قرار وزاري رقم (139) لسنة 2023

وزير الدولة لشئون الإسكان:

- بعد الاطلاع على القانون رقم (47) لسنة 1993 في شأن الرعاية السكنية والقوانين المعدلة له،
- وعلى المرسوم رقم 266 لسنة 2006 بإنشاء الجهاز المركزي لتكنولوجيا المعلومات وتعديلاته.
- وعلى القانون رقم 20 لسنة 2014 في شأن المعاملات الإلكترونية.
- وعلى لائحة شئون التوظف بالمؤسسة الصادرة بالقرار الوزاري رقم (39) لسنة 2016 وتعديلاتها،
- وعلى ما تقتضيه مصلحة العمل.

قـــرر

مادة أولى: يعمل بما ورد بوثيقة أمن وتداول المعلومات في المؤسسة العامة للرعاية السكنية المرفقة.

مادة ثانية: يصدر المدير العام قرار بتسمية " ضابط أمن المعلومات " ينص فيه على اختصاصاته وصلاحياته واختيار معاونيه.

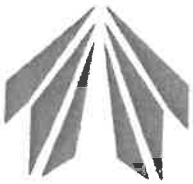
مادة ثالثة: يعمل بهذا القرار اعتبارا من تاريخ صدوره، وعلى كل فيما يخصه تنفيذه.

فالح عبدالله الرقبة

وزير العدل ووزير الدولة لشئون الإسكان

فالح عبدالله الرقبة
وزير العدل
ووزير الدولة لشئون الإسكان

وزير الدولة لشئون الإسكان
MINISTER OF STATE FOR HOUSING AFFAIRS



قرار وزاري رقم ( ) لسنة 2023

وزير الدولة لشئون الإسكان:

- بعد الاطلاع على القانون رقم (47) لسنة 1993 في شأن الرعاية السكنية والقوانين المعدلة له،
- وعلى المرسوم رقم 266 لسنة 2006 بإنشاء الجهاز المركزي لتكنولوجيا المعلومات وتعديلاته.
- وعلى القانون رقم 20 لسنة 2014 في شأن المعاملات الإلكترونية.
- وعلى لائحة شئون التوظف بالمؤسسة الصادرة بالقرار الوزاري رقم (39) لسنة 2016 وتعديلاتها،
- وعلى ما تقتضيه مصلحة العمل.

قـــرر

مادة أولى: يعمل بما ورد بوثيقة أمن وتداول المعلومات في المؤسسة العامة للرعاية السكنية المرفقة.

مادة ثانية: يصدر المدير العام قرار بتسمية - ضابط أمن المعلومات - ينص فيه على اختصاصاته وصلاحياته واختيار معاونيه.

مادة ثالثة: يعمل بهذا القرار اعتبارا من تاريخ صدوره، وعلى كل فيما يخصه تنفيذه.

فالح عبدالله الرقبة

وزير العدل ووزير الدولة لشئون الإسكان

الأصل بتوقيع

فالح عبدالله الرقبة

وزير العدل
ووزير الدولة لشئون الإسكان

إدارة مكتب الوزير
وارد 772
2023-12-20

م/ راشد فادي وحيل الرشيدي
مدير عام
المؤسسة العامة للرعاية السكنية بالتكليف

عبدالله محمد الكندري
مراقب التشغيل والدعم الفني

عبدالعزيز عبدالله الدوسري
مدير إدارة نظم المعلومات

(+965) 25393734 / 25388117 (+965) 25384541

وثيقة أمن وتداول المعلومات
في المؤسسة العامة للرعاية السكنية

وثيقة أمن وتداول المعلومات في المؤسسة العامة للرعاية السكنية

- بعد الاطلاع على المرسوم رقم 266 لسنة 2006بإنشاء الجهاز المركزي لتكنلوجيا المعلومات وتعديلاته،
- وعلى القانون رقم 16 لسنة 1960 بإصدار قانون الجزاء والقوانين المعدلة له،
- وعلى القانون رقم 17 لسنة 1960 بإصدار قانون الإجراءات والمحاكمات الجزائية والقوانين المعدلة له،
- وعلى القانون رقم 22 لسنة 1980 في شأن المعلومات المدنية،
- وعلى القانون رقم 64 لسنة 1999 في شأن الملكية الفكرية،
- وعلى القانون رقم 47 لسنة 1993 في شأن الرعاية السكنية والقوانين المعدلة له،
- وعلى القانون رقم 20 لسنة 2014 في شأن المعاملات الالكترونية،
- وعلى لائحة شؤون التوظف بالمؤسسة الصادرة بالقرار الوزاري رقم (39) لسنة 2016 وتعديلاتها،
- وعلى ما تقتضيه مصلحة العمل،

تمهيـــــد:

تعتبر المعلومات ذات أهمية قصوى للمؤسسات الحكومية وحماية هذه المعلومات أمر حيوي للحفاظ على أعمالها، لذا ومن أجل ضمان سلامة هذه الممتلكات الفكرية، كانت هذه الوثيقة مطلب لا غنى عنه.

