المركز الوطني للإحصاء والمعلومات
تعزيز المعرفة
سلطنة عُمان

تعداد 2020
التعداد الإلكتروني للسكان والمساكن والمنشآت
Electronic Census of Population, Housings and Establishments

رؤية عُمان 2040
Oman Vision

إدارة أمن المعلومات للتعداد الإلكتروني للسكان والمساكن والمنشآت 2020

سلسلة وثائق التعداد الإلكتروني 2020
03

صاحب الجلالة السلطان هيثم بن طارق المعظم

حفظه الله ورعاه

يعتمد نتائج التعداد الإلكتروني للسكان والمساكن والمنشآت 2020، وفق التاريخ المرجعي 12 ديسمبر 2020م. معربا جلالته عن ارتياحه للنجاح الذي حققه مشروع التعداد وإنجازه وفق ما هو مخطط له، مؤكداً - أعزه الله - على أهمية البيانات والمؤشرات التي توفرها نتائج التعداد في رفد رؤية عُمان 2040، والتخطيط للتنمية في كافة القطاعات بالسلطنة.

14 ديسمبر 2020

المحتويات	الصفحة
المقدمة	7
1. سياسة أمن المعلومات	8
1.1. الغرض	8
1.2 النطاق	8
1.3. السياسة	9
1.4.المسؤوليات	12
1.5 انتهاك	15
1.6 المسؤولية	15
2. سياسة الاستخدام المقبول	16
2.1. الغرض	16
2.2. النطاق	16
2.3 السياسة	16
3. سياسة التوعية الأمنية	17
3.1. الغرض	17
3.2. النطاق	17
3.3. السياسة	17
3.4. انتهاك	17
3.5. المسؤول	17
الخاتمة	18

المقدمة

اعتمد التعداد الإلكتروني 2020 في منهجيتة على السجلات الإدارية الإلكترونية ، والتي يتم من خلالها جمع البيانات الخاصة بالسكان والمساكن والمنشآت. و تعد هذه المعلومات والبيانات سرية ويحظر تداولها أو نشرها إلا بصورة تجميعية ولأغراض الإحصاء فقط وذلك وفقا لقانون الإحصاء الصادر بالمرسوم السلطاني السامي رقم 29 /2001.

ومن أجل حماية هذه البيانات تم اعداد وثيقة لأمن المعلومات في مشروع التعداد الإلكتروني توضح آلية إدارة أمن المعلومات وآلية جمع واستخدام وحفظ المعلومات التي يتم تجميعها من المؤسسات الحكومية والخاصة والجهات الأخرى عن الأفراد والمساكن والمنشآت، مع ضمان توافر هذه المعلومات إلى الأشخاص المخولين بالتعامل مع هذه البيانات والمعلومات.

وقد تم اعداد هذه الوثيقة مع مراعاة توافقها مع القانون الإحصائي الصادر بالمرسوم السلطاني (29 /2001)، وقانون تصنيف وثائق الدولة وتنظيم الأماكن المحمية، الصادر بالمرسوم السلطاني رقم 118/ 2011م، وقانون المعاملات الإلكترونية الصادر بالمرسوم السلطاني رقم (69 /2008) ويتبع الممارسة الجيدة، وقانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني 12 /2011 والمرسوم السلطاني رقم (15 /2015) الخاص بإجراء التعداد الإلكتروني للسكان والمساكن والمنشآت لعام 2020م وسياسة أمن المعلومات لهيئة تقنية المعلومات.

وتتناول هذه الوثيقة سياسة أمن المعلومات والتي تحدد السياسة التي وضعتها إدارة المشروع والأسس الإدارية لأمن المعلومات في مشروع التعداد الإلكتروني 2020 وكذلك سياسة الاستخدام المقبول والتي تحدد الممارسات المقبولة المتعلقة باستخدام موارد المعلومات في مشروع التعداد الإلكتروني 2020 التي تشمل على سبيل المثال لا الحصر، البيانات، المعدات الحاسوبية، البرامج، خدمات الشبكة، البريد الإلكتروني، الإنترنت / الإنترانت ووسائط التخزين و تحتوي هذه السياسة على الحد الأدنى الذي يجب على كل موظف معرفته بالإضافة الى السياسة التوعية الأمنية التي تُعلم الموظفين بأن أمن المعلومات مسؤولية الجميع وأن الجميع مطالبون بالتعرف على أمن المعلومات وحضور الأحداث / التدريبات / ورش العمل المتعلقة بأمن المعلومات.

