04 سياسات تقنية المعلومات ...

04.1 سياسة حماية البيانات
04.2 سياسة الأمن السبراني
04.3 سياسة استخدام الشبكة
04.4 سياسة خصوصية البيانات

04/1

سياسة حماية البيانات

04-1 عنوان السياسة: سياسة حماية البيانات

04/1/1 الغرض من السياسة:

تحدد سياسة حماية البيانات مدى إهتمام والتزام (المركز) بمعالجة بيانات ومعلومات موظفيه وأعضاء جمعيته العمومية وأعضاء مجلس إدارته وأعضائه المنتسبين والزوار ومعداته ومشاريعه ومقاوليه وموردیه وأصحاب المصلحة والأطراف المعنية الأخرى بأقصى درجات الحذر والسرية.

ويضمن (المركز) من خلال هذه السياسة جمع البيانات وتخزينها ومعالجتها بشكل عادل وشفاف مع مراعاة خصوصية كافة الأشخاص المتعاملين مع (المركز).

04/1/2 نطاق السياسة:

تشير هذه السياسة إلى جميع الأطراف (الموظفين والمرشحين للوظائف والأعضاء والموردين وما إلى ذلك) الذين يقدمون (للمركز) أي قدر من المعلومات.

يجب على موظفي (المركز) والجهات المتعاملة معه اتباع هذه السياسة. كما يتم تغطية المقاولين من الباطن والاستشاريين والشركاء وأي كيان خارجي آخر. بشكل عام ، تشير هذه السياسة إلى أي شخص يتعاون مع (المركز) أو يتصرف نيابة عنه وقد يحتاج إلى الوصول من حين لآخر إلى البيانات.

04/1/3 عناصر السياسة:

تتكون هذه السياسة من العناصر التالية:

أولاً: التعامل العادل مع البيانات:

يحتاج (المركز) كجزء من عملياته، إلى الحصول على المعلومات ومعالجتها. وتتضمن هذه المعلومات البيانات التي يمكن الوصول اليها بوسائل التقنية الحديثة أو عبر الإنترنت مما قد يكشف البيانات الشخصية مثل الأسماء والعناوين وأرقام الهواتف وأسماء المستخدمين وكلمات المرور والبصمات الرقمية والصور وأرقام الضمان الاجتماعي والبيانات المالية وما إلى ذلك.

يجب على (المركز) أن يحصل على مثل تلك المعلومات فقط بطريقة شفافة وبالتعاون الكامل وبالمعرفة المسبقة من الأطراف المعنية.

و بمجرد توفر هذه المعلومات لقسم تقنية المعلومات في (المركز) ، تطبق القواعد التالية:

- ينبغي أن تكون البيانات دقيقة ومحدثة؛
- يجب جمع البيانات بشكل عادل ولأغراض نظامية ومبررة فقط؛
- يجب معالجة البيانات من قبل (المركز) ضمن الحدود القانونية والأخلاقية؛
- يجب حماية البيانات ضد أي وصول غير مصرح به أو غير قانوني من قبل أي طرف من داخل أو خارج (المركز).

ثانياً: سوء استخدام البيانات:

للحيلولة دون اساءة استخدام البيانات، يلتزم (المركز) بما يلي:

- عدم السماح بالوصول إلى البيانات بشكل غير رسمي؛
- عدم تخزين البيانات لأكثر من فترة زمنية محددة؛
- عدم نقل البيانات (إلكترونيًا أو غير ذلك) إلى كيانات أو أفراد غير مصرح لهم (باستثناء الطلبات المشروعة من السلطات القانونية)؛
- السماح للأشخاص بمعرفة البيانات التي يتم جمعها عنهم؛
- اتخاذ الإجراءات المناسبة في حالات فقدان البيانات أو تلفها أو تعرضها للخطر.

