جمعية مراكز الاحياء

بمنطقة مكة المكرمة

# دليل سياسات وإجراءات تقنية المعلومات

**تاريخ الإصدار ٥ يناير ٢٠١٥**

**النسخة النهائية**

## المحتويات


- جدول اعتماد الدليل ..... ٦
- ١.١ الغرض والأهداف من الدليل ..... ٧
- ٢.١ استخدام الدليل ..... ٧
- ٣,١ مراقب الدليل ..... ٨
- ٤,١ حق الاطلاع على الدليل ..... ٨
- ٥,١ الموافقة على الدليل ..... ٨
- ٦,١ تنفيذ الدليل ..... ٨
- ٧,١ تعزيز الدليل ..... ٨
- ٨,١ الانحراف عن السياسات والإجراءات ..... ٩
- ٩,١ نطاق الدليل ..... ٩
- ١٠,١ صيانة الدليل وتكرار معدل المراجعة ..... ٩
- ١١,١ إجراءات التحديث ..... ١٠
- ١٢.١ سجل مراقبة عمليات التحديث ..... ١١
- ١٣,١ حقوق التأليف والنشر ..... ١١
- ١٤,١ عام ..... ١٢
- ١٥.١ الهيكل التنظيمي لإدارة تقنية المعلومات ..... ١٣
- ٢. سياسة التخطيط الاستراتيجي لتقنية المعلومات ..... ١٦
- ١,٢ المقدمة والأهداف ..... ١٦
- ٢,٢ السياسات ..... ١٦
- ٣,٢ الإجراءات ..... ١٧
- ٤,٢ دورات العمل ..... ١٩
- ٣. سياسة إدارة الموارد البشرية لتقنية المعلومات ..... ٢٠
- ١,٣ المقدمة والأهداف ..... ٢٠
- ٢,٣ السياسات ..... ٢٠
- ٣,٣ الإجراءات ..... ٢٢
- ٤.٣ دورات العمل ..... ٢٤
- ٤. سياسة إدارة الجودة ..... ٢٦
- ١,٤ المقدمة والأهداف ..... ٢٦
- ٢,٤ الإجراءات ..... ٢٨
- ٥. سياسة تقييم مخاطر تقنية المعلومات ..... ٢٩

١,٥ المقدمة والأهداف ..... ٢٩
٢,٥ الإجراءات ..... ٣٢
٣.٥ دورات العمل ..... ٣٣
٦. سياسة شراء أنظمة وموارد المعلومات ..... ٣٤
١,٦ المقدمة والأهداف ..... ٣٤
٢,٦ السياسات ..... ٣٤
٣,٦ الإجراءات ..... ٣٥
٤.٦ دورات العمل ..... ٣٨
٧. سياسة إدارة التغيير ..... ٤٠
١,٧ المقدمة والأهداف ..... ٤٠
٢,٧ السياسات ..... ٤٠
٣,٧ الإجراءات ..... ٤٢
٤,٧ دورات العمل ..... ٤٨
٨. سياسة إدارة عمليات التشغيل في تقنية المعلومات ..... ٥١
١,٨ المقدمة والأهداف ..... ٥١
٢,٨ السياسات ..... ٥١
٣,٨ الإجراءات ..... ٥٢
٤,٨ دورات العمل ..... ٥٤
٩. سياسة ضمان استمرارية الأعمال ..... ٥٦
١,٩ المقدمة والأهداف ..... ٥٦
٢.٩ السياسات ..... ٥٦
٣,٩ الإجراءات ..... ٥٧
٤.٩ دورات العمل ..... ٥٨
١٠.سياسة معدل الاستخدام الأمثل للأنظمة ..... ٥٩
١,١٠ المقدمة والأهداف ..... ٥٩
٢.١٠ السياسات ..... ٥٩
٣,١٠ الإجراءات ..... ٦٥
١١.سياسة إدارة الخدمات المقدمة من طرف ثالث ..... ٦٦
1.11 المقدمة والأهداف ..... ٦٦
2.11 السياسات ..... ٦٦
3.11 الإجراءات ..... ٦٧

١٢.سياسة النسخ الاحتياطي والاسترجاع في حال الكوارث ..... ٦٨
1.12 المقدمة والأهداف ..... ٦٨
2.12 السياسات ..... ٦٨
3.12 الإجراءات ..... ٧٠
٤.١٢ دورات العمل ..... ٧٢
١٣.سياسة تقييم أداء تقنية المعلومات ..... ٧٤
1.13 المقدمة والأهداف ..... ٧٤
2.13 السياسات ..... ٧٤
3.13 الإجراءات ..... ٧٦
4.13 دورات العمل ..... ٧٧
١٤.سياسة أمن المعلومات ..... ٧٨
1.14 المقدمة والأهداف ..... ٧٨
2.14 السياسات ..... ٧٨
3.14 الإجراءات ..... ٧٩
٤.١٤ دورات العمل ..... ٨٢
١٥.سياسة الأمن المادي والبيئي ..... ٨٤
1.15 المقدمة والأهداف ..... ٨٤
2.15 السياسات ..... ٨٤
3.15 الإجراءات ..... ٨٦
١٦.سياسة إدارة وصحة المعلومات ..... ٨٦
1.16 المقدمة والأهداف ..... ٨٦
2.16 السياسات ..... ٨٦
3.16 الإجراءات ..... ٨٨
١٧.سياسة أمن الوسائط الإلكترونية ..... ٨٩
1.17 المقدمة والأهداف ..... ٨٩
2.17 السياسات ..... ٨٩
3.17 الإجراءات ..... ٩٢
4.17 دورات العمل ..... ٩٣
١٨.سياسة الحماية من الفيروسات والبرامج الضارة ..... ٩٤
1.18 المقدمة والأهداف ..... ٩٤
2.18 السياسات ..... ٩٤

3.18 الإجراءات ..... ٩٧

١.١٨ دورات العمل ..... ٩٩

١٩.سياسة الوصول المنطقي ..... ١٠٠

1.19 المقدمة والأهداف ..... ١٠٠

2.19 السياسات ..... ١٠٠

3.19 الإجراءات ..... ١٠٦

4.19 دورات العمل ..... ١١٠

- **جدول اعتماد الدليل**

| المستند | تاريخ الإصدار | المراجع | المعتمد |
|---|---|---|---|
| **دليل السياسات والإجراءات لإدارة تقنية المعلومات** | **١٠ يوليو ٢٠١٤**<br><br>**المسودة الأولى** | **مدير تقنية المعلومات**<br><br>**الأستاذ/** | **أمين المجلس الفرعي**<br><br>**الأستاذ/** |
| | | **التوقيع:**<br><br>**التاريخ:** | **التوقيع:**<br><br>**التاريخ:** |

## مقدمة

### ١.١ الغرض والأهداف من الدليل

١.١.١ توفير مستند مرجعي لإدارة تقنية المعلومات وتحديد السياسات والإجراءات للأعمال ذات الصلة بإدارة تقنية المعلومات وكذلك تعزيز الضوابط على تلك السياسات والإجراءات.

٢.١.١ توثيق السياسات والإجراءات المرتبطة بإدارة تقنية المعلومات وتحديد الصلاحيات والمسؤوليات المرتبطة بها.

٣.١.١ يهدف هذا الدليل الى التالي:

- داخلياً – أن يشكل مجموعة من المعايير والنظم والقواعد الحاكمة التي تقوم الجمعية بتسجيل نشاطاتها التقنية بناء عليها، وكذلك نتائج عملياتها، ويشكل هذا الدليل مستند مرجعي لموظفي إدارة تقنية المعلومات وأداة لتعزيز الضوابط على عملها.
- خارجياً – تزويد مستخدمي البيانات التقنية بتفاصيل عن أسس الافصاح وتقديم وبيان الوضع الحالي لتقنية ونظم المعلومات، ونتائج عملياته.