إن هذه الوثيقة مبنية على أفضل الأساليب المجربة في بيئات العمل، مراعين بذلك الاختصار والإيجاز والتبسيط ليكون في متناول الجميع، ففي خضم مشاغل الحياة اليومية لمؤسسات الدولة فإن الرسائل والتوجيهات يجب أن تكون موجهه وذات هدف واضح يصلح للتطبيق على مجال واسع. لهذا السبب، فإن السياسات في هذا الدليل تم وضعها بشكل مختصر وعام بما يسهل عملية إتباعها.

تقوم الوثيقة على تأصيل سياسات عامة وتفصيلية تخص عدة جوانب من المؤسسة مثل سياسات تصنيف واستخدام وتوزيع المعلومة وسياسة كلمات السر وسياسات تطوير التطبيقات الداخلية وسياسة الأمن المادي وسياسة أمن مركز البيانات وسياسة استمرارية العمل وسياسة الموظفين وسياسة المورد الخارجي ومنفذي عقود ومشاريع المؤسسة.

الباب الأول: السياسات العامة لأمن المعلومات

1.1 سياسة أمن المؤسسة

1.1.1 هدف السياسة:

الهدف الأساسي من سياسة أمن المؤسسة العامة للرعاية السكنية هي تحديد المتطلبات والضوابط لأمن المؤسسة وذلك من خلال المنظور الشمولي للإدارة العليا.

1.1.2 مجال ومسؤولية السياسة

إن المستهدف الأساسي لهذه السياسة هم كافة الوحدات التنظيمية بالمؤسسة وعلى الأخص مجلس الإدارة والمدير العام ونواب المدير العام ومدراء الإدارات والمراقبين ورؤساء الأقسام ورؤساء الشعب، بينما يعتبر باقي الموظفين في المؤسسة كمستهدف ثانوي لهذه السياسة.

1.1.3 تفاصيل السياسة:

1. أمن وحماية المعلومات هو مسؤولية الجميع.
2. الأصل في استخدام الموارد المعلوماتية المنع الى أن يتم تصريح التداول بها داخل المؤسسة حسب آلية التصاريح المعتمدة في المؤسسة.
3. جميع عمليات الوصول إلى موارد ومعلومات المؤسسة يجب أن تكون مبنية على أساس الحاجة للمعرفة وهو أساس يفترض اخفاء المعلومة ما دامت استمرارية العمل المؤسسي لا تحتم اظهارها.
4. جميع المعلومات المصنفة تحت بند حساسة للغاية يجب إنشاءها وانجازها بطريقة ما بحيث يمنع الاطلاع أو إعادة الكتابة عليها.
5. المؤسسة تحرص على حفظ المعلومة واستمرارية تداولها على أن يقوم ضابط أمن المعلومات بالمؤسسة بتنسيق الجهود لتطبيق كل سياسات الأمن وفقا للاختصاصات الممنوحة له وفقا لقرارات المؤسسة المنظمة لهذا الشأن.
6. تقوم إدارة نظم المعلومات بإعداد قائمة رسمية لحصر وتحديد جميع الأجهزة والموارد المعلوماتية في المؤسسة مع مراعاة حسن تصنيفها وعنونتها بما يناسب مع طبيعة الموارد، وذلك ليسهل الرجوع إليها عند الحاجة.
7. يجب إخضاع شبكة المعلومات الداخلية للمؤسسة لعمليات المراقبة والفحص والدعم والتحديث الملائمة وبشكل منتظم.
8. يجب إبلاغ ضابط أمن المعلومات بأي محاولات لاختراق المعلومات وتهديدات للأمن المعلوماتي.
9. يجب إتباع تدابير وضوابط خاصة في حالة نقل المعلومات خارج نطاق المؤسسة وذلك للحفاظ على سريتها.
10. يجب فحص جميع البرامج المطورة (داخل أو خارج حدود المؤسسة) بغرض الاستخدام في المؤسسة، وذلك قبل السماح بتداولها أو استخدامها في بيئات العمل.
11. ضابط أمن المعلومات يقع على عاتقه تنظيم برامج وندوات من شأنها رفع وتعزيز مستوى الوعي الأمني للمؤسسة.
12. يعتبر الأمن المادي ذو أهمية جوهرية يتوجب عدم إغفالها، لذا فإن كل الجهود يجب أن تبذل لدعم تحديد صلاحيات الدخول للمباني والممتلكات التابعة للمؤسسة.
13. تقوم المؤسسة بتحديد مسؤولية مراجعة وتنقيح وثيقة أمن المعلومات وبشكل دوري.
14. يجب إجراء فحص سنوي للنظام وذلك لفحص التحكم بالأنظمة وفقا للمعمول به في إدارة نظم المعلومات.