ثالثاً: حماية البيانات:

لضمان حماية البيانات، يلتزم (المركز) بما يلي:

- تقييد ومراقبة الوصول إلى البيانات الحساسة؛
- وضع إجراءات شفافة لجمع البيانات؛
- تدريب الموظفين على إجراءات الخصوصية والأمن على الإنترنت؛
- أنشاء شبكات آمنة لحماية البيانات عبر الإنترنت من الهجمات السيبرانية؛
- وضع إجراءات واضحة للإبلاغ عن انتهاكات الخصوصية أو إساءة استخدام البيانات؛
- تضمين العقود المبرمة مع المركز بما يفيد كيفية تعامل (المركز) مع البيانات؛
- وضع ممارسات حماية البيانات (تمزيق المستندات ، وتأمينات آمنة ، وتشفير البيانات، والنسخ الاحتياطي المتكرر ، وتفويض الوصول وما إلى ذلك)؛
- إظهار أحكام حماية البيانات الخاصة بوضوح على الموقع الإلكتروني الرسمي (للمركز).
- يلتزم المركز بإنشاء قناة رسمية للإبلاغ عن أي خرق لسياسة حماية البيانات عبر قسم تقنية المعلومات أو لجنة التدقيق.
- يتم الاحتفاظ بالبيانات لمدة لا تتجاوز (خمس سنوات) أو حسب ما تقتضيه الأنظمة السارية.
- تتم مراجعة هذه السياسة بشكل سنوي للتأكد من ملاءمتها مع التغيرات التقنية والقانونية.

04/1/4 العواقب التأديبية لعدم الالتزام بسياسة حماية البيانات:

سيتبع (المركز) جميع المبادئ الموضحة في هذه السياسة بدقة. وسيؤدي انتهاك إرشادات حماية البيانات إلى اتخاذ إجراءات تأديبية وربما قانونية ضد المخالفين.

نهاية سياسة حماية البيانات

04/2

سياسة الأمن السيبراني

04-2 عنوان السياسة: سياسة الأمن السيبراني

04/2/1 الغرض من السياسة:

يمكن أن تسبب الأخطاء البشرية وهجمات القرصنة الإلكترونية وأعطال النظام، أضرار مالية كبيرة وقد تعرض سمعة (المركز) والمسؤولين فيه للخطر؛

توضح سياسة الأمن السيبراني في (المركز) المبادئ التوجيهية والأحكام الخاصة بالحفاظ على أمان البنية التحتية للبيانات والمعلومات المرتبطة بها.

سوف ينفذ (المركز) ضمن هذه السياسة عددًا من الإجراءات الأمنية الوقائية، والتي سوف تساعد في التخفيف من المخاطر الأمنية.

04/2/2 نطاق السياسة:

تنطبق هذه السياسة على جميع موظفي (المركز) والمقاولين ومقاوليهم من الباطن والمتطوعين وأي شخص لديه إذن بالوصول الدائم أو المؤقت لأنظمة وأجهزة (المركز) الإلكترونية أو الخوادم أو المستندات والسجلات الورقية.

04/2/3 عناصر السياسة:

تتكون هذه السياسة من العناصر التالية:

أولاً: حماية البيانات:

تعتبر بعض البيانات الخاصة سرية وقيمة، ومن ذلك:

- كافة المعلومات المالية غير المنشورة؛
- الخطط والبرامج غير المعلنة؛
- بيانات المؤسسون / أعضاء مجلس الإدارة / الشركاء / المستأجرون / المتطوعون؛
- براءات الاختراع أو الصيغ أو التقنيات الجديدة؛
- قوائم المشتركين الحاليين والمحتملين من الأعضاء.

وبموجب هذه السياسة، يلتزم جميع الموظفين بحماية تلك البيانات، وسوف يقدم (المركز) لموظفيه تعليمات واضحة والتدريب اللازم حول كيفية الحماية وتجنب الخروقات الأمنية.

ثانياً: حماية الخوادم:

تعتبر الخوادم من أهم الأجهزة التي تحتوي على البيانات والمعلومات الخاصة (بالمركز)، ولا يسمح على الإطلاق الوصول لهذه الخوادم لغير الموظفين المصرح لهم من قبل إدارة (المركز) ومقاول الصيانة المرتبط بعقد تشغيل وصيانة أو عقد ترقية الأنظمة.