### ٢.١ استخدام الدليل

١.٢.١ يستخدم هذا الدليل كمرجعية لعمل موظفي إدارة تقنية المعلومات لدى الجمعية، بحيث يتم الرجوع إلى الجزء ذي العلاقة من هذا الدليل للاسترشاد به.

٢.٢.١ ينبغي على إدارة تقنية المعلومات القيام بعملية مراجعة دورية لهذا الدليل، وذلك بهدف تقييم مدى ملاءمته وقابليته للتطبيق، أو حاجته إلى التعديل وفقاً للتغيرات التي قد تطرأ في الجمعية أو البيئة المحيطة بها.

٣.٢.١ يقسم هذا الدليل إلى عدة أقسام يحتوي كل منها على سياسات وإجراءات عامة لضمان فاعلية سياسات تقنية المعلومات المتبعة في الجمعية، ويشمل كذلك الإجراءات المفصلة لكل نشاط، والشخص المسؤول عن تنفيذها.

### ٣.١ مراقب الدليل

١.٣.١ مراقب هذا الدليل هو مدير تقنية المعلومات. يجب أن توجه كافة الاستفسارات والأمور المتعلقة بهذا الدليل ونطاقه وأهدافه إلى مراقب الدليل. إن مسؤولية الحفاظ على الدليل ومحتوياته وتوزيعه كليا أو جزئياً، بالإضافة إلى تحديثه وتطبيقه على نحو صحيح هي من صلاحيات مراقب الدليل.

### ٤.١ حق الاطلاع على الدليل

١.٤.١ إن كافة العاملين المعنيين في الجمعية لهم حرية الاطلاع على هذا الدليل بعد الحصول على موافقة مسبقة من مراقب الدليل. كما يجب أن يتاح لكافة المدراء فضلاً عن العاملين في تقنية المعلومات الاطلاع على الدليل.

### ٥.١ الموافقة على الدليل

١.٥.١ يجب أن يتم اعتماد دليل سياسات وإجراءات تقنية المعلومات من قبل أمين المجلس الفرعي وذلك قبل وضعه قيد التطبيق.

٢.٥.١ يتم تفعيل الدليل بدءاً من تاريخ اعتماده من قبل أمين المجلس الفرعي

### ٦.١ تنفيذ الدليل

١.٦.١ يتولى مراقب الدليل مسؤولية التأكد من تنفيذ والالتزام بسياسات وإجراءات عمليات إدارة تقنية المعلومات.

٢.٦.١ يمكن لمراقب الدليل تفويض مسؤولية تنفيذ سياسات وإجراءات إدارة تقنية المعلومات وفقاً لما هو وارد بهذا الدليل إلى شخص مختص في التعامل مع المسئوليات داخل إدارة تقنية المعلومات.

### ٧.١ تعزيز الدليل

١.٧.١ يهدف هذا الدليل إلى أن يكون بمثابة وثيقة حية يتم إضافة سياسات وإجراءات بها عند الضرورة. و إنه من المتوقع أن تتطلب السياسات والإجراءات القائمة إلى تعديل وكذلك يتطلب الأمر إضافة سياسات وإجراءات جديدة.

٢.٧.١ يجب أن تتم كافة التعديلات والتحديثات على هذا الدليل وفقاً لإجراءات التحديث الواردة في هذا الجزء.

## ٨.١ الانحراف عن السياسات والإجراءات

١.٨.١ يجب على جميع الموظفين في تقنية المعلومات التأكد من الامتثال التام لنص وروح هذا الدليل والعمل على مساعدة مدير تقنية المعلومات على تطبيقه بالشكل الصحيح.

٢.٨.١ عند مواجهة صعوبة ما في فهم مضمون الدليل أو بعض النقاط الواردة فيه، يجب استشارة مدير تقنية المعلوما والحصول على التوضيح اللازم.

٣.٨.١ عند ضرورة الانحراف مؤقتاً عن أي من السياسات والإجراءات الواردة في هذا الدليل، يجب إخطار مدير تقنية المعلومات وأخذ التعليمات اللازمة بهذا الشأن.

## ٩.١ نطاق الدليل

١.٩.١ نطاق تطبيق هذا الدليل وما يتصل به هو من اختصاص إدارة تقنية المعلومات تحت الإشراف المباشر من مدير تقنية المعلومات.

## ١٠.١ صيانة الدليل وتكرار معدل المراجعة

١.١٠.١ يجب أن يتم مراجعة واعتماد الدليل على فترات منتظمة لتعكس التغييرات في أنشطة أعمال الجمعية.

٢.١٠.١ يتناول الجدول التالي معدل تكرار المراجعة ومسؤولية أداء المراجعة ومسؤولية المعتمد النهائي:

| المراجعة | معدل تكرار المراجعة | مسؤولية المراجعة | مسؤولية الموافقة |
|---|---|---|---|
| السياسات | كل ١٢ شهر | مدير تقنية المعلومات | أمين المجلس الفرعي |
| الاجراءات | كل ١٢ شهر | مدير تقنية المعلومات | أمين المجلس الفرعي |

## ١١.١ إجراءات التحديث

١.١١.١ يتم عمل التعديلات بالدليل كنتيجة لسبب أو مجموعة من الأسباب التالية التي لها تأثير مباشر على أعمال إدارة تقنية المعلومات:

التغييرات في السياسات العامة للجمعية

التغييرات في وظائف وأنشطة الجمعية

التغييرات في الهيكل التنظيمي للجمعية

التغييرات على أنظمة المعلومات المستخدمة في الجمعية

٢.١١.١ يتم طلب تحديث الدليل (الإضافة / الإلغاء / التعديل) من قبل مستخدم الدليل الذي يرفعه مدير تقنية المعلومات للموافقة. يجب أيضا أن يلقي طلب التغيير / التحديث الضوء على أثر التغييرات المقترحة.

٣.١١.١ سوف يتم تحديث هذا الدليل للتأكد من التصريح بكافة التغييرات وتوثيقها سواء كانت تلك التغييرات مؤقتة أو دائمة وكذلك التأكد من أن محتويات الدليل تعكس باستمرار الممارسات الحالية في إدارة تقنية المعلومات.

٤.١١.١ سوف تتم عملية التحديثات فقط من خلال طلب تحديث الدليل.

٥.١١.١ سوف يتم منح الموافقة المبدئية والنهائية لأية تغييرات وفقا للمبدأ التوجيهي لمعدل تكرار الصيانة والمراجعة الوارد في هذا الجزء.

٦.١١.١ بمجرد الحصول على الموافقة، سوف يتم إعادة طلب تحديث الدليل إلى مراقب الدليل ليتم تسجيله في سجل ضبط تحديثات الدليل الوارد في هذا الجزء.

٧.١١.١ سوف يتم إصدار كافة التغييرات المؤقتة في صيغة مذكرة مستقلة مع إتباع نفس الإجراء الخاص بتحديث الدليل مع إشارة تدل على الأجزاء ذات الصلة المتأثرة في هذا الدليل.

٨.١١.١ يجب أن يتم الاحتفاظ بالحد الأدنى من التغييرات المؤقتة وسوف يتم تفعيلها لمدة لا تتجاوز شهراً واحداً وأن لا يتطلب الأمر إعادة إصدار مذكرة محدثة بالتغييرات المؤقتة.

