المملكة العربية السعودية
وزارة البيئة والمياه والزراعة
الإدارة العامة للأمن السيبراني
إدارة مخاطر الأمن السيبراني

م	جميع مشاريع وزارة البيئة والمياه والزراعة
1.	يجب توقيع الطرف الخارجي وممثليه (أفراداً وكيانات) على وثيقة عدم الإفصاح ويكون أثرها مستمر حتى بعد انتهاء العلاقة بالوزارة ، وتتضمن الحذف والإتلاف الآمن بحيث لا يمكن استرجاعها من وسائطها المخزنة فيها أياً كانت.
2.	يلتزم الطرف الخارجي وممثليه (أفراداً وكيانات) بتطبيق متطلبات وارشادات وسياسات الأمن السيبراني المعتمدة في وزارة البيئة والمياه والزراعة والمتطلبات التشريعية والتنظيمية ذات العلاقة وما يستجد منها.
3.	توفير الطرف الخارجي وثيقة المسح الأمني للأفراد التابعين له في الوظائف التقنية ذات الصلاحيات الهامة والحساسة.
4.	يلتزم الطرف الخارجي مباشرة بعد إنهاء ، انتهاء علاقة أي فرد تابع له مع الوزارة بالعمل بإجراءات مراجعة وإلغاء الصلاحيات على الأصول المعلوماتية والتقنية ،وبإجراء كافة متطلبات إخلاء الطرف بالتنسيق مع الجهات ذات العلاقة بالوزارة.
5.	يلتزم الطرف الخارجي بالإفصاح عن أي مخاطر أو حادثة آمن سيبراني لديه وإبلاغ الوزارة عبر الهاتف (0112038888 ، تحويلة 4555) والبريد الإلكتروني (Soc@mewa.gov.sa).
6.	تضمين متطلبات الامن السيبراني ضمن العقود والاتفاقيات مع الطرف الخارجي مثل اتفاقية مستوى الخدمة (SLA)
	المشاريع التقنية بوزارة البيئة والمياه والزراعة
7.	توثيق وتوفير المعايير التقنية الأمنية الخاصة بالحلول المقدمة من قبل الشركة المنفذة حسب توجهات المُصنَع والمعايير الدولية ذات العلاقة وذلك بالتنسيق مع الإدارة العامة للأمن السيبراني بالوزارة.
8.	تطبيق الحلول وتجربتها بشكل كلي في بيئة مستقلة (بيئة التطوير ، بيئة الاختبار) قبل انطلاقها في البيئة الفعلية والتنسيق مع الجهات المعنية بذلك قبل الإطلاق.
9.	ضمان التكامل الآمن على كافة المستويات للحل المقدم وبحيث لايوجد أي تعارض ، على سبيل المثال لا الحصر : • فيما بين مكونات الحل المقدم. • مع أنظمة وزارة البيئة والمياه والزراعة. • مع الحلول الأمنية والبنية التحتية التقنية المطبقة في وزارة البيئة والمياه والزراعة.
10.	الإفصاح عن أي مخاطر أو ثغرات أمنية في الحلول والمنتجات المقدمة ومعالجتها.

11.	تقييم واكتشاف الثغرات ومعالجتها قبل الإطلاق والتنسيق بذلك مع الإدارة العامة للأمن السيبراني وأخذ الموافقة النهائية قبل الإطلاق.
12.	إجراء مراجعة الإعدادات والتحصين وحزم التحديثات والإصلاحات اللازمة قبل الإطلاق والتدشين والتنسيق بذلك مع الإدارة العامة للأمن السيبراني وأخذ الموافقة النهائية ، وعلى سبيل المثل لا الحصر ما يلي: • تقييم واكتشاف الثغرات ومعالجتها. • مراجعة الإعدادات والتأكد من توافقها مع المعايير (الإعدادات) التقنية الأمنية. • مراجعة منافذ وبروتوكولات وخدمات الشبكة والأجهزة والأنظمة التقنية للتأكد من سلامتها وإغلاق وإلغاء الغير مستخدم منها وذلك حسب ما يتوافق مع توجيهات المُصنَع. • مراجعة وتغيير الإعدادات الافتراضية من المصُنَع التي قد تؤثر على الأمن السيبراني للأصول المعلوماتية والتقنية. • مراجعة هويات الدخول والصلاحيات وتعطيل أو إلغاء الحسابات الغير مستخدمة منها ، ومنها الحسابات الافتراضية الغير ضرورية (default accounts). • مراجعة كلمات المرور والتأكد من عدم وجود كلمات مرور ثابتة أو افتراضية من المصُنَع (Hard-coded or Default passwoeds) • التأكد من أن كلمات المرور معقدة وذلك حسب سياسات الأمن السيبراني بالوزارة المعتمدة. • التأكد من عمل الاعدادات الخاصة بوضع حد معين لعدد محاولات الدخول الفاشلة المتتالية إلى الأنظمة (حسب سياسات الإدارة العامة للامن السيبراني بوزارة البيئة والمياه والزراعة). • التأكد من عمل الاعدادات الخاصة بانتهاء صلاحية كلمات المرور بعد الفترة المحددة في سياسات الامن السيبراني بالوزارة. • المراجعة للتأكد من التقييد الحازم ومنع استخدام وسائط التخزين الخارجية أو توصيل الأجهزة المحمولة بكافة أنواعها على جميع الشبكة سواءً الداخلية أو الشبكة الصناعية الخاصة بأنظمة التحكم الصناعي (OT/ICS). • مراجعة مزامنة التوقيت (Clock synchronization) مركزياً. • التأكد من شمولية عملية النسخ الاحتياطي لجميع الأصول المعلوماتية والتقنية لجميع الأنظمة الداخلية أو الأنظمة الصناعية (OT/ICS) والتي تستلزم ذلك. • اختبار استرجاع النسخ الاحتياطية والتأكد من القدرة على سرعة الاستعادة والتعافي . • التأكد من أن التوثيق بجميع أنواعه يعكس فعلياً ما تم عمله. • التأكد من تشفير النسخ الاحتياطية ووضعها في مكان آمن منفصل عن الموقع.

