



جمعية دارك للإسكان التنموي
Darak for development housing



سياسة الأمن السيبراني للبيانات

بجمعية دارك للإسكان التنموي

الإصدار الأول
2025/05/15

سياسة الأمن السيبراني: للبيانات

بجمعية دارك للإسكان التنموي:

جمعية دارك للإسكان التنموي
Darak for development housing



معلومات الوثيقة

سياسة الأمن السيبراني للبيانات	عنوان السياسة
P – IT - 015	الرقم المرجعي
v 1.01	رقم الإصدار
مجلس إدارة جمعية دارك للإسكان التنموي	مالك السياسة
داخلي <input checked="" type="checkbox"/> خارجي <input checked="" type="checkbox"/>	نطاق الوثيقة
١٤٤٦/١١/١٧ هـ - ٢٠٢٥/٥/٢٥ م	تاريخ الاعتماد
-	تاريخ المراجعة
داخلي <input checked="" type="checkbox"/> خارجي <input checked="" type="checkbox"/>	النشر

سياسة الأمن السيبراني للبيانات

بجمعية دارك للإسكان التنموي

جمعية دارك للإسكان التنموي
Darak for development housing



المحتويات

٤	الغرض من السياسة
٤	نطاق السياسة
٤	بنود السياسة
٦	الالتزام بالسياسة
٦	المراجعة الدورية وتحديث السياسة



الغرض من السياسة

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة بالأمن السيبراني للبيانات الخاصة بجمعية دارك للإسكان التنموي لتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية وذلك لتحقيق الأهداف الرئيسية للحماية وهي: سرية المعلومات، وسلامة أنظمة المعلومات، وتوافرها.

نطاق السياسة

تنطبق هذه السياسة على جميع البيانات التي تحتفظ بها جمعية دارك للإسكان التنموي وتخزنها وتعالجها وتنقلها من خلال الأصول المعلوماتية والتقنية، وعلى جميع العاملين (الموظفين والمتعاقدين) في جمعية دارك للإسكان التنموي.

بنود السياسة

١- البنود العامة

- ١-١ يجب أن تلتزم جمعية دارك للإسكان التنموي بالمتطلبات التشريعية والتنظيمية المتعلقة بحماية البيانات في المملكة العربية السعودية، والسياسات والإجراءات المتبعة في جمعية دارك للإسكان التنموي.
- ٢-١ يجب أن تحدد الجمعية وتحديث متطلبات الأمن السيبراني للبيانات بشكل دوريًا.
- ٣-١ يجب على الجمعية ضمان إدارة متطلبات الأمن السيبراني للبيانات بكفاءة وفقاً لسياسة الأمن السيبراني في الموارد البشرية وسياسة إدارة الأصول الخاصة بالجمعية.
- ٤-١ يجب أن تضمن الجمعية حماية الأجهزة المحمولة وفقاً لسياسة أمن الأجهزة المحمولة في الجمعية.
- ٥-١ يجب أن تستخدم الجمعية تقنيات وحلول منع تسريب البيانات.
- ٦-١ يحظر استخدام بيانات الجمعية في أي بيئة غير بيئة الإنتاج، إلا بعد إجراء تقييم للمخاطر وتطبيق الضوابط لحماية تلك البيانات، مثل: تقنيات تعقيم البيانات (masking) أو تقنيات مزج البيانات (data scrambling).
- ٧-١ يجب أن تحدد الجمعية التقنيات والأدوات والإجراءات للتخلص من البيانات بطريقة آمنة حسب مستوى التصنيف.
- ٨-١ يجب أن تعمل الجمعية على إعداد وتنفيذ استراتيجية للخروج لضمان وسائل الإتلاف للأمن للبيانات عند إنهاء أو انتهاء سريان العقد مع مقدم الخدمة السحابية.
- ٩-١ يجب أن تضمن الجمعية الاستخدام المناسب والفعال لتقنيات التشفير لحماية بيانات جمعية دارك للإسكان التنموي وفقاً لسياسة ومعايير التشفير في جمعية دارك للإسكان التنموي والمتطلبات التشريعية والتنظيمية ذات العلاقة.
- ١٠-١ يجب على الجمعية تحديد الأدوار والمسؤوليات للأمن السيبراني لضمان ان البيانات متوافقة مع المتطلبات القانونية والتنظيمية.