## ١٢.١ سجل مراقبة عمليات التحديث

١.١٢.١ يجب وضع أي متغيرات تطرأ على هذا الدليل مؤرخة ومتسلسلة.

٢.١٢.١ يتم إدخال تاريخ إجراء التحديث إلى جانب رقم التغيير في كل صفحة من صفحات دليل تقنية المعلومات.

٣.١٢.١ يتولى مراقب الدليل التحقق من معرفة جميع الموظفين بالتحديثات ورقم آخر إصدار من إصدارات الدليل وتاريخ بدء التطبيق.

٤.١٢.١ يجب الاستعانة بالجدول الآتي وتوقيعه لإجراء جميع التحديثات على الدليل.

تاريخ هذا الإصدار: ***xxx/xx/xx*** تاريخ الإصدار التالي: ***xxx/xx/xx***

| الإصدار | التاريخ | ملخص التغييرات |
|---|---|---|
| | | |
| | | |

## ١٣.١ حقوق التأليف والنشر

١.١٣.١ إن هذا الدليل هو ملك لجمعية مراكز الأحياء وقد أعد للاستخدام الداخلي فيها فقط.

٢.١٣.١ لا يسمح أن يتم نسخ أو تخزين أي جزء من هذا الدليل في أي نظام أو شكل أو أن يتم نقله في أي شكل من خلال أي وسيلة – سواء الكترونية أو مصورة أو مسجلة أو غير ذلك – دون الحصول على موافقة خطية مسبقة من مراقب الدليل بعد موافقة أمين عام الجمعية.

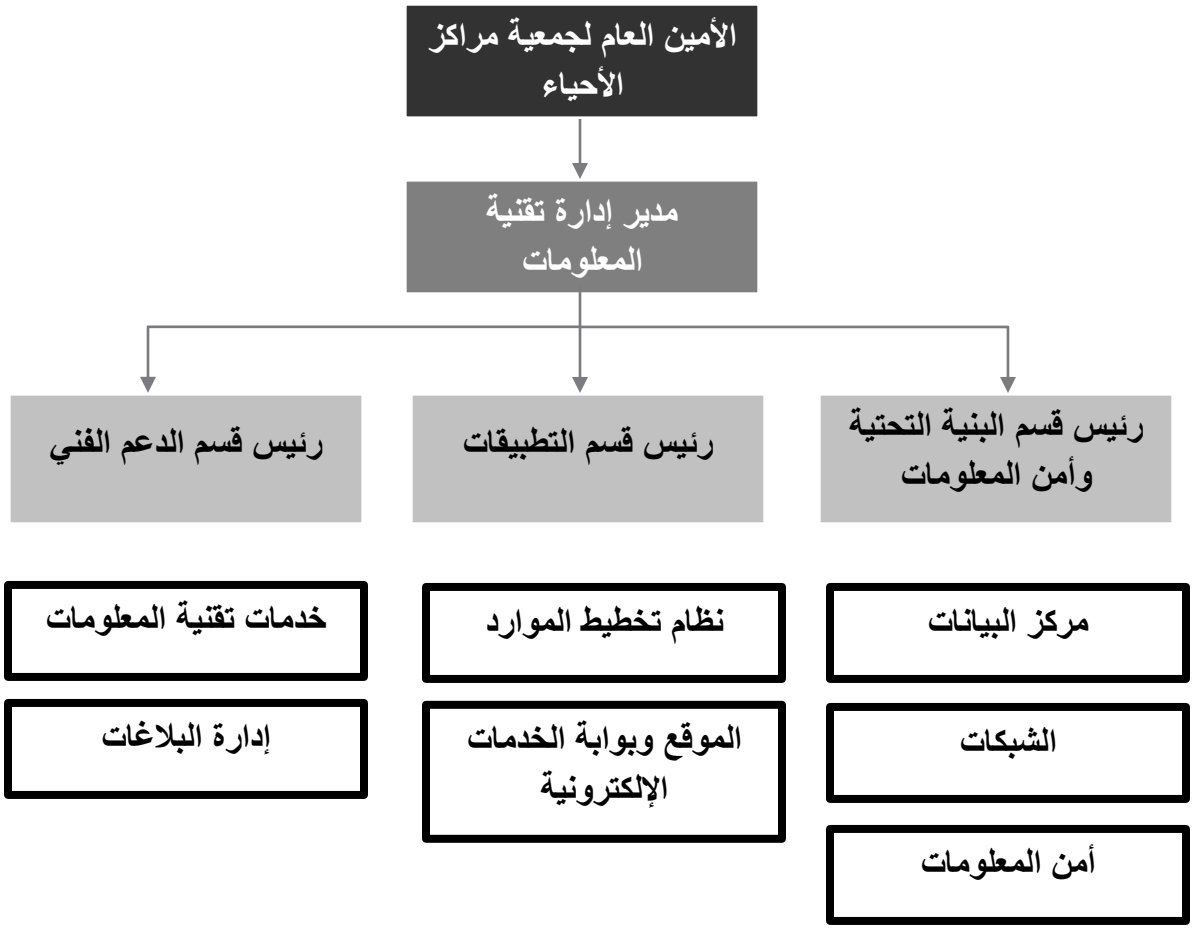
٣.١٣.١ قد تؤدي مخالفة أي من الفقرات الواردة أعلاه إلى إخضاع الجهة المخالفة إلى الإجراءات القانونية المعمول بها وفقا لقوانين المملكة العربية السعودية وسياسات الجمعية بما يختص بحقوق النشر.

## ١٤.١ عام

١.١٤.١ يعد ضروريا بالنسبة لإدارة تقنية المعلومات أن يكون لديها مجموعة جيدة من أعضاء مؤهلين من أجل تنفيذ السياسات والإجراءات الموضحة في هذا الدليل.

٢.١٤.١ يجب أن يكون لدى كل عضو من الأعضاء وصف وظيفي محدد وتكليف معين لمساعدته في معرفة تفاصيل وظيفته.

## ١٥.١ الهيكل التنظيمي لإدارة تقنية المعلومات



# سياسات وإجراءات إدارة تقنية المعلومات

# إطار عمليات إدارة تقنية المعلومات

## نموذج إطار عمليات إدارة تقنية المعلومات

| التخطيط والتنظيم | امتلاك و تطبيق | التقديم والدعم | الرقابة والتقييم | أمن المعلومات |
|---|---|---|---|---|
| تطوير الخطة الاستراتيجية لتقنية المعلومات | اختيار حلول أتمته الاعمال | ادارة مستوى الخدمات | تقييم الاداء المعلومات | ادارة اصول تقنية المعلومات |
| إدارة الموارد البشرية لتقنية المعلومات | تمكين العمليات والاستخدام | ادارة استمرارية خدمات تقنية المعلومات | معايير تقييم الاداء | ادارة امن معلومات |
| إدارة الجودة | مشتريات موارد التقنية | ادارة التغيير | | ادارة الدخول الى موارد تقنية المعلومات |
| ادارة وتقييم المخاطر | | تدريب المستخدمين | | |
| | | ادارة خدمات الطرف الثالث | | |
| | | النسخ الاحتياطي | | |
| | | الصيانة | | |

# التخطيط والتنظيم

## ٢. سياسة التخطيط الاستراتيجي لتقنية المعلومات

### ١.٢ المقدمة والأهداف

١.١.٢ يتركز دور إدارة تقنية المعلومات على البحث في الاحتياجات التقنية لجمعية مراكز الأحياء (الجمعية) والبحث عن أفضل التقنيات والخدمات الإلكترونية والعمل على توظيفها بالطريقة الأفضل. الهدف الرئيسي لهذه السياسة هو إدارة تقنية المعلومات بما يتوافق مع استراتيجية وميزانية الجمعية ويتضمن ذلك:

أ. تحديد توجه استراتيجي لإدارة تقنية المعلومات بما يتوافق مع استراتيجية جمعية مراكز الأحياء وأهدافها

ب. ترتيب وإعداد أولويات تنفيذ مبادرات و مشاريع تقنية المعلومات المزمع تنفيذها في المستقبل

ج. إدارة المتطلبات التقنية الطارئة للأعمال في الجمعية بما يخص تقنية المعلومات

### ٢.٢ السياسات

١.٢.٢ وضع الخطة الاستراتيجية لتقنية المعلومات

أ. تحدد الخطة الاستراتيجية لتقنية المعلومات كيفية مساهمة إدارة تقنية المعلومات في تحقيق الأهداف الاستراتيجية لجمعية مراكز الأحياء.