15. يجب أن تحتوي جميع الوثائق في المؤسسة على صفحة لضبط الإصدار بالإضافة لتاريخ الوثيقة، هذا مع مراعاة أن تكون جميع صفحات الوثيقة مرقمة.
16. يجب القيام بعمليات الفحص المناسبة لأنظمة المعلومات داخل المؤسسة وبشكل منتظم ودوري لضبط أي حالات ضعف أو قصور أمني.
17. يجب اتخاذ التدابير والمقاييس المناسبة لتأمين جميع معدات ومصادر وأسلاك الطاقة الكهربائية.
18. ضابط أمن المعلومات وبما يتفق مع اللوائح والنظم المعمول بها في المؤسسة له أن يعين أشخاصا (أو الاستعانة بجهات خارجية) في فريق الاستجابة لحوادث وأعطال الكمبيوتر، لديهم الكفاءة والقدرة على التعامل مع الحوادث والانتهاكات الأمنية في حالة التعرض لها.
19. على كل الموظفين ارتداء الشارات التعريفية الخاصة بهم وذلك خلال تواجدهم في مباني المؤسسة.
20. ضرورة تطبيق سياسة "المكتب النظيف" في كل أنحاء المؤسسة المعنية.
21. يجب كتابة جميع ما يعرف بسجلات الأداء (او سجلات النفاذ الى النظام) الهامة على أقراص ممغنطة تسمح بالقراءة فقط ولا تسمح بإعادة الكتابة، وذلك لمنع أي محاولة لتغيير محتوى هذه السجلات. آخذين بعيين الاعتبار أن هذه السجلات يجب أن تراجع بواسطة الأشخاص المفوضين فقط.
22. التزام المؤسسة بتطبيق كل ما من شأنه ان يؤكد ويدعم المعاملات الالكترونية
23. في حال الإخلال بأي ضوابط تقررها الوثيقة فإن لضباط أمن المعلومات تطبيق العقوبات التأديبية التي تقرها المؤسسة بعد التنسيق الإدارة القانونية وبما لا يتعارض مع النظم المعمول بها.

1.2 سياسة استخدام المعلومات

1.2.1 الغرض

الغرض من سياسة الاستخدام المتفق عليها هو تعريف السلوك المقبول للموظف، والذي يعتبر ضروريا لتحقيق سرية، واستمرارية وسلامة كلا من الأنظمة والمعدات والمعلومات.

1.2.2 المجال

المجال لهذه السياسة يغطي كل الموظفين بكافة مستوياتهم الوظيفية الدائمين/ذوي العقود، والمستشارين والبائعين/الأطراف الثالثة المنسوب لهم أعمال تخص المؤسسة.

1.2.3 السياسة

1. جميع المعلومات المخزنة والمتبادلة من خلال موارد المؤسسة تبقى ملكية خاصة بالمؤسسة، وللمؤسسة الحق الكامل المكفول بمراقبتها والتدقيق عليها.
2. يقع على عاتق الموظفين حماية كلمات السر والعبور الخاصة بهم، ولا يجدر بهم مشاركة هذه المعلومات مع أي أحد كان.
3. يجب تغيير كلمة السر بما يتوافق مع سياسة كلمة السر المحددة في هذه الوثيقة.
4. يجب إن تحوي جميع أجهزة الحاسوب، المكتبية والمحمولة، على كلمة سر لحماية شاشة الحفظ، على أن تفعل هذه الشاشة بعد مدة لا تزيد عن 10 دقائق من عدم الاستخدام.
5. يجب أن يتم حماية جميع المعلومات الهامة والحساسة المخزنة على أجهزة الحاسوب المحمولة بكلمة سر.
6. يجب تشغيل برنامج مكافح فيروسات محدث على جميع الأجهزة. ولا يسمح لأي موظف كان بتعطيل أو إيقاف محرك استكشاف الفيروسات.
7. يجب إتباع سياسة الإنترنت والبريد الإلكتروني وذلك عند استخدام البريد الإلكتروني أو الإنترنت.
8. يحظر النسخ أو الاستخدام غير قانوني للبرامج أيا كان انواعها.