- الخوادم محمية في غرفة خاصة تتوفرفيها كل المواصفات الفنية المطلوبة.
- كما تتوفر لدى (المركز) أجهزة التسجيل والدعم (Backup).

ثالثاً: حماية الأجهزة:

عندما يستخدم الموظفون أجهزتهم الرقمية للوصول إلى رسائل البريد الإلكتروني أو الحسابات الخاصة (بالمركز) ، فإنهم يعرضون بيانات (المركز) لمخاطر أمنية. وعلى موظفي (المركز) الحفاظ على أمان أجهزة الكمبيوتر الشخصية والأجهزة اللوحية والهواتف الخلوية الصادرة عنهم من خلال الالتزام بالقواعد البسيطة التالية:

- الحفاظ على حماية جميع كلمات المرور؛
- عدم ترك الأجهزة مكشوفة أو غير مراقبة؛
- اختيار وترقية البرامج المعروفة ذات السمعة الجيدة لمكافحة الفيروسات؛
- تثبيت التحديثات الأمنية للمتصفحات والأنظمة شهريًا أو بمجرد توفر التحديثات؛
- تجنب الوصول إلى أنظمة وحسابات (المركز) الداخلية من أجهزة الأشخاص الآخرين؛
- عدم إقراض الأجهزة الخاصة بموظفي (المركز) للآخرين؛
- اتباع التعليمات الصادرة لحماية الأجهزة والرجوع إلى قسم تقنية المعلومات لحل المشاكل الفنية وعدم محاولة حل المشاكل التقنية بواسطة غرباء عن (المركز).

رابعاً: حماية البريد الإلكتروني:

غالباً ما تتسرب عبر رسائل البريد الإلكتروني ما يعرف بالرسائل المؤذية (Spam) والتي تحمل فيروسات إلكترونية ضارة، ولتجنب الإصابة بالفيروسات أو سرقة البيانات، على موظفي (المركز) الإلتزام بما يلى:

- تجنب فتح المرفقات والنقر على الروابط عندما لا يتم شرح المحتوى بشكل كافٍ (على سبيل المثال، "شاهد هذا الفيديو ، إنه مذهل")؛
- عدم الانجذاب إلى العناوين البراقة (على سبيل المثال ، تقديم الجوائز والمشورة)؛
- التحقق من البريد الإلكتروني وأسماء الأشخاص الذين تصل منهم الرسائل؛
- التريث عند استلام رسالة تتضمن أخطاء نحوية، أو أحرف كبيرة، أو عدد غير طبيعي من علامات التعجب والاستفهام.

إذا لم يكن الموظف متأكدًا من أن البريد الإلكتروني الذي استلمه آمن ، فيمكنه طلب المساعدة من قسم تقنية المعلومات في (المركز).

خامساً: حماية كلمات المرور:

يعد تسرب كلمة المرور أمرًا خطيراً نظراً لأنه يمكن أن يعرض البنية التحتية بالكامل للخطر. ولا يكفي أن تكون كلمات المرور آمنة فحسب ، ولكن يجب أن تظل أيضًا سرية. لهذا السبب ، على موظفي (المركز) اتباع ما يلي لحماية كلمات المرور الخاصة بهم:

- اختيار كلمات مرور تتكون من ثمانية أحرف على الأقل (بما في ذلك الأحرف الكبيرة والصغيرة والأرقام والرموز) وتجنب المعلومات الواضحة مثل أعياد الميلاد أو الذكرى السنوية؛
- تذكر كلمات المرور بدلاً من تدوينها. إذا احتاج الموظفون إلى كتابة كلمات المرور الخاصة بهم ، فإنهم ملزمون بالحفاظ على سرية المستند الورقي أو الرقمي وتدميره عند الانتهاء؛
- تغيير كلمات المرور كل شهرين.

يمكن أن يكون تذكر عدد كبير من كلمات المرور أمرًا شاقًا. إذا قرر قسم تقنية المعلومات شراء جهاز لإدارة كلمات المرور، والذي يقوم بإنشاء كلمات المرور وتخزينها. يلتزم الموظفون بإنشاء كلمة مرور آمنة للجهاز نفسه.