1 | سياسة أمن المعلومات

1.1. الغرض

الغرض من هذه السياسة هو:

- إدارة التوجيه والدعم والالتزام بسياسة أمن المعلومات في مشروع التعداد الإلكتروني 2020.
- إبلاغ جميع موظفي مشروع التعداد الإلكتروني 2020 المتعاقدين والفرق التابعة للمشروع في المؤسسات الحكومية والخاصة والأشخاص المرتبطين بأعمال مع المشروع عن مسؤولياتهم والتزاماتهم فيما يتعلق بأمن المعلومات.
- ضمان توفر الموارد الكافية لتطبيق نظام فعال لإدارة أمن معلومات .
- تحديد وتقليل المخاطر الناجمة عن أي خلل أمني قد يتعرض له المشروع.
- ضمان استمرارية العمل في المشروع بدون انقطاع ناتج عن خلل في أمن المعلومات.

1.2 النطاق

تغطي هذه السياسة جميع أشكال المعلومات وتتضمن البيانات المخزنة على أجهزة الكمبيوتر والخوادم، أو التي يتم نقلها عبر الشبكات، أو تطبع أو تكتب على الورق، أو تُرسل بالفاكس، أو تُخزَّن على أشرطة أو أقراص، أو تسرد في محادثة أو عبر الهاتف.

المرافق: المكتب الرئيسي لمشروع التعداد الإلكتروني وجميع المباني والوحدات الواقعة في نطاق المشروع وجميع الموظفين والمتعاقدين والفرق التابعة للمشروع في المؤسسات الحكومية والخاصة وجميع الموردين والشركات والأشخاص المرتبطين بأعمال مع المشروع.

البيانات: تشمل البيانات الأولية الخام والمعالجة:

- ملفات البيانات الإلكترونية: تشمل جميع الملفات الإلكترونية بغض النظر عن وسائط التخزين الخاصة بها.
- المستندات الورقية: تشمل جميع الوثائق والمستندات الورقية.

البرامج: تشمل جميع البرامج المطورة محليًا والبرامج التي تم الحصول عليها من مصادر خارجية.

- برامج التطبيقات، وبرامج نظام التشغيل وجميع الأدوات المساعدة وبرامج الدعم المرتبطة بها.
- برامج تمكين التطبيقات بما في ذلك إدارة قواعد البيانات والبرامج الوسيطة والاتصالات السلكية واللاسلكية وبرامج الشبكات.

الموظفون: جميع الموظفين والمتعاقدين والفرق التابعة للمشروع في المؤسسات الحكومية والخاصة وجميع الموردين والشركات والأشخاص الذين يعملون في المشروع.

1.3. السياسة

سيقوم مشروع التعداد الإلكتروني 2020 بتنفيذ جميع التدابير الممكنة وذات الصلة لتحقيق الأهداف التالية: -