9. يحظر استخدام موارد المؤسسة لاختبار أي برنامج وذلك لاحتمالية أن يكون هذا البرنامج معطل أو أن يكون خبيث بطبيعته. هذا ويستثنى من ذلك البرامج المراد استخدامها لأغراض المؤسسة.
10. يمنع منعا باتا استكشاف ومسح المنافذ والثغرات للخوادم الداخلية والخارجية، إلا إذا كان هذا العمل جزء من اختبار الاختراق الرسمي المجرى بوساطة المؤسسة، وباتخاذ التدابير المضادة المناسبة.
11. لا يسمح لأي شخص بتصفح شبكة المؤسسة من كمبيوتره الشخصي أو من أي مورد آخر الا بعد أخذ الموافقة من فريق ضباط أمن المعلومات بعد التنسيق مع إدارة نظم المعلومات.

1.3 سياسة الوعي الأمني

1.3.1 الغرض

الغرض من هذه السياسة هو إبقاء الموظفين مواكبين لتطورات سياسة الأمن والتي تتغير بسرعة مذهلة.

1.3.2 المجال

هذه السياسة لجميع الموظفين بغض النظر عن المراكز التي يشغلونها.

1.3.3 السياسة

1. سيقوم ضابط أمن المعلومات بتقديم كتيبات وورش عمل بسياسات تفصيلية لجوانب مختلفة في امن المعلومات لجميع الموظفين وبشكل دوري
2. سيقوم ضابط أمن المعلومات بتنظيم ورشة عمل واحدة على الأقل سنويا، وحضور كل الموظفين المدعوين إلزامي.
3. إذا دعت الحاجة، فإن ضابط أمن المعلومات قد يلجأ للاستعانة بالنشرات والملصقات و/أو شاشة حفظ خاصة للوعي الأمني وذلك لزيادة أمن المعلومات.
4. سيكون الوعي بسياسة الأمن أحد المحاور التي يتم بموجبها تقييم الموظف.

1.4 سياسة تصنيف البيانات

1.4.1 الغرض

الغرض من هذه السياسة هو التوافق مع سياسات هيئة الاتصالات وتقنية المعلومات في دولة الكويت لتصنيف البيانات في المؤسسة وحفظ المعلومات فيها وتصميم طرق الاستضافة وحفظ امن المعلومات.

1.4.2 المجال

هذه السياسة موظفي إدارة نظم المعلومات في المؤسسة.

1.4.3 السياسة

1. تقوم ادارة نظم المعلومات بقيادة فرق مشتركة مع الإدارات الاخرى في المؤسسة بتنظيم وتنفيذ عمليات دورية لمراجعة كافة البيانات والتدقيق عليها واستبعاد أو معالجة البيانات غير الكاملة منها أو المبهمة أو الغامضة.
2. سيقوم فريق بمشاركة مسؤول قواعد البيانات في المؤسسة بمراجعة تصميم جداول وبيانات وقواعد البيانات بإضافة تصنيف لتلك البيانات حسب التصنيفات الأربعة التالية: بيانات عامة، بيانات خاصة غير حساسة، بيانات خاصة وحساسة، وبيانات عالية الحساسية وحسب تعريفات دليل تصنف البيانات الصادر من هيئة الاتصالات وتقنية المعلومات في الدولة.

