الاستشارية.
3	آ ع	استشاري إدارة بيانات	بكالوريوس علوم الحاسوب	7 سنوات	• خبرة تتجاوز 7 سنوات تنفيذ مشاريع حوكمة البيانات • تطوير سياسات وإجراءات إدارة البيانات وتصنيفها وحمايتها بما يتوافق مع أفضل الممارسات العالمية. • القدرة على استخدام أدوات مثل Power BI أو Tableau. • خبرة في تحليل متطلبات العمل وتحويلها إلى مؤشرات أداء.

					• تطوير نماذج البيانات الداعمة لاتخاذ القرار. • تطوير مؤشرات الأداء الرئيسية (KPIs) لمتابعة فعالية إدارة البيانات وربطها بالأهداف الاستراتيجية. • تدريب المستخدمين على أدوات ذكاء الأعمال.
4	ح ب	استشاري إدارة بيانات	بكالوريوس هندسة الحاسوب	3 سنوات	• تنفيذ مشاريع حوكمة البيانات وفق إطار عمل NDMO ومؤشر نُضج البيانات (نُضِئ). • تصميم وتشغيل نماذج إدارة البيانات: تصنيف البيانات، جودة البيانات، إدارة التعريفات، ومشاركة البيانات. • إدارة عمليات تقييم الفجوات وتحليل الوضع الراهن لأنظمة البيانات والحوكمة. • الإشراف على تنفيذ خطط تصنيف البيانات على مستوى المنصات والأنظمة والمستندات. • بناء قدرات الجهات من خلال تصميم وتنفيذ برامج تدريبية مخصصة حول إدارة البيانات. • العمل مع فرق متعددة التخصصات لتفعيل أدوار حوكمة البيانات (مالك بيانات، أمين بيانات، مستخدم). • إعداد تقارير الأداء والمراجعة الدورية الخاصة بحوكمة البيانات والامتثال التنظيمي.
5	ع ع	محلل تقنيات امن سيبراني	بكالوريوس في نظم المعلومات الحاسوبية	2 سنة	• تحليل وتصميم بنية أمنية متكاملة تشمل الشبكات، الأنظمة، التطبيقات، وأمن البيانات.

					• تنفيذ تقييمات الثغرات (Vulnerability Assessment) واختبارات الاختراق.(Penetration Testing) • تصميم سياسات وضوابط الأمن السيبراني وفقًا لأطر مثلNIST ، ISO 27001، وNCA CCC. • إعداد وتطوير نماذج تقييم مخاطر الأمن السيبراني.(Cyber Risk Models)
6	ب ا	استشاري الحوكمة وإدارة المخاطر والامتثال	ماجستير في هندسة الاتصالات	20 سنه	• تصميم وتطوير أطر حوكمة مؤسسية تتماشى مع أفضل الممارسات مثل COBITوISO 38500. • إجراء تقييمات شاملة للمخاطر المؤسسية (ERM) ووضع خطط المعالجة والتحكم. • تطوير سياسات وإجراءات حوكمة وإدارة مخاطر تتماشى مع الأنظمة التنظيمية المحلية والدولية. • إعداد مصفوفات الامتثال وضوابط الرقابة الداخلية وفقًا لمتطلبات الجهات الرقابية. • تنفيذ برامج الامتثال للأنظمة الوطنية مثل نظام حماية البيانات الشخصية (PDPL)وضوابط الهيئة الوطنية للأمن السيبراني.(NCA) • تقييم الفجوات التنظيمية والتشغيلية وتقديم توصيات التحسين. • تفعيل مؤشرات أداء الحوكمة والمخاطر والامتثال وربطها بالتقارير التنفيذية.
7	غ ح	استشاري حوكمة وإدارة مخاطر	بكالوريوس هندسة الحاسوب	4سنوات	• خبره في تطوير سياسات وإجراءات حوكمة وإدارة مخاطر تتماشى مع الأنظمة التنظيمية المحلية والدولية.

					• إعداد مصفوفات الامتثال وضوابط الرقابة الداخلية وفقًا لمتطلبات الجهات الرقابية. • تنفيذ برامج الامتثال للأنظمة الوطنية مثل نظام حماية البيانات الشخصية (PDPL)وضوابط الهيئة الوطنية للأمن السيبراني.(NCA) • تقييم الفجوات التنظيمية والتشغيلية وتقديم توصيات التحسين.