- **الإتاحة:** عمل ضوابط وإجراءات لضمان إمكانية الوصول إلى المعلومات للأشخاص المرخص لهم وضمان الاستعادة في حالة حدوث خلل.
- **النزاهة:** وضع ضوابط وإجراءات لضمان اكتمال ودقة المعلومات أثناء جمع المعلومات والبيانات وتخزينها ومعالجتها وعرضها والحماية من أي تعديل أو تدمير غير مصرح به.
- **الخصوصية:** وضع ضوابط وإجراءات لضمان إتاحة المعلومات أو الكشف عنها للمؤسسات أو الأفراد المصرح لهم فقط.
- **المساءلة:** وضع ضوابط وإجراءات لضمان المسؤولية عن المعلومات والإجراءات التي يتخذها مقدمو البيانات ومستخدموها.
- **التحقق من الهوية:** التأكد من هوية مستلم البيانات أو مسلم البيانات والتحقق من أنه مخول باستلام أو تسليم البيانات. كما تشمل التحقق من أي رسالة طلب بيانات مرسلة أنها رسالة حقيقية جاءت من المصدر الأصلي ولم تتعرض لأي تغيير أو تبديل.
- **عدم الإنكار:** ضمان عدم إنكار المستلم استلامه لهذه البيانات أو المعلومات، ولا بد من استخدام طريقة تثبت أن الشخص المستلم هو شخص مصرح له ويحمل توقيعه وبياناته، وكذلك بيانات الشخص المسلم لهذه البيانات.
- **الصلاحيات:** ضمان أن الصلاحيات المعطاة لأشخاص معينين مسموح لهم تداول معلومات معينة أو الحصول عليها في وقت محدد وبصلاحيات محددة من قبل المسؤول المباشر.
- **تدقيق أمن المعلومات لعمليات التسليم والتسلم:** وهي تسجيل كافة الأحداث والعمليات التي تتم بخصوص تسليم وتسلم البيانات، وتحديد حجم الملفات وأوقات التسلم والتسليم، وفحص البيانات المستلمة قبل تسليمها للمختبر للتأكد من خلوها من الملفات الخبيثة.
- **تطوير إجراءات مناسبة ومفصلة لتنفيذ الأمن** بما في ذلك توفير التوعية والتدريب في مجال أمن المعلومات للمرتبطين بمشروع التعداد الإلكتروني.
- **موارد المشروع** (بما في ذلك على سبيل المثال لا الحصر البريد الإلكتروني والإنترنت) مخصصة للاستخدام الوظيفي ويجب استخدامها لأغراض العمل فقط.

- **ملكية جميع المعلومات المخزنة أو المنقولة** عبر موارد المشروع لمشروع التعداد الإلكتروني 2020 ولها الحق في مراقبتها وتدقيقها. ويجب تحديدها وتصنيفها بالشكل المناسب.
- **توفير سياسة أمن المعلومات** يتم توفير هذه الإجراءات والمبادئ التوجيهية في المكاتب الخاصة في التعداد ولجميع العاملين في المشروع.
- **مراجعة سياسة أمن المعلومات** والسياسات الداعمة والمبادئ التوجيهية والإجراءات كل 6 أشهر.
- **مراقبة الالتزام بالسياسة** على أساس منتظم، سيتم مراقبة أصول المعلومات وآلية استخدامها.
- يجب أن يكون الوصول إلى موارد ومعلومات المشروع على أساس "المعرفة قدر الحاجة".
- ينبغي تعيين موظف/موظفي أمن المعلومات لتنسيق تنفيذ جميع السياسات الأمنية والمبادرات والمهام الأمنية ذات الصلة.
- سيضمن المسؤول عن أمن المعلومات معالجة القضايا الأمنية ووضع آلية لمنع تكرارها في المستقبل.
- عندما يتم نقل المعلومات إلى داخل أو خارج المشروع، يجب اتخاذ تدابير خاصة لتأمينها.
- يجب أن تخضع البرامج والمواقع التي يتم تطويرها أو استخدامها في مشروع التعداد الإلكتروني للحصول على موافقة أمنية مناسبة قبل الانتقال إلى بيئة العرض والاستخدام.
- يحتفظ مشروع التعداد الإلكتروني بالحق في مراقبة حركة المعلومات وجميع الاتصالات بغض النظر عن الوسيط المستخدم.
- يجب حماية شبكة المشروع بشكل مناسب باستخدام الأجهزة والبرامج المناسبة. يجب أن يتم مراقبتها والتحقق منها على أساس منتظم وإجراء فحوصات منتظمة على الشبكة والخوادم والمعدات الأخرى للتأكد من أن الشبكة آمنة.
- لتوفير الحماية ضد التهديدات المتوقعة لمشروع التعداد الإلكتروني، يجب توفير ضمانات مناسبة، بما في ذلك برامج مكافحة الفيروسات وجدران الحماية وأنظمة منع التطفل (IPS) ومتطلبات تقنية أخرى تتناسب مع حساسية وأهمية المشروع.
- استخدام الشبكة الحكومية الموحدة للتواصل بين المؤسسات الحكومية بصورة آمنة.
- يجب أن تحتوي جميع الوثائق في المشروع على رقم الإصدار مع رقم المستند ويجب ترقيم جميع الصفحات.
- يجب الإبلاغ عن جميع الحوادث الأمنية وأوجه الضعف وانتهاك أمن المعلومات الفعلية أو المشبوهة، والتحقيق فيها من قبل فريق أمن المعلومات بالمشروع.