- ١١-١ يجب أن تستخدم الجمعية طريقة آمنة لاستخراج ونقل البيانات واستخراج ونقل البنية التحتية الافتراضية.
 - ١٢-١ يجب أن تمنع الجمعية نقل أي بيانات للأنظمة الحساسة من بيئة الإنتاج إلى أي بيئة أخرى.
 - ١٣-١ يجب أن تستخدم الجمعية خاصية العلامات المائية (watermark feature) لترميز الوثيقة بأكملها عند إعدادها، أو تخزينها، وطباعتها، أو عرضها على الشاشة، والتأكد من احتواء كل نسخة من الوثيقة على رقم يمكن تتبعه.
 - ١٤-١ يجب قياس مؤشرات الأداء الرئيسية (KPI) للتأكد من التحسين المستمر لمتطلبات الأمن السيبراني لحماية البيانات.
- ٢- التصنيف والتعامل الآمن مع المعلومات**
- ١-٢ يجب تصنيف بيانات الجمعية وفقاً لسياسة تصنيف البيانات المعتمدة في جمعية دارك للإسكان التنموي.
 - ٢-٢ يجب تصنيف جميع بيانات الجمعية في كل الصيغ التالية:
 - ١-٢-٢ الصيغ الرقمية (مثل وثائق برنامج معالجة النصوص "Word"، وجداول البيانات "Spreadsheets"، وقواعد البيانات).
 - ٢-٢-٢ الاتصالات الإلكترونية (مثل رسائل البريد الإلكتروني وخدمات الاتصالات الصوتية والمؤتمرات والاتصالات الهاتفية وغيرها)
 - ٣-٢-٢ الصيغ المادية (مثل المطبوعات، والنسخ الورقية للقرود ودفاتر الملاحظات).
 - ٤-٢-٢ المحادثات الشفهية (مثل الاجتماعات والمقابلات).
 - ٣-٢ يجب أن يتجنب العاملون مناقشة بيانات الجمعية بصيغة شفوية في المناطق العامة، أو في مناطق قد تُسمع فيها مناقشاتهم. ويجب أن تتم المناقشات في مقرات جمعية دارك للإسكان التنموي وفي مواقع آمنة ضمن المقرات.
 - ٤-٢ يجب تصنيف جميع البيانات التي تحتفظ فيها الجمعية في كل الأنظمة (بما في ذلك الأنظمة الحساسة وأنظمة الحوسبة السحابية) وترميزها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة، وسياسة تصنيف البيانات المعتمدة في الجمعية.
 - ٥-٢ يجب أن يتولى المسؤولون عن البيانات، الذين عينتهم الجمعية للعمل مع الأطراف المعنية ذات العلاقة مع الجمعية ، مسؤولية تصنيف البيانات على النحو الوارد في هذه السياسة.
 - ٦-٢ يجب إبلاغ الأطراف المعنية ذات العلاقة في الجمعية على الفور عن أي مخالفة لهذه السياسة ولضوابط تصنيف البيانات.
 - ٧-٢ يجب تطبيق ضوابط الوصول عن بُعد للبيانات وفقاً لنموذج سياسة إدارة هويات الدخول والصلاحيات المعتمدة في الجمعية.
 - ٨-٢ يجب عدم حفظ البيانات المصنفة (سرية، سرية للغاية) في أجهزة تخزين محمولة مثل الأقراص الصلبة الخارجية أو وحدات التخزين "USB"، بغض النظر عن مستوى التشفير المستخدم في جهاز التخزين المحمول.