ب. تحدد الخطة الاستراتيجية لتقنية المعلومات كيفية تقديم الدعم الفني لجمعية مراكز الأحياء في متطلبات الأهداف الاستراتيجية للأعمال والاستثمارات، وتحدد أيضاً جميع المتطلبات لتحقيق ذلك بما في ذلك الميزانية والتمويل.

ج. تتضمن الخطة الاستراتيجية مشاريع لتحقيق أهداف إدارة تقنية المعلومات وتحدّد المسؤوليات والتوقعات من حيث الأداء والتنفيذ والنتائج بشكل واضح.

٢.٢.٢ تحديث الخطة الاستراتيجية لتقنية المعلومات

أ. يعاد النظر في الخطة الاستراتيجية لتقنية المعلومات بشكل دوري (يفضل أن يكون سنويا) لضمان تحديد ومعالجة المتطلبات الجديدة لتقنية المعلومات والأنظمة اللازمة لتحقيق الأهداف الاستراتيجية لجمعية مراكز الأحياء.

## ٣.٢ الإجراءات

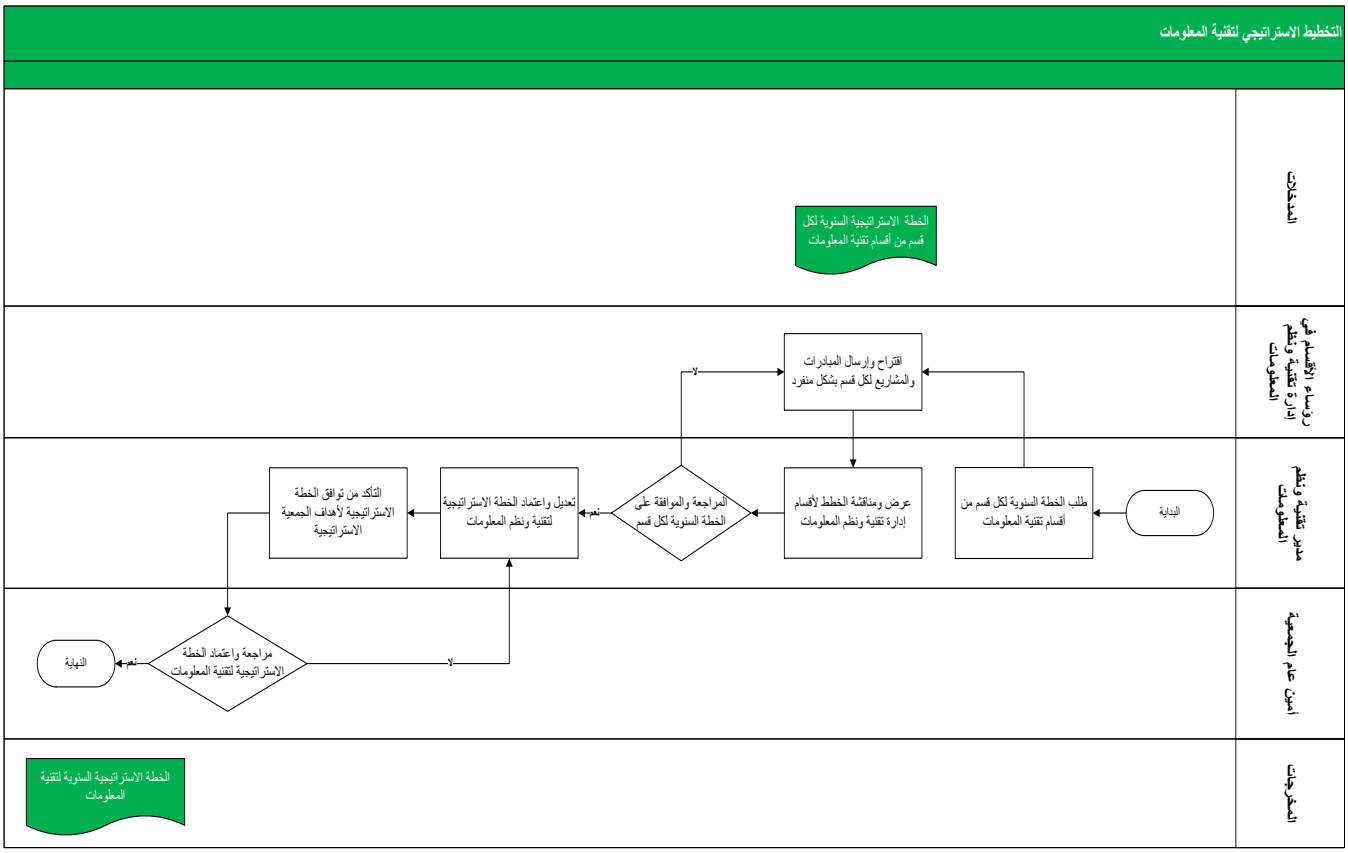
### ١.٣.٢ التخطيط الاستراتيجي لتقنية المعلومات

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | مدير تقنية المعلومات | عند نهاية كل سنة مالية يقوم مدير ادارة تقنية المعلومات بطلب الخطة السنوية المخطط لها من رؤساء الأقسام في إدارة تقنية المعلومات | | | لا يوجد |
| ٢. | رؤساء الأقسام في إدارة تقنية المعلومات (التطبيقات، البنية التحتية وأمن المعلومات، الدعم الفني) | يقوم رؤساء الأقسام اقتراح المشاريع والمبادرات حسب احتياجات الجمعية والتطلعات المستقبلية | | | لا يوجد |
| ٣. | رؤساء الأقسام في إدارة تقنية المعلومات (التطبيقات، البنية التحتية وأمن المعلومات، الدعم الفني) | يقوم رؤساء الأقسام بالاجتماع لمناقشة الخطط وترتيب الأولويات ومن ثم عمل الخطة الموحدة للمشاريع و يتم الاتفاق على أولويات تنفيذ للمشاريع والموارد التي سيتم استخدامها | | | لا يوجد |
| ٤. | رؤساء الأقسام في إدارة تقنية المعلومات (التطبيقات، البنية التحتية وأمن | يتم عرض الخطة على مدير ادارة تقنية المعلومات ويتم مناقشتها معه مع الأخذ بعين الاعتبار مداخلاته وتوجيهاته | | | لا يوجد |

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| | المعلومات، الدعم الفني) | | | | |
| ٥. | مدير تقنية المعلومات | يقوم مدير ادارة تقنية المعلومات بمراجعة الخطة و التأكد من أن الخطة الاستراتيجية السنوية لتقنية المعلومات متوافقة مع الخطة الاستراتيجية العامة لجمعية مراكز الأحياء | | | لا يوجد |
| ٦. | أمين الجمعية | يقوم مدير ادارة تقنية المعلومات برفع الخطة الاستراتيجية السنوية لأمين الجمعية للمناقشة والاعتماد | | | الخطة الاستراتيجية السنوية لتقنية المعلومات |

## ٤.٢ دورات العمل

### ١.٤.٢ التخطيط الاستراتيجي لتقنية المعلومات



## ٣. سياسة إدارة الموارد البشرية لتقنية المعلومات

### ١.٣ المقدمة والأهداف

١.١.٣ الغرض من هذه السياسة هو الحد من احتمالات إساءة استخدام أو تدمير أنظمة المعلومات لدى جمعية مراكز الأحياء، وذلك من خلال التأكد من نزاهة الموظفين الذين يتم منحهم إمكانية الوصول إلى أنظمة المعلومات والموارد التقنية لدى الجمعية.