3. تقوم فرق المراجعة بمراعاة الدقة في فرز ووضع البيانات في مستويات التصنيف وفقا لهذه السياسة لكي يتم تحديد المخاطر التي تحيط بكل مستوى، وتقييم هذه المخاطر لضمان سلامة وحماية تلك البيانات.
4. بغرض ضمان التطبيق الكامل لتصنيف البيانات ودعم توحيد الإجراءات مع مختلف الجهات الحكومية، تقوم إدارة نظم المعلومات في المؤسسة بما يلزم نحو وضع خارطة طريق وخطة عمل توضح كيفية قيامها بعملية تصنيف البيانات وفقا للأربعة مستويات الأساسية الموضحة في هذه السياسة، على أن يتم مراجعة تصنيف البيانات بشكل دوري ثابت.
5. يتعين على إدارة نظم المعلومات إنشاء والحفاظ على دليل للبيانات والذي يجب أن يتضمن معلومات ومعايير بيانات التعريف الخاصة بالبيانات بتنسيق موحد. كما يجب تحديث هذا الدليل بشكل دوري
6. يتوجب على إدارة نظم المعلومات في المؤسسة عمل ما يلزم لتشفير كافة البيانات المصنفة وفق المستوى الثالث والرابع حال نقلها الى جهة حكومية أخرى أو من خوادم قواعد البيانات الى المواقع التابعة للمؤسسة والموزعة جغرافيا في أماكن مختلفة.
7. يجب على إدارة نظم المعلومات في المؤسسة اعتماد طرق مختلفة لحماية البيانات وفقا لنظام التصنيف أعلاه والتأكد من توفير الحماية اللازمة لطريقة حفظ البيانات وفقا لدرجة تصنيفها وخصوصا تلك المصنفة وفق المستوى الثالث والرابع للحفاظ عليها من الاختراق.
8. يتعين على إدارة نظم المعلومات في المؤسسة التأكد من نقل أو إزالة كافة البيانات المصنفة وفقا للمستوى الثالث والرابع من مراكز البيانات والخوادم قبل تبديل أو التخلص من التجهيزات الآلية لمراكز البيانات والخوادم المستضيفة لتلك البيانات.
9. يمكن لإدارة نظم المعلومات استخدام مستويات تصنيف أخرى وفقا لأفضل الممارسات العالمية والمعايير مثل NIST 800-53، NIST SP 800-60، ISO 27001، PCI DSS، HIPAA لضمان صحة وجودة التصنيف.

الباب الثاني: السياسات التفصيلية لأمن المعلومات

2.1 سياسة حماية كلمة السر

2.1.1 الغرض

هذه الوثيقة تحدد سياسة المؤسسة المتعلقة بحماية كلمة السر، وتغييرها وصيانتها.

2.1.2 المجال

المجال لهذه السياسة يتضمن كل الموظفين بغض النظر عن مواقعهم.

2.1.3 السياسة

1. جميع كلمات السر الافتراضية يجب تغييرها بواسطة المستخدم وذلك قبل استخدام النظام.
2. يجب ألا تقل كلمة السر عن 8 حروف مكونة من خليط من الحروف والأرقام، مدمجة بأحرف صغيرة وكبيرة.
3. يجب تغيير كلمة السر كل 180 يوم (على الأقل) أو كلما حدث اختراق النظام أيا كان نوعه.
4. لا يجب استخدام الاسم الشائع أو أي معلومات شخصية ككلمة سر، على سبيل المثال: تاريخ الميلاد، اسم القرين أو اسم الحيوان الأليف أو رقم الهاتف.
5. يجب أن تكون كلمة السر مختلفة عن كلمات السر التي يستخدمها الموظف للاستخدام الشخصي أو في شبكة الانترنت.
6. يجب أن تحفظ كلمة السر بسرية دائما، ولا يجب إطلاع الأصدقاء أو زملاء العمل عليها.
7. يجب أن يتم تفعيل خيار "كلمة سر الجهاز" (كلمة السر عند التشغيل BIOS) في جميع أجهزة الحاسب الشخصية من قبل إدارة نظم المعلومات.
8. غير مسموح لأي شخص ترك كمبيوتره/ها الشخصي أو جهازه دون أن يسجل خروجه من النظام، أو دون أن تكون الشاشة محمية بكلمة سر.
9. في حالة الطوارئ أو في حالة عدم تواجد مدير النظام، فإنه يمكن الحصول على كلمة السر من الموظف المعين من قبل ضابط أمن المعلومات.

2.2 سياسة توظيف وتطوير التطبيقات العامة

2.2.1 الغرض

هذه السياسة تحدد متطلبات تطوير التطبيقات سواء كانت داخلية أو بطلب من المؤسسة.

2.2.2 المجال

هذه السياسة قابلة للتطبيق على كل برمجيات المؤسسة الأساسية والبرمجيات الأخرى، ولكنها على كل حال تستثني أنظمة التشغيل. المسؤولية في تطبيق هذه السياسة تقع على مدير تقنية المعلومات، ومحلل النظم، والمبرمج ومسؤول أمن المعلومات.