التواصل عن بعد:

يجب على الموظفين الين يتواصلون عن بعد اتباع تعليمات هذه السياسة أيضًا. نظرًا لأنهم سيصلون إلى حسابات وأنظمة (المركز) عن بُعد ، وبالتالي فهم ملزمون باتباع جميع وسائل تشفير البيانات، ومعايير الحماية وإعداداتها، وضمان أمان شبكاتهم الخاصة. وعلى المستخدمين عن بُعد طلب المشورة من قسم تقنية المعلومات في (المركز) قبل أن يبدأوا التواصل عن بعد.

سادساً: نقل البيانات:

عادة ما يرافق نقل البيانات مخاطر أمنية، وبالتاي يجب على موظفي (المركز) مراعاة ما يلي:

- تجنب نقل البيانات الحساسة (مثل معلومات العملاء وسجلات الموظفين) إلى أجهزة أو حسابات أخرى ما لم يكن ذلك ضروريًا. للنقل الجماعي للبيانات، يجب على الموظفين سؤال قسم تقنية المعلومات؛
- مشاركة البيانات السرية عبر شبكة (المركز) / النظام وليس عبر شبكة Wi-Fi عامة أو عبر اتصال خاص؛
- التأكد من أن مستلمي البيانات هم أشخاص أو منظمات مفوضين بشكل صحيح ولديهم سياسات أمنية كافية؛
- الإبلاغ عن عمليات الاحتيال وانتهاكات الخصوصية ومحاولات القرصنة

يحتاج موظفو قسم تقنية المعلومات لدى (المركز) إلى معرفة عمليات الاحتيال والانتهاكات والبرامج الضارة حتى يتمكنوا من حماية البنية الأساسية بشكل أفضل. لهذا السبب ، يتعين على الموظفين الإبلاغ عن الهجمات الملموسة أو رسائل البريد الإلكتروني المشبوهة أو محاولات الاحتيال في أقرب وقت ممكن إلى قسم تقنية المعلومات في (المركز) والذي يجب عليه التحقيق على الفور وحل المشكلة وإرسال تنبيه على مستوى (المركز) عند الضرورة.

سابعاً: الإجراءات الإضافية:

إجراءات من قبل جميع موظفي المركز

- إيقاف تشغيل الشاشات وقفل الأجهزة عند مغادرة المكاتب؛
- الإبلاغ عن المعدات المسروقة أو التالفة في أسرع وقت إلى قسم الموارد البشرية؛
- تغيير جميع كلمات مرور الحساب مرة واحدة عند سرقة الجهاز؛
- الإبلاغ عن أي تهديد محتمل أو ضعف أمني محتمل على الفور؛
- الامتناع عن تنزيل برامج مشبوهة أو غير مصرح بها أو غير قانونية؛
- تجنب الوصول إلى المواقع المشبوهة؛
- الامتثال لسياسة استخدام الإنترنت لدى (المركز).

إجراءات من قبل إدارة تقنية المعلومات بالمركز

- تثبيت جدران الحماية وبرامج مكافحة البرامج الضارة وحماية أنظمة الوصول؛
- التدريب الأمني لجميع الموظفين؛
- إبلاغ الموظفين بانتظام عن رسائل البريد الإلكتروني الجديدة أو الفيروسات وطرق مكافحتها؛
- التحقق من الخروقات الأمنية بدقة؛
- اتباع جميع أحكام سياسة الأمن السيبراني مثل بقية الموظفين الآخرين.

إجراءات من قبل إدارة المركز

- تمكين قسم تقنية المعلومات من الحصول على جميع البرامج والتطبيقات اللازمة لحماية المعلومات.
- إشعار الجميع وبصفة مستمرة، من الأعضاء والشركاء والموظفين والمقاولين، بأن بياناتهم آمنة، وأن الطريقة الوحيدة لكسب ثقتهم هي اتخاذ الإجراءات الاستباقية اللازمة.
- تتم مراجعة هذه السياسة بشكل دوري للتأكد من توافقها مع أنظمة الهيئة الوطنية للأمن السيبراني (NCA) والمعايير الدولية(ISO 27001)