13.	الالتزام بما ورد في سياسة متطلبات الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية المعتمدة في وزارة البيئة والمياه والزراعة.
14.	الالتزام في مشاريع تطوير التطبيقات والبرمجيات الخاصة بما يلي: • استخدام معايير التطوير الآمن وذلك بالتنسيق مع الإدارة العامة للأمن السيبراني على سبيل المثال لا الحصر: ○ عدم اتاحة أي معلومات حساسة مثل كلمات المرور والمعرفات الداخلية ونحوه. ○ تخصيص صفحات الخطأ بحيث لا تظهر فيها التقنيات المستخدمة ويمكن حسب الاتفاق أن تكون صفحة خطأ موحدة. ○ في حسابات الخدمات يجب تطبيق ما يلي: ▪ استخدام حساب مختلف لكل خدمة. ▪ إزالة الصلاحيات الغير ضرورية. ▪ استخدام كلمات مرور مختلفة لكل حساب خدمة. ▪ استخدام كلمات مرور معقدة لحسابات الخدمات. ○ التأكد من أن مكونات التطبيق محدثة وإزالة أي صفحات أو تطبيقات عامة غير ضرورية وإزالة الحزم الغير مستخدمة. ○ تأمين طريقة مصادقة الـ(API) للخدمات العامة باستخدام بيانات اعتماد مستخدم بدلاً من استخدام بينات اعتماد عامة واحدة لطلبات الـ(API). ○ يجب استخدام حسابات الوصول المحدود (Limited access accounts) عند الاتصال بقواعد البيانات. ○ تنفيذ الـ(CAPTCHA) على جميع النماذج المقدمة المواجهة للأنترنت لمنع هجمات محاولات التخمين (Brute force). ○ تطبيق ميزة التحقق متعدد العناصر (MFA) على كافة صفحات تسجيل الدخول المواجهة للأنترنت. ○ تطبيق الجدران النارية لتطبيقات الويب (WAF). • أن تكون مصادر وأدوات تطوير التطبيقات والمكتبات الخاصة بها (Libraries) مرخصة وموثوقة وسليمة من الثغرات الأمنية وتم اعتمادها لدى الإدارة العامة للأمن السيبراني بوزارة البيئة والمياه والزراعة. • اجراء اختبار للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمنية السيبرانية وذلك بالتنسيق مع الإدارة العامة للأمن السيبراني. • التأكد من أمن التكامل بين التطبيقات وذلك بالتنسيق مع الإدارة العامة للأمن السيبراني.

الحوادث السيبرانية	
15.	يلتزم الطرف الخارجي بالإفصاح عن أي حادثة آمن سيبراني لديه وإبلاغ الإدارة العامة للأمن السيبراني بالوزارة عبر الهاتف (0112038888) ،تحويلة (4555) والبريد الإلكتروني (Soc@mewa.gov.sa).
16.	يجب على الطرف الخارجي التنسيق مع الإدارة العامة للأمن السيبراني بالوزارة بالاطلاع على سياسة إدارة الحوادث السيبرانية والمعتمدة من الإدارة.
17.	تضمين التوعية السيبرانية (دليل التعامل مع الحوادث السيبرانية) للطرف الخارجي وممثليه (أطرافاً وكيانات) والأفراد التابعين له في الوظائف التقنية ذات الصلاحيات الهامة والحساسة قبل البدء الفعلي للمهام وذلك بالتنسيق مع الإدارة العامة للأمن السيبراني بالوزارة ، وتشمل الحوادث السيبرانية على سبيل المثال لا الحصر ما يلي: • التغييرات غير المصرح بها في إعدادات أجهزة المستخدمين المكتبية و/أو المحمولة، والتغييرات في إعدادات الخوادم. • الإصابة بالبرمجيات الضارة. • التغييرات في التطبيقات من حيث المظهر (المظهر غير الاعتيادي) والتعديلات على صلاحيات المستخدم مثل رفع مستوى الوصول. • الوصول غير المصرح به إلى البيانات، و/أو تعديلها دون تصاريح أو صلاحيات المستخدمين • محاولات الحصول على معلومات يمكن استخدامها في تنفيذ الهجمات، مثل فحص منافذ الشبكة (Port Scans)، والهندسة الاجتماعية (Attacks Social Engineering)، وفحص مجال شبكة محددة (Targeted Scans Across IP Range)، وغيرها. • التفعيل غير المصرح به لحسابات مستخدمين موقوفة أو محذوفة.
18.	يلتزم الطرف الخارجي وممثليه (أطرافاً وكيانات) بعدم الإفصاح عن أي معلومات متعلقة بالحوادث الأمنية إلى أطراف خارجية.
19.	في حال تطلبت معالجة حادثة سيبرانية إجراء تغييرات على المكونات التقنية، يجب الالتزام بإجراءات إدارة التغيير المعتمدة والصادرة من الإدارة العامة للأمن السيبراني.