- يمكن اتخاذ إجراءات تأديبية حسب ما تنص عليها التشريعات والقوانين التي تستند عليها هذه الوثيقة.
- يجب أن يكون لدى فريق الاستجابة لحوادث أمن المعلومات خطة موثقة للاستجابة لحالات الطوارئ تتضمن جميع الإجراءات الضرورية.
- يجب إجراء الفحص الصحيح لجميع الأنظمة على أساس منتظم بمساعدة اختبار الاختراق والأمن المادي والهندسة الاجتماعية. وينبغي إجراء تدقيق نصف سنوي لأمن المعلومات للتحقق من فعالية ضوابط التنفيذ. يتم مراجعة تقرير التدقيق من قبل الإدارة والتدابير المناسبة المتخذة لتعزيز الأمن داخل مشروع التعداد 2020 على أساس مستمر.
- الأمن المادي ذو أهمية عالية. وينبغي بذل جميع الجهود لتأمين المحيط المادي ونقاط الدخول المادية وغرف المكاتب والمختبرات وغرف السيرفرات باستخدام بطاقة الدخول وبصمة الأصبع. واتخاذ التدابير المناسبة لتأمين جميع المعدات وإمدادات الطاقة والكابلات.
- يجب ضمان تأمين المعدات والأجهزة أثناء صيانتها خارج نطاق المشروع.
- يجب على جميع موظفي المشروع وموظفي الشركات والزائرين أن يرتدوا شارات الهوية الخاصة بهم ويضمنوا أن تكون مرئية في جميع مرافق المشروع.
- ممنوع منعا باتا مناقشة المعلومات الحساسة (الفردية، السكان، المساكن، المنشآت) في الأماكن العامة. أو حتى الحديث عنها لمن ليس له علاقة داخل المشروع.
- يجب مراجعة جميع الإعلانات عن الوظائف والمناقصات بدقة، بحيث لاتكشف عن أي معلومات خارج المسموح به.
- إذا قام أحد موظفي المشروع بتقديم ورقة عمل أو تقديم عرض تقديمي أو إلقاء خطاب في منتدى أو مؤتمر عام، فيجب مراجعة جميع المواد من قبل المسؤول المباشر عنه، ومن ثم أخذ الموافقة الخطية من المدير العام لمشروع التعداد الإلكتروني.
- يجب أن يلتزم مشروع التعداد الإلكتروني بجميع المتطلبات القانونية التي حددتها حكومة سلطنة عمان ولا يجوز للموظفين الانغماس في نشاط غير قانوني بموجب القانون المحلي أو الدولي.
- يجب على جميع المعنيين ضمان الامتثال لهذه السياسة، والسياسات الأخرى المدرجة في دليل الضوابط والمعايير والإجراءات والمبادئ التوجيهية والسياسة التفصلية ذات الصلة (خارج هذا الدليل).

1.4. المسؤوليات

يتحمل كل من يعمل مع مشروع التعداد الإلكتروني 2020 المسؤولية حسب تخصصه لتنفيذ سياسة أمن معلومات بشكل فعال، بما فيها جمع البيانات وتخزينها ومعالجتها بالشكل المناسب. فعلى كل فريق يتعامل مع البيانات الشخصية ضمان التعامل معها ومعالجتها بما يتماشى مع مبادئ وسياسة حماية البيانات.

1. **يقوم المسؤول عن أمن المعلومات بضمان تطبيق المبادئ والتوجيهات والإجراءات لتنفيذ هذه السياسة،** وسيكون مسؤولاً عن مراجعة مستمرة لفعاليتها والتأكد من أن جميع الموظفين على علم تام بالتزاماتهم ومسؤوليتهم.

2. **يطلب المسؤول عن أمن المعلومات من جميع الموظفين،** سواء كانوا موظفي مشروع التعداد الإلكتروني 2020 المتعاقدين أو الفرق التابعة للمشروع في المؤسسات الحكومية والخاصة والأشخاص المرتبطين بأعمال مع المشروع أو زوار، الامتثال لسياسة أمن المعلومات.