### ٢.٣ السياسات

١.٢.٣ شروط وأحكام التوظيف:

أ. المسئوليات المتعلقة بالتعامل الآمن مع المعلومات وأنظمة المعلومات الخاصة بجمعية مراكز الأحياء من قبل الموظف إشارة إلى الإجراءات الإدارية التي ستطبق في حالة مخالفة أحكام التوظيف ويجب الرجوع الى ادارة الموارد البشرية لتنفيذ هذه العملية.

ب. يتعين على جميع المستخدمين من الموظفين لدى جمعية مراكز الأحياء توقيع شروط وأحكام التوظيف/ الارتباط بالإضافة الى اتفاقية السرية للدلالة على قبولهم بها.

ج. يجب الرجوع إلى سياسة الموارد البشرية فيما يخص إجراءات التوظيف والتدريب للموظفين

٢.٢.٣ الاعتماد على الأشخاص

أ. ينبغي على جمعية مراكز الأحياء الحد من مخاطر الاعتماد بصورة كبيرة على موظفين رئيسيين وذلك من خلال تفعيل المشاركة في المعرفة، وتخطيط التعاقب

والإحلال الوظيفي، ووجود احتياطي من الموظفين، والوسائل الأخرى في هذا الصدد.

٣.٢.٣ عملية الإجراءات التأديبية

أ. يجب أن تتخذ جمعية مراكز الأحياء إجراءات تأديبية في حال تم انتهاك سياسات تقنية وأمن المعلومات.

ب. يجب توثيق واعتماد أي استثناءات تسمح بعدم تعريض أحد موظفي جمعية مراكز الأحياء للإجراءات التأديبية.

٤.٢.٣ التدريب وتطوير كفاءات تقنية المعلومات

أ. يجب على إدارة تقنية المعلومات دراسة الاحتياجات التدريبية لموظفيها بشكل دوري بناء على تقييم أداء الموظفين في الإدارة والتكنولوجيا الحديثة بما يتعلق بأعمال الجمعية، وإعداد خطة تدريب سنوية لتنفيذ هذه الاحتياجات.

ب. يتم تعديل خطة التدريب في حال تطبيق تقنيات جديدة أو تحديث التقنيات القائمة بشكل جذري.

ج. يتم تقديم تدريب لمستخدمي أنظمة معلومات الجمعية من قبل إدارة تقنية المعلومات حسب احتياجات العمل.

٥.٢.٣ تغيير دور أو استقالة أو إقالة موظف أو مقاول

أ. في حالة تغيير الدور أو استقالة أو إقالة موظف ، فإن على مدير إدارة الموارد البشرية/ الإدارة المعنية القيام فوراً بإبلاغ إدارة تقنية المعلومات لإلغاء/ تعديل

صلاحيات الدخول لذلك الموظف على أنظمة المعلومات. واسترجاع كافة العهد. ويجب التعامل مع ذلك وفقاً لإجراءات تغيير الدور أو الاستقالة أو الإقالة.

٦.٢.٣ مراقبة سلوك الموظف

أ. تقع على عاتق موظفي ومقاولي جمعية مراكز الأحياء مسئولية تبليغ إدارة تقنية المعلومات/ الموارد البشرية/ أو الإدارة المعنية عن أي أنشطة مشبوهة يقوم بها زملاؤهم أو المقاولين أو الأشخاص الآخرين الذين لديهم إمكانية الوصول إلى أنظمة المعلومات لدى جمعية مراكز الأحياء.

## ٣.٣ الإجراءات

### ١.٣.٣ التوظيف وتقديم الموظفين

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | مدير تقنية المعلومات | قبل بداية العام (وكذلك خلال العام عند الحاجة)، كجزء من التخطيط السنوي لتقنية المعلومات، يقوم مدير تقنية المعلومات بتحديد احتياجات القسم من الموارد البشرية والتي يجب اضافتها للوظائف الحالية ويجب الرجوع في ذلك إلى سياسة الموارد البشرية | | | لا يوجد |
| ٢. | رؤساء الأقسام في تقنية المعلومات | يقوم مدير تقنية المعلومات بالتنسيق مع رؤساء الأقسام بإجراء المقابلات الوظيفية من أجل اختيار المرشحين للمناصب الشاغرة في إدارة تقنية المعلومات وفقاً لسياسات الموارد البشرية. | | | لا يوجد |
| ٣. | مدير تقنية المعلومات | يقوم مدير تقنية المعلومات بالموافقة على العروض الوظيفية للمرشحين المجتازين للمقابلات الشخصية وفقاً لسياسات الموارد البشرية | | | العرض الوظيفي |