- ٩-٢ يجب عدم إدخال أو معالجة أو تغيير أو حفظ أو نقل البيانات المصنفة (سرية، وسرية للغاية) إلى الأجهزة التي يملكها الموظفون، والتي يُطلق عليها استخدام الأجهزة الشخصية للعاملين في الجهة (BYOD)، ما لم تكن تلك البيانات خاصة بالموظفين.
- ١٠-٢ يجب حماية البيانات المصنفة (سرية، وسرية للغاية) التي يمكن الوصول إليها أو معالجتها أو حفظها أو نقلها من خلال أنظمة الدخول عن بعد، ما لم تكن تلك البيانات خاصة بالموظفين.
- ١١-٢ يجب تحديد المجموعات الفرعية من البيانات المصنفة (مثل سرية، وسرية للغاية)، التي يمكن الوصول إليها أو معالجتها أو حفظها أو نقلها من خلال أنظمة العمل عن بُعد، وفقًا للمتطلبات التنظيمية ذات العلاقة.
- ١٢-٢ يجب ألا تحتوي الأصول التقنية لإدارة حسابات مواقع التواصل الاجتماعي للجمعية على بيانات مصنفة، وفقًا للمتطلبات التنظيمية ذات العلاقة.

٣- الاحتفاظ بالسجلات

- ١-٣ يجب أن تحتفظ الجمعية بسجلات المعتمدة المقدمة من ملاك البيانات، ويجب أن تحتفظ بسجلات سحب أو إلغاء الموافقات لفترة زمنية محددة وفقًا للمتطلبات التشريعية والتنظيمية.
- ٢-٣ يجب أن تحتفظ الجمعية بسجل لجميع عمليات الإتلاف الأمن للبيانات التي تم تنفيذها.
- ٣-٣ يجب أن تحتفظ الجمعية بالبيانات طوال المدة المحددة وفقًا للمتطلبات التشريعية والتنظيمية أو عندما تصبح البيانات الحساسة غير مطلوبة للغرض الذي جمعت من أجله.
- ٤-٣ يجب أن تُنشئ الجمعية سجل بأنشطة المعالجة وتحديثه عند الحاجة مع الاحتفاظ بنسخ طوال المدة المحددة وفقًا للمتطلبات التشريعية والتنظيمية.
- ٥-٣ يجب تحديد فترة الاحتفاظ بجميع البيانات المتعلقة بالأنظمة وفقًا للتشريعات ذات العلاقة، والاحتفاظ فقط بالبيانات المطلوبة في بيئة الإنتاج.

الالتزام بالسياسة

- ١- يجب على وحدة الشؤون الإدارية والمالية التأكد من التزام الجمعية بهذه السياسة دوريًا.
- ٢- يجب على جميع العاملين في الجمعية الالتزام بهذه السياسة.
- ٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في الجمعية.

المراجعة الدورية وتحديث السياسة

تتم مراجعة وتحديث سياسة إعادة توجيه مبلغ التبرع بشكل دوري، على الأقل مرة واحدة سنويًا، لضمان توافقها مع التغييرات القانونية والمالية. تهدف المراجعة إلى تحسين الإجراءات وضمان الالتزام بالضوابط الشرعية، بالإضافة إلى تحديث الإجراءات الخاصة بإعادة توجيه التبرعات بما يتماشى مع رغبات المتبرعين وأهداف الجمعية.



سجل الاعتمادات

الرقم	المسمى الوظيفي	الاسم	الاجراء	التوقيع	التاريخ
1	مسؤول/ أخصائي الحوكمة		إعداد		
2	مدير وحدة الشؤون الإدارية والمالية		مراجعة		
3	المسؤول التنفيذي		مراجعة ومصادقة		
4	مجلس الإدارة	- - - - - -	الاعتماد		