3. **يتحمل المدراء مسؤولية الحفاظ على البيانات وأصول المعلومات الأخرى** التي تدعم أنشطة المشروع والتي تتم تحت إشرافهم لضمان تأمين تلك الأصول بشكل كافٍ. كما يجب عليهم التأكد من الالتزام بالمبادئ التوجيهية والإجراءات لأمن المعلومات في أداء هذه الأنشطة.

4. **مسؤول أمن المعلومات مسؤول عن الإدارة اليومية** لإجراءات وممارسات أمن المعلومات. ويقدم تقاريره مباشرة إلى المدير العام.

5. **مدير عام التعداد مسؤول عن ضمان تطبيق السياسة الأمنية** في المشروع.

6. **.فريق إدارة المشروع والتحليل مسؤولان عن:**

- إبقاء المدير العام على اطلاع حول مسؤوليات حماية البيانات.
- مراجعة جميع إجراءات حماية البيانات والسياسات ذات الصلة، تماشيا مع جدول زمني متفق عليه.
- ضمان جمع البيانات وتخزينها ومعالجتها بشكل مناسب.

7. فريق جمع البيانات:

- صلاحية جمع البيانات معطاة لأشخاص معينين مسموح لهم بنقل معلومات معينة أو الحصول عليها في وقت محدد وبصلاحيات محددة من قبل إدارة التعداد.
- يتم طلب البيانات اللازمة للأغراض الإحصائية الخاصة بالتعداد فقط.
- التأكد من أن جميع الأنظمة والخدمات والمعدات المستخدمة لتخزين البيانات تستوفي المعايير الأمنية المقبولة وفقا للسياسة المقترحة.
- إجراء فحوصات ومسح منتظم بالتعاون مع الفنيين المختصين لضمان عمل الأجهزة والبرامج الأمنية بشكل صحيح.
- التعاون مع الجهات المانحة بالرد على استفساراتهم في حالة وجود تساؤلات لديهم.
- يتم استلام جميع البيانات الفردية فقط من خلال البريد الإلكتروني (ecensus.data@ncsi.gov.om). على أن يتم حماية البيانات برقم سري.
- يجب على الموظفين طلب المساعدة من مديرهم المباشر إذا كانوا غير متأكدين من أي جانب من جوانب حماية البيانات.
- يشكل فريق مكون من شخصين لاستلام البيانات، ولا تسلم في حالة عدم تواجدهما معا.

8. الجهات المانحة للبيانات:

- التعامل مع الطلبات الواردة من موظفي مشروع التعداد لمعرفة البيانات أو الحصول عليها أو الحصول على الإحصائيات.
- تنبيه فريق جمع البيانات بالتحديثات والتعديلات المهمة على البيانات.
- التأكد من هوية جامع البيانات أو الطلب المرسل بالبريد الإلكتروني قبل تسليم البيانات. ويتم إرسال جميع البيانات الفردية فقط من خلال البريد الإلكتروني (ecensus.data@ncsi.gov.om). على أن يتم حماية البيانات برقم سري.
- التأكد من أن البيانات يتم نقلها على أجهزة موثوقة ومشفرة وأن يتم تشفير البيانات قبل نقلها. وألا يتم منح مستقبل البيانات كلمة السر مباشرة بل يتم إرسالها إلى البريد الإلكتروني (ecensus.data@ncsi.gov.om).
- والتحقق من أن أي رسالة طلب بيانات مرسلة هي رسالة حقيقية جاءت من المصدر الأصلي ولم يطرأ عليها أي تغيير أو تبديل.

9. مدير قاعدة البيانات السكانية ومدير قاعدة بيانات المنشآت هما المسؤولان عن:

- اقتراح أسماء الموظفين المكلفين باستلام البيانات؛ للحصول على موافقة المدير العام مع التأكيد عليهم باتخاذ كافة التدابير اللازمة لسلامة البيانات.
- تقييم خدمات أي طرف ثالث يرغب المشروع في استخدام خدماته للاطلاع على البيانات.
- التعامل مع أسئلة حماية البيانات من الموظفين وغيرهم ممن تشملهم هذه السياسة.
- المساهمة في تطبيق سياسة أمن المعلومات وحماية البيانات للأشخاص الذين تشملهم هذه السياسة.