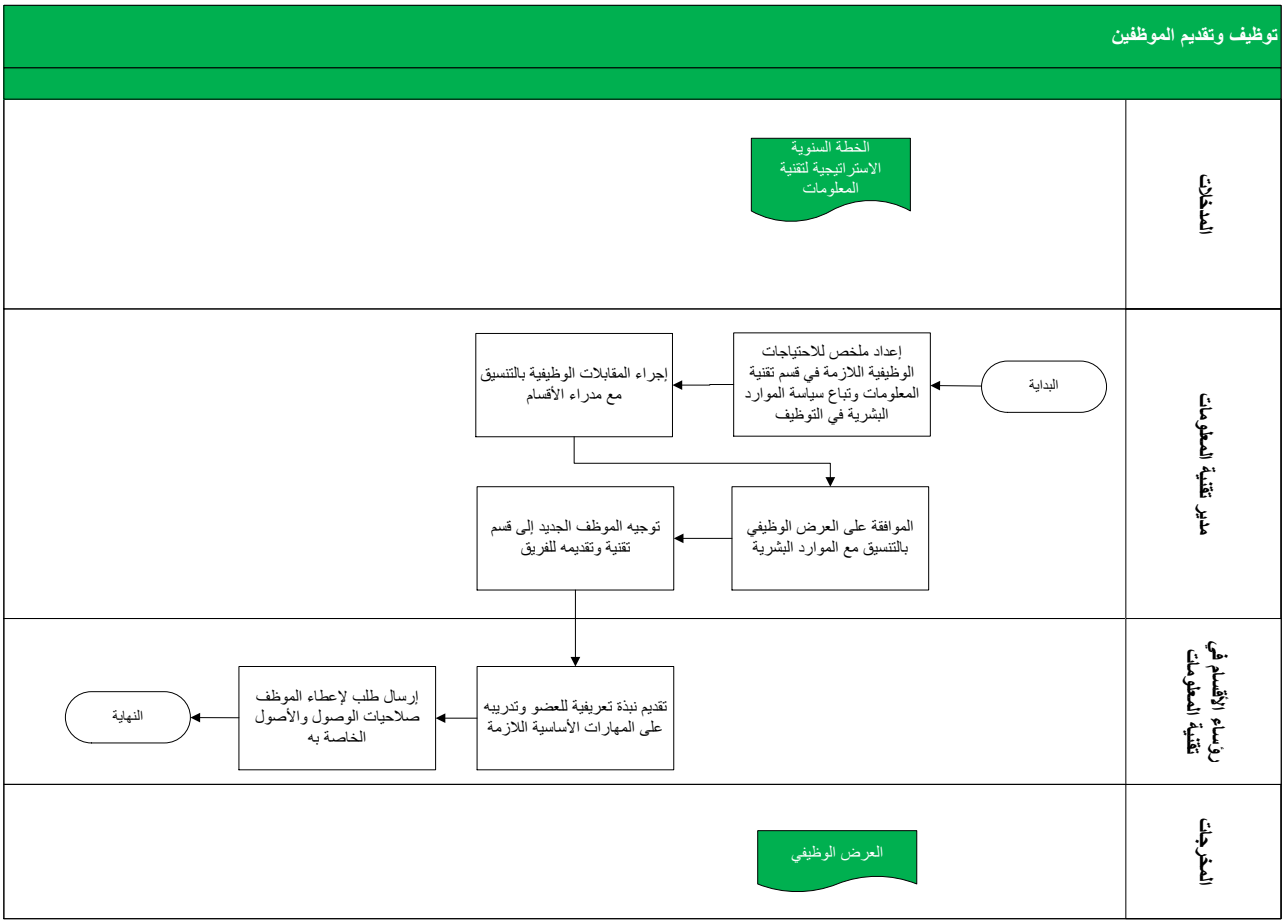
| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ٤. | مدير تقنية المعلومات | يقوم مدير تقنية المعلومات بتعيين موظف جديد إلى قسمه وتوجيهه إلى رئيس القسم المعني (رئيس قسم التطبيقات، رئيس قسم الدعم الفني المعلومات، رئيس قسم البنية التحتية)، الذي يشرف عن كثب على الموظف الجديد، ومراقبة أدائه ، بالإضافة وتوفير التوجيه والدعم له خلال فترة التجربة (٣)أشهر | | | لا يوجد |

## ٢.٣.٣ تدريب وتطوير كفاءات تقنية المعلومات

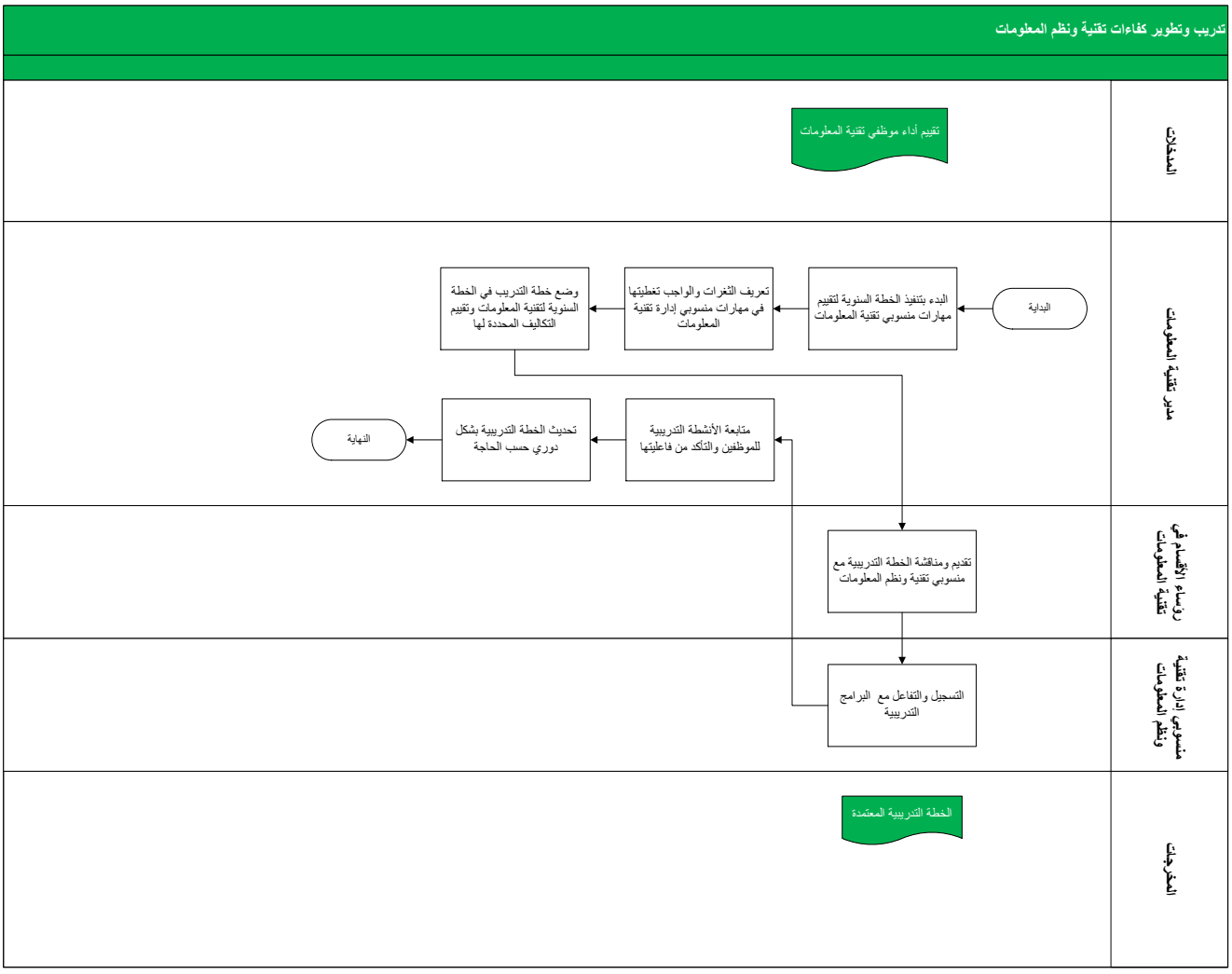
| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | رؤساء الأقسام في تقنية المعلومات | يقوم رؤساء الأقسام بتقييم المهارات والمتطلبات الوظيفية لمنسوبي الإدارة في بداية كل سنة بناء على تقييم أداء الموظفين وتحديد مواطن التطوير. | | | لا يوجد |
| ٢. | رؤساء الأقسام في تقنية المعلومات | يقوم رؤساء الأقسام بتحديد متطلبات التدريب حسب التقنيات المستخدمة حاليا و في المستقبل ويتم مناقشتها مع مدير تقنية المعلومات لاعتمادها. | | | لا يوجد |
| ٣. | مدير تقنية المعلومات | يقوم مدير إدارة تقنية المعلومات بإرسال متطلبات التدريب لإدارة الموارد البشرية لإدخالها في خطة التدريب العامة للجمعية . | | | لا يوجد |
| ٤. | مدير تقنية المعلومات | يتم التنسيق مع إدارة الموارد البشرية لتطبيق خطة التدريب المعتمدة. | | | خطة التدريب |

## ٤.٣ دورات العمل

### ١.٤.٣ التوظيف وتقديم الموظفين



## ٢.٤.٣ تدريب وتطوير كفاءات تقنية المعلومات



## ٤. سياسة إدارة الجودة

### ١.٤ المقدمة والأهداف

١.١.٤ الغرض من هذه السياسة هو تحقيق معايير الجودة فيما يخص التطبيقات والبنية التحتية والأنظمة المساندة التي تخدم أعمال جمعية مراكز الأحياء.