04/2/4 عواقب عدم الالتزام بسياسة الأمن السيبراني:

على جميع موظفي (المركز) اتباع هذه السياسة بمنتهى المسؤولية، وسوف تدرس إدارة (المركز) كل مخالفة على حدة لمعرفة مدى خطورتها، وقد يواجه أولئك الذين يتسببون في خروقات أمنية إجراءات تأديبية قاسية:

- المرة الأولى، خرق أمني صغير غير مقصود: يجوز للمركز إصدار تحذير شفهي وتدريب الموظف على الأمن.
- الانتهاكات المتعمدة أو المتكررة أو واسعة النطاق (التي تتسبب في أضرار مالية أو غيرها من الضرر الشديد): ستستدعي إجراءات تأديبية أكثر شدة قد تصل إلى إنهاء عقد الموظف.
- بالإضافة إلى ذلك، سيواجه الموظفون الذين يتجاهلون تعليمات الأمان في (المركز) إشعارات الإنذار التدريجي، حتى لو لم ينتج عن سلوكهم خرق أمني.

نهاية سياسة الأمن السيبراني

04/3

سياسة استخدام الشبكة

04-3 عنوان السياسة: سياسة استخدام الشبكة

04/3/1 الغرض من السياسة:

تحدد سياسة استخدام الإنترنت والإنترانت إرشادات لموظفي (المركز) لاستخدام الاتصال الداخلي بالمركز وبالمعدات وبشبكة الإنترنت. وتحرص الإدارة على تجنب استخدام الإنترنت غير اللائق أو غير القانوني الذي يخلق مخاطر على صعيد خصوصية البيانات وعلى سمعة (المركز).

04/3/2 نطاق السياسة:

تنطبق هذه السياسة على جميع موظفي (المركز) والمقاولين ومقاوليهم من الباطن والمتطوعين وأي شخص لديه إذن بالوصول الدائم أو المؤقت لأنظمة وأجهزة المركز الإلكترونية.

04/3/3 عناصر السياسة:

تتكون هذه السياسة من العناصر التالية:

أولاً: الاستخدام اللائق للشبكة:

لا ترغب إدارة (المركز) في تقييد وصول موظفيها إلى مواقع الويب التي يختارونها، ولكنها تتوقع من الموظفين ممارسة المهنية العالية أثناء استخدام الإنترنت وحصر استخدام اتصالات الإنترنت / إنترانت الخاصة (بالمركز) للأغراض التالية:

- إكمال واجباتهم الوظيفية؛
- البحث عن المعلومات التي يمكنهم استخدامها لتحسين عملهم؛
- للوصول إلى حساباتهم على وسائل التواصل الاجتماعي، مع الالتزام بسياسات (المركز).

يجب استخدام شبكة واتصالات المركز مع ضمان حماية البيانات، وبالتالي على الموظفين:

- الحفاظ على سرية كلمات المرور الخاصة بهم في جميع الأوقات؛
- تسجيل الدخول إلى حسابات (المركز) الخاصة بهم فقط من الأجهزة الآمنة؛
- استخدم كلمات مرور قوية لتسجيل الدخول إلى مواقع الويب والخدمات المرتبطة بالعمل.

ثانياً: الاستخدام غير اللائق للشبكة:

يجب على الموظفين عدم استخدام شبكات (المركز) للقيام بأي مما يلي:

- إرسال معلومات سرية إلى جهات غير مصرح لها؛
- إختراق خصوصية شخص آخر والوصول لمعلوماته الحساسة؛
- زيارة مواقع الويب التي يحتمل أن تكون خطرة والتي يمكن أن تعرض سلامة شبكة (المركز) وأجهزة الكمبيوتر التابعةله للخطر؛
- القيام بأعمال غير مصرح بها أو غير قانونية، مثل القرصنة والاحتيال وشراء / بيع السلع غير القانونية وما شابه ذلك.

سوف لن تكون إدارة (المركز) مسؤولة عن أي تلف للبيانات الشخصية أو إصابة أجهزة الموظفين بسبب البرامج الضارة الناتجة عن الاستخدام غير اللائق للشبكة من قبل الموظفين.