10.مدير الإعلام مسؤول عن:

- الرد على أي استفسارات حول حماية البيانات من الصحفيين أو وسائل الإعلام مثل الصحف ووسائل التواصل الاجتماعي.
- العمل مع الموظفين الآخرين لضمان التزام مبادرات التسويق والإعلام بمبادئ حماية البيانات.
- منع تقديم أي تصريح إعلامي يخص مشروع التعداد الإلكتروني 2020 من قبل أي موظف أو متعاقد مع المشروع قبل الحصول على موافقة المدير العام.

1.5. انتهاك

في حالة انتهاك السياسة أو المبادئ التوجيهية أو الإجراءات، سيتم اتخاذ الإجراءات القانونية وفق ما تنص عليه القوانين في الدولة.

1.6. المسؤول

جميع موظفي مشروع التعداد الإلكتروني 2020 المتعاقدين والفرق التابعة للمشروع في المؤسسات الحكومية والخاصة والأشخاص المرتبطين بأعمال مع المشروع.

2 | سياسة الاستخدام المقبول

2.1.الغرض: الغرض من سياسة الاستخدام المقبول هو الإبلاغ عن الحد الأدنى الذي يجب على كل المشاركين في مشروع التعداد الإلكتروني 2020 معرفته لضمان أمن الأنظمة والأصول والمعلومات.

2.2. النطاق: يغطي نطاق هذه السياسة. جميع موظفي مشروع التعداد الإلكتروني 2020 المتعاقدين والفرق التابعة للمشروع في المؤسسات الحكومية والخاصة والأشخاص المرتبطين بأعمال مع المشروع.

2.3.السياسة:

- أمن المعلومات هي عملية مشتركة بين الجميع وهي مسؤولية الجميع يوميا. يجب على الجميع المساهمة في تطبيق سياسة الأمن الموضوعة في مشروع التعداد الإلكتروني 2020.
- موارد المشروع (على سبيل المثال: البريد الإلكتروني والإنترنت) مخصصة للاستخدام الوظيفي فقط.
- اتباع الإرشادات التي يقوم مسؤول أمن المعلومات بإصدارها من وقت لآخر.
- جميع المعلومات المخزنة أو المنقولة عبر موارد المشروع هي ملك لمشروع التعداد الإلكتروني 2020. ولمشروع التعداد الإلكتروني 2020 الحق في مراقبة استخدامها.
- يحظر نسخ أو نقل المعلومات إلا عند حاجة العمل وبترخيص مسبق من مدير عام المشروع للمعنيين فقط.
- يجب حماية جميع كلمات المرور وعبارات المرور المخصصة للموظف. ولا ينبغي له مشاركتها مع أي شخص آخر.
- يجب تغيير كلمة المرور وفقًا لسياسة كلمة المرور. ولا يجوز تركها مكتوبة في مكان يسهل الوصول إليه.
- يجب احتواء جميع أجهزة الكمبيوتر المكتبية وأجهزة الكمبيوتر المحمول على شاشة توقف محمية بكلمة مرور وتنشيطها بعد فترة لا تزيد عن 3 دقائق من عدم الاستخدام.
- التأكد من عدم وجود بيانات فردية مخزنة في جهاز الكمبيوتر المحمول والخاص بالعمل والمستخدمة خارج المختبرات، جميع البيانات الفردية تخزن في خوادم خاصة ومحمية.
- عدم السماح بتعطيل وإلغاء تنشيط محرك الكشف عن الفيروسات.
- يجب اتباع سياسة البريد الإلكتروني والإنترنت أثناء استخدام البريد الإلكتروني أو الإنترنت.
- حظر إجراء فحص ومسح المنفذ للخوادم ما لم يكن جزءًا من اختبار الاختراق الرسمي الذي يقوم به مشروع التعداد ويتم فيها اتخاذ تدابير مناسبة.
- التأكد من أن جميع معلومات الأفراد، والمساكن والمنشآت المطبوعة كنسخة ورقية أو على شكل إلكتروني محفوظة بشكل آمن.
- يمنع منعا باتا إخراج الحاسب الخاص بالمشروع خارج نطاق المشروع، كما يمنع إخراج أي احصائيات أو تقارير أو تعريفات خاصة بالمشروع دون الحصول على إذن مسبق.
- يعتبر فهم واتباع سياسة أمن المعلومات مسؤولية فردية على جميع العاملين في المشروع.

