وزارة الصحة

اسم الخطة: إدارة الصيانة	رمز الخطة: MOH PLN D IM 11
عدد الصفحات : 7	الطبعة: الأولى

الاعداد : مديرية التحول الالكتروني و تكنولوجيا المعلومات		المعنيين بالخطة : موظفو مديرية التحول الالكتروني و تكنولوجيا المعلومات
تاريخ الاعداد:		
التوقيع:		
التدقيق والمراجعة :	التوقيع:	تاريخ التدقيق: 2024/2/14
التدقيق من ناحية ضبط الجودة :	التوقيع :	تاريخ تدقيق ضبط الجودة : 2024/2/15
الاعتماد: عطوفة الأمين العام للشؤون الإدارية والفنية تاريخ الإعتماد:	التوقيع:	تاريخ المراجعة القادم: 2024/2/18

وزارة الصحة
مديرية التطوير المؤسسي وضبط الجودة
السياسات و الاجراءات
Policies & Procedures
١٨ شباط ٢٠٢٤
ختم الاعتماد
معتمدة
Approved

تتم مراجعة السياسة كل سنتين على الأقل من تاريخ اعتماد آخر طبعة:		
رقم الطبعة	تاريخ الاعتماد	مبررات مراجعة السياسة

ختم النسخة الأصلية

MASTER COPY

وزارة الصحة

اسم الخطة: إدارة الصيانة					رمز الخطة:	MOH PLN D IM 11
عدد الصفحات : 7					الطبعة: الأولى	

المقدمة:

ادارة الصيانة هي عبارة عن مجموعة الإجراءات وسلسلة العمليات المستمرة التي يجب القيام بها بهدف وضع الآلة في وضع الاستعداد التام للعمل وإبقاء أجهزة الخوادم والشبكات وأجهزة الحاسوب وتوابعها والأنظمة المحوسبة في حالة عمل جيدة .

نطاق الخطة:

1- البنية التحتية للفضاء السيبراني

2- البريد الالكتروني

3- الموقع الالكتروني

4- موزعات الشبكة (SWITCHES)

5- غرفة البيانات (Data Center)

6- الخوادم (SERVERS)

7- متابعة ادامة تشغيل نظام حكيم بالتعاون مع شركة الحوسبة الصحية.

8- الأنظمة المحوسبة

الأهداف:

1- الحد من حدوث أي مخاطر تتعلق بالبنية التحتية الرقمية اوالخوادم أو موزعات الشبكه أو الموقع الالكتروني و غيره من المكونات المادية او البرمجيات المملوكة لوزارة الصحة .

2- زيادة كفاءة و جودة و سلامة المرافق و تقليل التكاليف و الاعطال و المخاطر

3- وضع الاجراءات اللازمة للتصدي لأي مخاطر يتعرض لها اي بند من بنود نطاق الخدمة.

4- التأكد من جاهزية موظفي المديرية و البرامج و التطبيقات والاجهزة و البروتوكولات اللازمة لمعالجة أي خطر او عطل عند وقوعه .

المسؤوليات والمهام:

1- مدير مديرية التحول الالكتروني و تكنولوجيا المعلومات

- الايعاز بالنقل التدريجي للأنظمة المحوسبة الى السحابة الالكترونية في وزارة الاقتصاد الرقمي بعد ترقية كافة الأنظمة المحوسبة لغايات النقل.
- توقيع اتفاقيات ادامة الصيانة وترقية الأنظمة المحوسبة.
- تأهيل الكوادر لمواجهة المخاطر التي تتعلق بالبنية التحتية للفضاء السيبراني الواردة في بند نطاق الخدمة

2- رئيس قسم الحكومة الالكترونية :

- تطبيق الفحوصات الأمنية اللازمة عند إطلاق الخدمات الالكترونية أو الربط مع شركاء الخدمات.
- الايعاز لموظفي القسم تطبيق سياسة كلمة المرور بحيث تطابق متطلبات التعقيد وتغييرها بشكل دوري.
- تجميد حساب البريد الالكتروني المخترق مؤقتا والتواصل مع الجهات المعنية الى ان يتم حل الاختراق.
- التعميم على الموظفين لتطبيق سياسة كلمة المرور.
- التعميم على الموظفين عند وجود تحديثات أمنية على البرامج أو التطبيقات.

وزارة الصحة

اسم الخطة: إدارة الصيانة					رمز الخطة:	MOH PLN D IM 11
عدد الصفحات : 7					الطبعة: الأولى	

3- رئيس قسم انظمة المعلومات و البرمجة

- متابعة تنفيذ عقود صيانة البرمجيات وقواعد البيانات مع الشركات المتخصصة.
- النسخ الاحتياطي للبرمجيات وقواعد البيانات.
- ترقية الأنظمة المحوسبة تمهيدا لنقلها الى السحابة الحكومية.
- مراقبة أداء الأنظمة المحوسبة وأسباب التعديلات على قواعد البيانات.
- إدارة تحديثات البرامج وأنظمة التشغيل

4- رئيس قسم الشبكات و الاتصالات :

- (اعلام الجهات المعنية (المركز الوطني للامن السيبراني ومديرية الامن السيبراني في وزارة الاقتصاد الرقمي) في حالة حدوث أي اختراقات امنية وبالتنسيق مع رئيس قسم الحكومة الالكترونية.
- استخدام برامج حماية
- استخدام الجدار الناري
- الابلاغ عن أي مشكلة أو عطل يقع على السيرفرات او غرفة مركز البيانات للجهات المسؤولة.