٢.١.٤ السياسات

٣.١.٤ الجودة في اختيار وتطبيق البرامج الجاهزة :

أ. استخدام آلية معتمدة لاختيار الأنظمة الجاهزة من الجهات الخارجية ، على أن تتضمن هذه الآلية بحد أدنى على مقارنات فيما يخص:

- الملف التعريفي للمورد وملائته المالية
- الوظائف المطلوبة من البرنامج (Application) وملائمتها لمتطلبات الاعمال في الجمعية
- الخصائص التقنية للتطبيق وتوافقها مع البنية التحتية
- الخصائص التقنية لشبكة المعلومات في الجمعية
- كيفية تقديم الدعم الفني والصيانة من قبل المورد
- منهجية إدارة

ب. منهجية إدارة المشروع في مرحلة تطبيق البرنامج (Implementation Phase)

٤.١.٤ الجودة في تطوير البرامج :

أ. اعتماد إطار عمل متكامل لتطوير البرامج ( System Development Life Cycle) والاستفادة من نموذج نضج إمكانية التكامل ( Capability Maturity

(Model Integration) لتحسين عملية تطوير البرامج بهدف التوافق مع أهداف الجمعية.

ب. اعتماد منصة تطوير (Development Platform) موحدة لتطوير البرامج التي تحتاجها الجمعية ، بحيث يتم اختيار هذه المنصة على أسس واضحة وتلقي التدريب الكافي على استخدامها.

ج. تحديد مسؤوليات فريق تطوير البرامج ومراقبة ذلك من خلال تطبيق حل متكامل يتضمن جميع مراحل تطوير البرامج وإدارة شفرات المصدر ( Source Code Management)، ومثال ذلك (MS Visual Studio).

د. القيام بإجراء اختبارات رسمية موثقة على البرامج المطورة داخليا وتوثيق نتائج الاختبارات.

٥.١.٤ الجودة في أمن المعلومات:

هـ. يجب على إدارة تقنية المعلومات في الجمعية مراعاة تطبيق الضوابط ذات العلاقة في مقياس أيزو (ISO 27001) من خلال دمج هذه الضوابط في عمليات تقنية المعلومات .

و. القيام بمراقبة الالتزام بهذه الضوابط بشكل دوري من خلال القيام بإجراء عمليات مراجعة على هذه الضوابط.

ز. إعداد تقارير دورية حول حوادث أمن المعلومات وتقارير المراجعة وإعداد خطط لتحسين هذه الضوابط واقتراح حلول وتوصيات لتحسين مستوى من المعلومات في الجمعية.

ح. القيام بحملات توعية أهمية الالتزام بمعايير وضوابط أمن المعلومات لجميع المستخدمين.

٦.١.٤ الجودة في تقديم الدعم الفني وخدمات تقنية المعلومات :

ط. تحديد قائمة الخدمات التي تقدمها إدارة تقنية المعلومات ومتطلبات الحصول عليها

ي. تحديد دورات العمل المتعلقة بكل خدمة والوقت القياسي للحصول على كل خدمة

ك. متابعة الطلبات/والبلاغات المقدمة من قبل المستخدمين والتأكد من معالجتها حسب اتفاقيات مستوى الخدمة(Service Level; Agreement)

ل. إصدار تقارير حول كيفية جودة تقديم الخدمات وحل البلاغات من خلال مراجعة عينات عشوائية منها ، بالإضافة قياس مدى رضى المستخدمين بشكل دوري.

## ٢.٤ الإجراءات

١.٢.٤ لا تحتاج هذه السياسة لإجراءات تشغيلية بموجب هذا الإطار. وقد تم تحديد الخطوات العملية المطلوب اتباعها ضمن السياسة.

## ٥. سياسة تقييم مخاطر تقنية المعلومات

### ١.٥ المقدمة والأهداف

١.١.٥ الغرض من هذه السياسة لوضع إطار عمل لتحليل و تقييم المخاطر والتخفيف من آثارها على تقنية المعلومات و ادارات الاعمال في الجمعية.

٢.١.٥ السياسات

٣.١.٥ إطار عمل تقييم مخاطر تقنية المعلومات :

أ. يجب أن يكون إطار عمل تقييم المخاطر في تقنية المعلومات متوافقاً مع إطار إدارة المخاطر في الجمعية ، بحيث يتم تعريف مخاطر تقنية المعلومات وفقاً لمتطلبات الأعمال في الجمعية

ب. ينبغي تأسيس سياق لتقييم مخاطر تقنية المعلومات (Risk Assessment Context) ، ويجب أن يشمل هذا السياق ما يلي:

- تحديد أهداف سياق المخاطر الداخلية والخارجية على تقنية المعلومات
- ووضع أهداف واضحة لعملية تقييم المخاطر
- تحديد معايير (Criteria) لكل خطر من المخاطر وكيفية تقييمها

٤.١.٥ تعريف الأحداث وتقييم المخاطر:

أ. الأحداث هي عبار تهديدات واضحة وواقعية تستغل نقاط الضعف في أنظمة الجمعية ، والتي قد تؤدي إلى التأثير سلباً على إجراءات الأعمال في الجمعية ، ويشمل ذلك ما يلي:

- متطلبات سير العمل
- الأنظمة والقوانين الداخلية والخارجية
- التقنيات المستخدمة
- الموارد البشرية
- الجوانب التشغيلية

ب. يجب تحليل طبيعة ومدى تأثير المخاطر المترتبة على الحدث وحفظ هذه المعلومات في سجل مخاطر تقنية المعلومات

ج. يجب تقييم الأحداث المحتمل وقوعها مع جميع المخاطر المتعلقة بها باستخدام أساليب التحليل الكمية والنوعية.

د. ينبغي أن تحدد احتمال وتأثير المخاطر المرتبطة بشكل فردي، وذلك حسب تصنيف هذه المخاطر.

٥.١.٥ وضع خطة للحد من تأثير المخاطر:

أ. تطوير خطة الاستجابة للمخاطر تهدف إلى ضمان رقابة فعالة من حيث التكلفة للضوابط الواجب تطبيقها وتخفيف احتمالية التعرض للمخاطر التي تم حصرها بشكل مستمر.

ب. ينبغي لعملية الاستجابة للمخاطر تحديد استراتيجيات معالجة المخاطر مثل:

a. التجنب (Avoidance)،

b. الحد (Reduction)،

c. والتقسيم (Sharing)،

d. القبول(Acceptance)

كما ينبغي تحديد المسؤوليات المرتبطة بهذه الخطة ؛ والنظر في مستويات تحمل المخاطر المقبولة لدى الجمعية (Acceptable Risk Tolerance Level).

ج. يجب إعطاء الأولوية والتخطيط لأنشطة الاستجابة للمخاطر على جميع المستويات وذلك لتنفيذ خطة الاستجابة للمخاطر التي تم تحديدها حسب مسبقاً، ويشمل ذلك تحديد التكاليف والفوائد ومسؤولية التنفيذ.