ثالثاً: البرمجيات والوسائط الإلكترونية:

تمنع إدارة (المركز) بشكل صارم موظفيها من استخدام شبكة (المركز) لتنزيل أو تحميل أي مما يلي:

- مواد فاحشة أو مسيئة أو غير قانونية؛
- الصور أو الأفلام أو الموسيقى أو المواد المحمية بحقوق النشر؛
- البرامج أو التطبيقات المحمية بحقوق الطبع والنشر؛
- تطبيقات برمجيات التجارب المجانية؛
- برنامج مكافحة الفيروسات وتشفير القرص.

على موظفي (المركز) توخي الحذر عند تنزيل وفتح / تنفيذ أي ملف أو برنامج، وإذا كانوا غير متأكدين مما إذا كان الملف أو البرنامج آمناً، فعليهم الاستعانة بإدارة تقنية المعلومات (بالمركز). ويكون لقسم تقنية المعلومات بالمركز الصلاحية الحصرية لتثبيت برامج مكافحة الفيروسات وتشفير القرص الصلب على أجهزة الكمبيوتر التابعة (للمركز)، ولا يجوز للموظفين إلغاء تنشيط أو تكوين الإعدادات وجدران الحماية بدون موافقة كتابية من مدير تقنية المعلومات.

رابعاً: البريد الإلكتروني:

يمكن للموظفين استخدام حسابات البريد الإلكتروني الخاصة بهم والتابعة (للمركز)للأغراض الشخصية والعملية على حد سواء طالما أنهم لا ينتهكون قواعد هذه السياسة. ومع ذلك ، لا يجب على الموظفين استخدام البريد الإلكتروني التابع (للمركز) من أجل:

- تسجيل الدخول لمواقع وخدمات غير قانونية أو غير آمنة أو مشكوك فيها أو مشبوهة؛
- إرسال رسائل ومحتويات فاحشة أو مسيئة أو عنصرية؛
- إرسال إعلانات غير مصرح بها أو رسائل بريد إلكتروني لطلب العروض الخاصة؛
- تسجيل الدخول لمصلحة منافس للمركز ما لم يأذن بذلك.
- يلتزم المركز بأن تكون مراقبة الشبكة في حدود ما تقتضيه متطلبات العمل والأمن فقط، مع احترام خصوصية الموظفين.
- تتم توعية الموظفين بشكل دوري بسياسة الاستخدام الأمثل للشبكة وأمثلة عملية على الممارسات الممنوعة.
- تتم مراجعة هذه السياسة بشكل سنوي لتقييم فعاليتها وتحديثها عند الحاجة.

خامساً: الأجهزة والملحقات الإلكترونية:

- على الموظفين احترام وحماية معدات (المركز)، والتي تشمل الهواتف وأجهزة الكمبيوتر المحمولة والأجهزة الطرفية واللوحية وأية معدات إلكترونية أخرى مملوكة (للمركز).
- الموظفون مسؤولون عن المعدات الموجودة في عهدتهم كلما أخرجوها من مكاتبهم.
- على الموظفين قفل أجهزتهم الإلكترونية في مكاتبهم عندما لا يستخدمونها.
- لا يسمح (المركز) باستخدام ألأقراص المدمجة وأقراص الفلاش على أجهزتهم.

04/3/4 عواقب عدم الالتزام بسياسة استخدام الشبكة:

يحق (للمركز) مراقبة رسائل البريد الإلكتروني الصادرة والواردة للموظفين عبر الحساب الخاص (بالمركز). كما لديه الحق في مراقبة مواقع الويب التي يزورها الموظفون على أجهزة الكمبيوتر التابعة (للمركز) وسيواجه الموظفون الذين لا يلتزمون بهذه السياسة إجراءات تأديبية. وقد تكون الانتهاكات خطيرة بحيث تؤدي إلى إنهاء عقد الموظف، أو اتخاذ إجراء قانوني عند الاقتضاء.