5- رئيس قسم البنية التحتية

- تجهيز البينة التحية السليمة والامنة لتشغيل كافة الأنظمة المحوسبة بدون انقطاع.
- الايعاز لموظفي القسم بتزويد المواقع التابعة لوزارة الصحة بالأجهزة الالكترونية حسب حاجتها وتركيبها وتشغيلها

وزارة الصحة

اسم الخطة: إدارة الصيانة					رمز الخطة:	MOH PLN D IM 11
عدد الصفحات : 7					الطبعة: الأولى	

6- رئيس قسم الدعم الفني

- تنزيل برامج مضاد الفيروسات
- الايعاز لموظفي القسم بتقديم الدعم الفني اللازم لصيانة أي جهاز يحتاج لصيانة او تركيب ملحقات.

7- المركز الوطني للأمن السيبراني

- معالجة اي اختراق في حال حدوثه
- تجميد اي بريد الكتروني او حساب مستخدم تم اختراقه لحين حل المشكلة.
- اصدار التقارير بحالة خوادم الوزارة والأنظمة المستضافة عليها

الخطة /الإجراءات:

- مخاطر تتعلق بالبنية التحتية للفضاء السيبراني (سرقة البيانات /تعديل البيانات)
  1- استخدام برامج حماية
  2- استخدام الجدار الناري
  3- إدارة الأحداث من قبل المركز الوطني للأمن السيبراني
- اختراق البريد الالكتروني للموظف

1-تطبيق سياسة كلمة المرور بحيث تطابق متطلبات التعقيد وتغييرها بشكل دوري.
2- مخاطبة وزارة الاقتصاد الرقمي والريادة في حال حدوث أي اختراقات.
3- تجميد البريد الالكتروني المخترق مؤقتا الى ان يتم حل الاختراق.

وزارة الصحة

اسم الخطة: إدارة الصيانة					رمز الخطة:	MOH PLN D IM 11
عدد الصفحات : 7					الطبعة: الأولى	

- اختراق الموقع الالكتروني الخاص بوزارة الصحة

1. التنسيق التام مع مديرية الامن السيبراني والمركز الوطني للأمن السيبراني لمواجهة خطر الاختراق لمعرفة ثغرة الاختراق والعمل على معالجتها.
2. اعادة الموقع الالكتروني للعمل بعد معالجة كافة الثغرات الامنية.
3. تقييم الاجراءات والسياسات المعتمدة في وزارة الاقتصاد الرقمي لعدم تكرار حدوث الاختراق

- مخاطر تتعلق بموزعات الشبكة (SWITCHES)

1. ربط الكبائن الخاصة بالموزعات بمزود طاقة في حال انقطاع التيار الكهربائي.
2. يوجد عدد من الموزعات الاحتياطية في حال تلف احد الموزعات.
3. عقد صيانة مع شركة متخصصة.

- مخاطر تتعلق بغرفة البيانات (Data Center)

1. وجود غاز FM200 لمكافحة خطر نشوب حريق.
2. توفر نظام للمراقبة للكشف وللتنبيه في حالة حدوث:
   - دخان حريق
   - تعطل اجهزة التكييف
   - ارتفاع درجات الحرارة.
   - تسرب مياه
   - انقطاع التيار الكهربائي المغذي لمركز البيانات.
3. يتم ربط التكييف بمولد كهرباء الوزارة في حال انقطاع الكهرباء.

- مخاطر تتعلق بالخوادم (SERVERS) مثل خطر التعرض لانقطاع الكهرباء/تعطل نظام التشغيل/تعطل الخادم نفسه/التعرض للاختراق.
  1- استخدام الجدار الناري
  2- استخدام أنظمة الحماية التي توفرها وزارة الاقتصاد الرقمي والريادة للأنظمة المستضافة لدى لديها
  3- مخاطبة وزارة الاقتصاد الرقمي والريادة والمركز الوطني للأمن السيبراني في حال حدوث أي حالات للاختراقات لمعالجتها

وزارة الصحة

اسم الخطة: إدارة الصيانة					رمز الخطة:	MOH PLN D IM 11
عدد الصفحات : 7					الطبعة: الأولى	

- مخاطر تتعلق ببيانات الأنظمة مثل فقدان البيانات/سرقة البيانات/تعديل البيانات

1. التنسيق مع المركز الوطني للأمن السيبراني ومديرية الامن السيبراني لمعرفة الثغرة الامنية التي تم استغلالها لعملية الاختراق ومعالجتها.
2. الرجوع لآخر نسخة احتياطية وارجاعها.
3. تغيير كافة كلمات المرور.
4. يتم العمل حاليا على اعتماد وثيقة الافصاح عن كافة حسابات المستخدمين لكل موظف يعمل في قسم أنظمة المعلومات والصلاحيات التي يمتلكها الموظف على كل نظام وقاعدة بيانات تابعة له.

المتابعة والقياس:

1- عدد الأعطال التي تمكن فريق مديرية التحول الالكتروني و تكنولوجيا المعلومات من حلها و عمل صيانة لها

2- المدة الزمنية التي استغرقت لحل المشكلة

المراجع :

- معايير وضوابط الأمن السيبراني للجهات المتعاقدة مع الوزارات والدوائر الحكومية 2023
- قانون الامن السيبراني رقم (16) لسنة 2019