2.2.3 السياسة

1. يجب أن تتضمن المتطلبات الرسمية عند تطوير الأنظمة للمؤسسة سواء كانت داخلية أو خارجية جزئيات تتعلق بقدرة هذه الأنظمة لحفظ أمن المعلومات فيها.
2. يجب الفصل بين بيئة الإنتاج وبيئة الاختبار/التطوير.
3. قبل أن يتم نقل النظام إلى بيئة الإنتاج (العمل الحقيقي) فإنه يجب توثيق البرنامج بشكل مناسب يضمن قدرة المستخدمين داخل المؤسسة للوقوف على الأخطاء التنفيذية إن وجدت.
4. يجب ألا يتم استخدام أي نسخ تجريبية، أو مجانية أو تحت التطوير في بيئات العمل الحقيقي إلا بموافقة الإدارة ومدير أمن المعلومات وتحت ظروف استثنائية.
5. جميع عمليات الدخول يجب أن تبنى على أساس - الحاجة للمعرفة.
6. يجب أن تمتلك المؤسسة أكواد المصدر الأساسية للتطبيق، أو أن يكون هناك اتفاقات ضمان مع المورد المزود للتطبيقات يمنعه من التصرف بها وبيعها أو نقلها لجهات اخرى.
7. يجب أن يخضع التطبيق لتجربة مستفيضة وذلك قبل نقله لبيئة الإنتاج أو العمل الحقيقية.
8. يجب تطبيق اختبار قبول المستخدم على أية تطبيق قبل نقله إلى بيئة العمل.
9. عند بداية انتاج أية تطبيق، يجب تهيئة بيئة انتاج نظيفة تماما وخالية من أية حسابات خاصة بالمطور هناك، بحيث ألا يملك المطور أي حساب في آلة الإنتاج.
10. يجب أن تتبع قواعد البيانات سياسة كلمة السر المذكورة ضمن السياسات السابقة.
11. أي عملية لتحديث قاعدة البيانات يجب أن تتم بطريقة صحيحة وباستخدام قناة آمنه بين خادم التحديث وبيئة قواعد البيانات.
12. عند استخدام تطبيق مستودع البيانات المركزي (data warehousing) فإن عملية الدخول يجب أن تقتصر على الإدارة العليا والوسطى.

2.3 سياسة الأمن المادي العامة (الممتلكات)

سياسة الأمن المادي تقع مسؤوليتها على عاتق كل وحدة تنظيمية في المؤسسة وفقا لاختصاصها وبما لا يتعارض مع السيايات المقررة في هذه الوثيقة ولضابط أمن المعلومات إبداء ملاحظاته وممارسة صلاحياته المقررة حال وجود أي إجراء ينتج عنه الإخلال بسياسة أمن المعلومات المقررة في هذه الوثيقة.

2.3.1 الغرض

هذه السياسة تحدد متطلبات الأمن المادي. إذا ما كان الأمن المادي ضعيف، كل شيء يصبح غير آمن، بغض النظر عن جودة حلول ونتائج الأمن الأخرى.

2.3.2 المجال

هذه السياسة صالحة لكل المناطق المادية لمكاتب المؤسسة، متضمنة تلك الموجودة حاليا أو تلك التي من الممكن إضافتها لاحقا. المسؤولية تقع في تطبيق هذه السياسة على ممثلي إدارة نظم المعلومات وإدارة الشئون الإدارية، ومسؤول أمن المعلومات. مستقبلا، فإن بعض المهام المتعلقة بالأمن المادي، قد تؤول إلى مسؤول أمن المؤسسة عند شغل هذه المنصب. لكن إن لم يوجد، فإن مسؤول أمن المعلومات سيكون مسؤول عن هذه المهام.