3 | سياسة التوعية الأمنية

3.1.الغرض:

الغرض من هذه السياسة هو إبقاء الموظفين على اطلاع بمتغيرات أمن المعلومات.

3.2.النطاق:

تنطبق السياسة على جميع الموظفين الدائمين/المتعاقدين المنتدبين والمستشارين والشركات الاستشارية بمشروع التعداد الإلكتروني 2020.

3.3.السياسة:

- ينظم مسؤول أمن المعلومات ورشة عمل واحدة كل 6 أشهر على الأقل وسيكون حضور كل موظف إلزامياً.
- سيتم التعريف بسياسة أمن المعلومات للتوعية الأمنية لكل موظف جديد أو شركة تنضم للعمل في نطاق المشروع من خلال "تعهد" والذي يحتاج إلى توقيع من قبل الموظف.
- تقع على عاتق كل فرد مسؤولية تثقيف نفسه وتحديث معلوماته الأمنية من خلال القراءة والمشاركة في التدريبات والورش الأمنية التي يجريها مشروع التعداد.
- يجب إبلاغ مسؤول أمن المعلومات فوراً بأي خرق أمني أو استفسار حول الأمن.
- معرفة السياسة الأمنية هي واحدة من المجالات التي سيتم من خلالها تقييم الموظف.

3.4.انتهاك:

في حالة انتهاك السياسة أو المبادئ التوجيهية أو الإجراءات، سيتم اتخاذ الإجراءات القانونية وفق ما تنص علية القوانين في الدولة.

3.5.المسؤول:

مسؤول أمن المعلومات، مدقق أمن المعلومات (داخليا وخارجيا).

الخاتمة

يشير أمن المعلومات الذي يُرمز إليه غالبًا بـ(InfoSec) إلى العمليات والأدوات المصممة والمستخدمة لحماية كافة المعلومات بأنواعها، وهي عملية مشتركة بين الجميع ومسؤولية الجميع يوميا، لذا وجب على الجميع المساهمة في تطبيق سياسة الأمن التي وضعتها إدارة مشروع التعداد الإلكتروني متمثلة في تحديد الأسس الإدارية والدعم والتزام مبادرات أمن المعلومات في مشروع التعداد الإلكتروني 2020، كما تحدد هذه السياسة الممارسات المقبولة المتعلقة باستخدام موارد معلومات مشروع التعداد الإلكتروني 2020 التي تشمل على سبيل المثال لا الحصر، البيانات، المعدات الحاسوبية، البرامج، خدمات الشبكة، البريد الإلكتروني، الإنترنت / الإنترانت ووسائط التخزين، إضافة الى ذلك تحتوي هذه السياسة على الحد الأدنى الذي يجب على كل موظف معرفته، وتُعلم هذه السياسة الموظفين بأن أمن المعلومات مسؤولية الجميع وأن الجميع مطالبون بالتعرف على أمن المعلومات وحضور الأحداث / التدريبات / ورش العمل المتعلقة بأمن المعلومات.

ومن خلال كافة العمليات الإحصائية والمعالجات التي تمت في المختبرات والأدوار التي قامت بها كافة اللجان والفرق فقد أتت السياسة الأمنية التي وضعتها إدارة المشروع نتائجها بدقة عالية من خلال المحافظة على سرية البيانات والمعلومات، والتأكد من أن جميع الأنظمة والخدمات والمعدات المستخدمة لتخزين البيانات تستوفي المعايير الأمنية المقبولة وفقا للسياسة المقترحة، ولضمان الحماية ضد التهديدات المتوقعة لمشروع التعداد الإلكتروني، وتوفير الضمانات المناسبة، بما في ذلك برامج مكافحة الفيروسات وجدران الحماية وأنظمة منع التطفل (IPS) ومتطلبات تقنية أخرى تتناسب مع حساسية وأهمية المشروع.

سلسلة وثائق التعداد الإلكتروني 2020