نهاية سياسة استخدام الشبكة

04/4

سياسة خصوصية البيانات

04-4 عنوان السياسة: سياسة خصوصية البيانات

04/4/1 الغرض من السياسة:

توجب سياسة خصوصية البيانات على كل من يعمل لصالح (المركز)، ويشمل ذلك أعضاء مجلس الإدارة والمسؤولين التنفيذيين والموظفين والمستشارين والمتطوعين، المحافظة على خصوصية بيانات المانحين والمتبرعين والمتطوعين والمستفيدين وعدم مشاركتها لأي أحد إلا في نطاق ضيق جداً حسب ما سيوضح في الفقرات التالية. كما توجب السياسة استخدام البيانات الخاصة لأغراض (المركز) فقط وفق ما تقتضيه المصلحة.

كما تهدف هذه السياسة إلى توضيح إجراءات التعامل مع البيانات والمحافظة على خصوصيتها داخل (المركز) أو من خلال موقع (المركز) الإلكتروني.

04/4/2 نطاق السياسة:

تطبق هذه السياسة على جميع من يعمل لصالح (المركز) سواء كانوا أعضاء في مجلس الإدارة أو مسؤولين تنفيذيين أو موظفين أو متطوعين أو مستشارين بصرف النظر عن مناصبهم في (المركز).

04/4/3 عناصر السياسة:

تتكون هذه السياسة من العناصر التالية:

أولاً: البيانات:

وتشمل أي بيانات عامة أو خاصة مثل البيانات الشخصية أو البريد الإلكتروني أو المراسلات أو أي بيانات أخرى تُقدَّم (للمركز) سواء من المتطوعين، المانحين، المتبرعين أو المستفيدين من خدمات (المركز):

ثانياً: بيانات المتعاملين مع المركز:

يضمن (المركز) ما يلي:

- نشر سياسة (المركز) خصوصية البيانات على موقعه الإلكتروني، وأن تكون متوفرة عند الطلب مطبوعة أو إلكترونية.
- الإعلان عن سياسة (المركز) الخاصة بخصوصية بيانات متصفحي موقعه الإلكتروني.
- التعامل مع جميع بيانات المتعاملين معه بسرية تامة وعدم التصرف ببيانات المتعاملين معه سواء بالنشر أو بالهبة أو بالمشاركة أو بالبيع مع أي جهة أخرى دون إذنهم.
- عدم إرسال رسائل نصية تسويقية للمتعاملين معه سواء بواسطته أو بواسطة أي جهة اخرى دون إذنهم.

ثالثاً: بيانات زوار الموقع الإلكتروني:

يضمن (المركز) ما يلي:

- انتهاج سياسة خاصة بالتعامل مع بيانات زوار ومتصفحي الموقع الإلكتروني (للمركز).
- الإعلان عن سياسة (المركز) الخاصة بخصوصية بيانات متصفحي الموقع الإلكتروني (للمركز).
- عدم الترويج لأي حملات تجارية لأية جهة كانت على موقع (المركز) الإلكتروني.

رابعاً: نموذج الرسالة الموجهة إلى متصفحي موقع المركز الإلكتروني:

نشكر الزائرين لزيارتهم موقعنا على الانترنت ونتعهد لهم بالمحافظة على خصوصية بياناتهم التى يزودونا بها من خلال الموقع. كما نلتزم بتوضيح سياستنا المتعلقة بخصوصية البيانات الشخصية:

التزامات مركز الملك سلمان الاجتماعي:

- حماية حقوق جميع زوار ومستخدمي الموقع الإلكتروني والحفاظ على سرية بياناتهم على هذا الموقع.
- عدم استخدام تلك البيانات إلا بالطريقة الملائمة للحفاظ على خصوصية المستخدمين بشكل آمن.
- عدم السماح بتبادل البيانات الشخصية مع أي جهة تجارية باستثناء ما يتم الإعلان عنه للمستخدم وبعد موافقته على ذلك.
- عدم السماح باستخدام بيانات المستخدمين بإرسال رسائل ذات محتوى تجاري أو ترويجي.
- حصر استخدام البيانات المسجلة فى الموقع لعمل الاستبانات وأخذ الآراء بهدف تطوير الموقع وتقديم تجربة استخدام أكثر سهولة وفعالية للزوار والمستخدمين.
- عدم مشاركة هذه البيانات مع أطراف خارجية إلا إذا كانت هذه الجهات لازمة فى عملية استكمال طلب يقدمه المستخدم، ما لم يكن ذلك في إطار بيانات جماعية تُستخدم للأغراض الإحصائية والأبحاث، دون اشتمالها على أية بيانات من الممكن استخدامها للتعريف علىلا هوية المستخدم.