2.3.3 السياسة

1. يجب أن يقوم مسؤول أمن المعلومات بتعريف مناطق الأمن في المؤسسة. فمثلا:
   - المنطقة أ: منطقة الاستقبال، حيث باستطاعة أي شخص أن يدخلها (تعتبر الأقل أمنا).
   - المنطقة ب: وهي المنطقة المتاحة للموظفين والزوار المصرح لهم.
   - المنطقة جـ: وهي المنطقة التي يسمح فقط لبعض الموظفين بدخولها، من مثل غرفة الخوادم ومناطق العمل الأخرى الهامة.
2. يجب أن يطبق مسؤول أمن المعلومات معايير الحماية المناسبة لكل منطقة من المناطق.
3. يجب أن يتم توثيق وحفظ المخططات الخاصة بأرض المكتب والرسوم البيانية لكل خطوط كابل الهاتف، والكهرباء والماء والشبكة، بالإضافة إلى أماكن مطافئ الحريق.
4. يجب أن يتم عمل وحفظ قائمة للتحكم بالدخول للمرافق مرتبطة بأوقات العمل فيها.
5. يجب أن يتم حراسة مدخل المؤسسة بشكل كافي.
6. يجب أن يتم توفير آليات مناسبة لمقاومة واكتشاف الحرائق.
7. يجب أن يتم حفظ دليل هواتف لأرقام الطوارئ في مكان يسهل الوصول إليه عند الحاجة.
8. يجب أن يتم توفير صندوق للإسعافات الأولية، على أن يحفظ في مكان يسهل الوصول إليه، مع مراعاة فحصه واستكمال أي نقص فيه بانتظام.

2.4 سياسة أمن مركز بيانات/غرفة الخوادم

2.4.1 الغرض

هذه السياسة تناقش المتطلبات الازمة لحماية أنظمة الكمبيوتر ولإدارة العاملين في مركز بيانات/غرفة الخوادم.

2.4.2 المجال

هذه السياسة صالحة لكل المناطق المادية لمكاتب المؤسسة، متضمنة تلك الموجودة حاليا أو تلك التي من الممكن إضافتها لاحقا.

2.4.3 السياسة

1. سيكون الدخول إلى غرفة الخوادم مقصورا على أفراد المؤسسة المخولين فقط.
2. يجب مرافقة مندوبي الطرف الثالث والموردين إذا ما قاموا بزيارة غرفة الخوادم.
3. يجب حفظ سجل لوقت أي دخول أو خروج على غرفة الخوادم.
4. يجب توفير نظام إنذار ومقاومة حرائق مناسب.
5. يجب أن يتم مراقبة والمحافظة على درجة الحرارة بحدود مناسبة.
6. سيقوم ضابط أمن المعلومات بتنسيق الجهود لتطوير المعايير الخاصة بأمن المعلومات لغرفة الخوادم بشكل دوري وذلك بالتنسيق مع إدارة نظم المعلومات.
7. سيقوم ضابط أمن المعلومات بتنسيق الجهود للتأكد من وجود مزود طاقة ذو كفاءة عالية لغرفة الخوادم، وللتأكد من توفر الضمانات الكافية لحماية الأجهزة وذلك بالتنسيق مع إدارة نظم المعلومات.
8. لا يسمح بالأكل أو الشرب أو التدخين في غرفة الخوادم.
9. يمنع استخدام الهاتف النقال في مركز البيانات.

2.5 سياسة أمن الخادم

2.5.1 الغرض

هذه السياسة تناقش المسائل المتعلقة بأمن الخوادم الداخلية للمؤسسة، وذلك للتأكد من أنه ليس هناك أي دخول غير مخول على معلومات المؤسسة.

2.5.2 المجال

هذه السياسة تنطبق على كل الخوادم المملوكة أو المدارة بوساطة المؤسسة أو التي تحتوي تطبيقات تستخدمها المؤسسة إما عن طريق الامتلاك أو عن طريق التأجير.

2.5.3 السياسة

1. يجب وضع الخادم في منطقة مادية آمنة حسب سياسات الأمن المادي لمراكز البيانات.
2. كل سياسات إدارة التغيير يجب أن تطبق بحزم على الخوادم.
3. يجب أن يوافق مسؤول أمن المعلومات على كل إعدادات الخوادم.
4. يجب مراقبة سجل الخادم بطريقة دورية ومنتظمة بحسب الجدول الذي يحدده مسؤول أمن المعلومات.
5. يجب تعطيل جميع الحسابات المصنعية (default account) وحسابات الزوار (guest account) أو تغيير كلمة السر لها.
6. إذا ما لزم الأمر لإدارة الخادم عن بعد، فإنه يجب استخدام قناة آمنة لهذا الغرض حسب سياسات القنوات الافتراضية الآمنة.
7. يجب الحد من استخدام حساب التحكم بالخادم، من مثل مستخدم أول أو المستخدم الجذري، فقط عند الحاجة.
8. سيقوم ضابط أمن المعلومات بعمل مراجعة دورية على هذه السياسات ومتى دعت الضرورة.

2.6 سياسة الموظفين

2.6.1 الغرض

هذه السياسة تختص بالإرشادات والمقاييس المتعلقة بالموارد البشرية ذات الصلة الخاصة بأمن المعلومات.