التعامل مع البيانات في الحالات الطبيعية:

- فى الحالات الطبيعية يتمُّ التعامل مع البيانات بصورة آلية (الكترونية) من خلال التطبيقات والبرامج المحدَّدة لذلك، دون أن يستلزم ذلك مشاركة الموظفين أو إطلاعهم على تلك البيانات.
- تنطبق سياسة الخصوصية هذه على كافّة الخدمات والتعاملات التى يتم إجراؤها على الموقع إلا فى الحالات التي يتمُّ فيها النصُّ على خدمات أو تعاملات ذات خصوصية؛ فإنه يكون لها سياسةُ خصوصية منفصلة، وغير مدمجة بسياسة الخصوصية هذه.

التعامل مع البيانات في الحالات الاستثنائية:

- في حالات استثنائية (كالتحقيقات والقضايا) قد يطّلع عليها موظفو الجهات الرقابية أو من يلزم اطلاعه على ذلك؛ خضوعًا لأحكام القانون وأوامر الجهات القضائية
- قد يحتوي هذا الموقع على روابط لمواقع إلكترونية أخرى تقع خارج سيطرة (المركز)، ولا تغطيها سياسة الخصوصية هذه.
- في حال تم الوصول إلى مواقع أخرى من خلال استخدام الروابط المتاحة على موقعنا؛ فإن المستخدم سوف يخضع لسياسة الخصوصية المتعلّقة بتلك المواقع، والتي قد تختلف عن سياسة موقع المركز؛ مما يتطلب من المستخدم قراءة سياسة الخصوصية المتعلّقة بتلك المواقع.

استخدام مركز الملك سلمان الاجتماعي للبيانات:

- للحفاظ على بيانات المستخدمين الشخصية، يتم تأمين التخزين الإلكتروني والبيانات الشخصية المرسلة باستخدام التقنيات الأمنة المناسبة.
- يمكن لمركز الملك سلمان الاجتماعي استخدام البيانات الشخصية للتواصل مع المستخدمين عند الحاجة في حالة رغبتهم بالتبرُّع للمشاريع والأعمال الخيرية أو رغبتهم في الاطلاع على ما يستجد من المشاريع والأعمال الخيرية التي يقوم بها المركز حيث تساعد هذه البيانات في التواصل معهم، والإجابة عن استفساراتهم، وتنفيذ طلباتهم قدر الإمكان.
- في كل الأحوال لن يقوم مركز الملك سلمان الاجتماعي بالبيع أو التأجير أو المتاجرة ببيانات المستخدمين أو الإفصاح عنها لمصلحة أي طرف ثالث خارج هذا الموقع. وسنحافظ في كافّة الأوقات على خصوصية كافة بيانات المستخدمين الشخصية التي يتحصل عليها وسريتها.
- نظرًا للتطوُّر الهائل في مجال التقنية، والتغيُّر في نطاق القوانين المتعلقة بالمجال الإلكتروني؛ فالموقع يحتفظ بالحقِّ في تعديل بنود سياسة الخصوصية هذه وشروطها في أي وقتٍ يراه ملائماً، ويتم تنفيذ التعديلات على هذه الصفحة، ويتم إخطار المستخدمين في حالة إجراء أية تعديلات ذات تأثير.
- سوف تخضع أي مخالفة لسياسة خصوصية البيانات للإجراءات التأديبية وفق لوائح (المركز) والأنظمة السارية.
- تراجع هذه السياسة بشكل دوري للتأكد من توافقها مع التطورات والأنظمة ذات العلاقة.
- تعتبر هذه السياسة مكملة لسياسة حماية البيانات وسياسة الأمن السيبراني المعتمدة في (المركز).

نهاية سياسة خصوصية البيانات