2.6.2 المجال

هذه السياسة تنطبق على كافة موفي المؤسسة على مختلف مستوياتهم الوظيفية.

2.6.3 السياسة

1. يجب على الموظفين التوقيع على تعهد بقبول المسؤولية بالانضمام لسياسات الأمن في المؤسسة.
2. ستقوم إدارة نظم المعلومات بالتأكد من أنه تم حذف كل حسابات الكمبيوتر للموظف المغادر للمؤسسة وذلك قبل التسوية النهائية له/لها.

2.7 سياسة الطرف الثالث

2.7.1 الغرض

هذه السياسة تختص بالإرشادات والمقاييس المتعلقة بالطرف الثالث والمورد الخارجي.

2.7.2 المجال

هذه السياسة تنطبق على الأطراف أيا كانوا، سواء موردين، متعهدين، مستشارين أو موردين خارجيين مختصين.

2.7.3 السياسة

1. تعتبر الموافقة على اتفاقية المحافظة على السرية أو كما تسمى أحيانا اتفاقية عدم الكشف (أو الإفصاح) - ضرورية، وذلك قبل مشاركة المعلومات الهامة مع أي طرف ثالث.
2. يجب تحديد دور ومسؤوليات الطرف الثالث بوضوح.
3. سيتم إعطاء الطرف الثالث صلاحية الدخول على نظام الكمبيوتر للمؤسسة، فقط بعد التوقيع على عقد رسمي يحوي كل المتطلبات الأمنية الواجب على الطرف الثالث الالتزام بها.
4. في حالة ما إذا تم تعريف مستخدمين خارجيين أو طرف ثالث على النظام، فإنهم جميعا يجب أن يكون لديهم تاريخ انتهاء صلاحية إجباري للدخول.

المؤسسة العامة للرعاية السكنية
Public Authority for Housing Welfare

السيد / الفاضل راشد هادي العنزي المحترم

مدير عام المؤسسة العامة للرعاية السكنية بالتكليف

تحية طيبة وبعد ،،،

الموضوع سياسة امن وتداول المعلومات

بالإشارة الى الموضوع أعلاه والحاقا الى كتابنا رقم 3736 المؤرخ في 2023/11/21 والمتضمن تأشيرتكم لنا (لإعداد القرار الوزاري بعد المداولة) ، وتأكيدا على أهمية الموضوع بضرورة التحول الرقمي وحفاظا على أنظمة المؤسسة من التعرض للاختراقات الخارجية والداخلية لبياناتها ، وعليه نرفق لكم مسودة القرار الوزاري لوثيقة امن وتداول المعلومات في المؤسسة لاعتمادها ورفعها الى معالي الوزير.

وتفضلوا بقبول فائق الاحترام والتقدير،،،

امينة عبدالكريم العوضي

نائب المدير العام لشئون

الرقابة ونظم والمعلومات

مكتب المدير العام
صادر 10488
2023-12-20

م. ع. لشئون الرقابة ونظم المعلو
صادر 4078
2023-12-14

ادارة مكتب المدير العام
وارد 10037
2023-12-20

المؤسسة العامة للرعاية السكنية
Public Authority for Housing Welfare

السيد / الفاضل راشد هادي العنزي المحترم

مدير عام المؤسسة العامة للرعاية السكنية بالتكليف

تحية طيبة وبعد ،،،

الموضوع سياسة امن وتداول المعلومات

بالإشارة الى الموضوع أعلاه والحاقا الى كتابنا رقم 3736 المؤرخ في 2023/11/21 والمتضمن تأشيرتكم لنا (لإعداد القرار الوزاري بعد المداولة) ، وتأكيدا على أهمية الموضوع بضرورة التحول الرقمي وحفاظا على أنظمة المؤسسة من التعرض للاختراقات الخارجية والداخلية لبياناتها ، وعليه نرفق لكم مسودة القرار الوزاري لوثيقة امن وتداول المعلومات في المؤسسة لاعتمادها ورفعها الى معالي الوزير.

وتفضلوا بقبول فائق الاحترام والتقدير،،،

امينة عبدالكريم العوضي

الاصل بتوقيعه

امينه عبدالكريم العوضي

نائب المدير العام لشئون الرقابة

ونظم المعلومات

نائب المدير العام لشئون

الرقابة ونظم والمعلومات

ادارة مركز نظم المعلومات

صادر 1730

2023-12-14

مدير ادارة نظم المعلومات