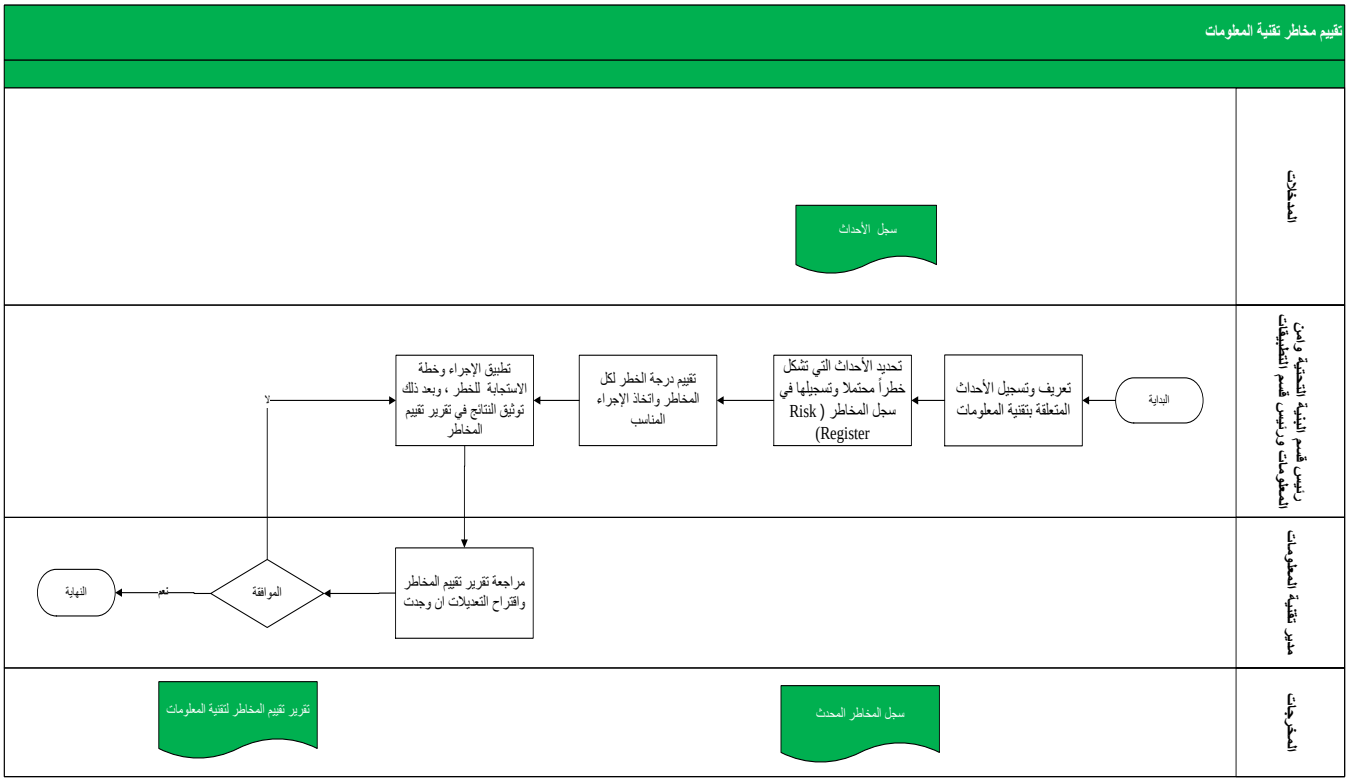
## ٢.٥ الإجراءات

### ١.٢.٥ تقييم مخاطر تقنية المعلومات

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | رئيس البنية التحتية وأمن المعلومات و رئيس التطبيقات | تعريف وتسجيل الأحداث المتعلقة بتقنية المعلومات التي قد تشكل خطرا محتملا على سير الأعمال في الجمعية | | | سجل الأحداث |
| ٢. | رئيس البنية التحتية وأمن المعلومات و رئيس التطبيقات | تحديد الأحداث التي تشكل خطراً محتملا وتسجيلها في سجل المخاطر (Risk Register) | | | سجل المخاطر المحدث |
| ٣. | رئيس البنية التحتية وأمن المعلومات و رئيس التطبيقات | تقييم درجة الخطر لكل المخاطر و وضع التوصية المناسب مثل التجنب (Avoidance) والحد (Reduction)، والتقسيم (Sharing) أو القبول(Acceptance) | | | لا يوجد |
| ٤. | رؤساء الأقسام في إدارة تقنية المعلومات (التطبيقات، البنية التحتية وأمن المعلومات، الدعم الفني) | تطبيق الإجراء وخطة الاستجابة للخطر ، وبعد ذلك توثيق النتائج | | | لا يوجد |
| ٥. | مدير تقنية المعلومات | مراجعة تقرير تقييم المخاطر واجراء التعديلات ان وجد | | | تقرير تقييم المخاطر |

## ٣.٥ دورات العمل

### ١.٣.٥ تقييم مخاطر تقنية المعلومات



# امتلاك وتطبيق

## ٦. سياسة شراء أنظمة وموارد المعلومات

### ١.٦ المقدمة والأهداف

١.١.٦ الغرض من هذا الإجراء هو تنظيم الحصول على الحلول والأنظمة والبنى التحتية التابعة لها (من قبل جهة خارجية) تدعم عمل جمعية مراكز الأحياء بكفاءة وفعالية وفقا لمتطلبات واهداف للجمعية.

### ٢.٦ السياسات

١.٢.٦ التخطيط المسبق لمتطلبات شراء أو تطوير نظام المعلومات:

أ. ينبغي على جمعية مراكز الأحياء أن تطور وتحافظ على وثيقة متكاملة لإدارة دورة حياة تطوير النظام لعمليات التطوير للأنظمة والتطبيقات الرئيسية التي تتم من قبل الجمعية أو جهة خارجية . وتشمل وثيقة دورة حياة تطوير النظام بحد أدنى ما يلي:

- بدء المشروع (التخطيط)
- تحديد المتطلبات (التحليل)
- تصميم النظام
- تطوير النظام
- الفحص
- التطبيق والدعم الفني

٢.٢.٦ الحد الأدنى لإعدادات النظم

أ. يتعين على جمعية مراكز الأحياء إعداد وتوثيق والحفاظ على وجود حد أدنى للإعدادات الخاصة بنظام المعلومات الجديد.

ب. يتعين على جمعية مراكز الأحياء تحديث الإعدادات الأساسية لنظام المعلومات كجزء متكامل من عملية تطبيق أجزاء نظام المعلومات اذا لم تتعارض مع الإعدادات والتقنيات المستخدمة حاليا.

٣.٢.٦ يجب تحديد المواصفات التقنية والوظيفية لعناصر البنية التحتية للأنظمة المزمع تطويرها أو شراؤها.

## ٣.٦ الإجراءات

١.٣.٦ شراء وتطوير أنظمة المعلومات

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | مدير تقنية المعلومات | عندما يجري تطوير نظام معلومات جديد (من مورد او من قبل طرف خارجي)، يقوم مدير إدارة تقنية المعلومات بتعيين فريق داخلي للمشاركة في عملية اختيار وتطبيق النظام. | | | لا يوجد |
| ٢. | قسم التطبيقات | يقوم الفريق بالتنسيق مع المورد الخارجي بتحليل التطبيق عبر عقد ورشات عمل مع المستخدمين النهائيين للتأكد وجمع وتحليل متطلبات الجمعية من التطبيق ومن ثم تبدأ عملية إنشاء التطبيق. | | | لا يوجد |

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ٣. | قسم التطبيقات | يعرض التطبيق على المستخدمين النهائيين وهو في طور الإنشاء للتحقق من ملاءمته للتوقعات وللحصول على ملاحظاتهم وبناءً عليه يتم عمل التغييرات والتعديلات اللازمة. | | | لا يوجد |
| ٤. | قسم التطبيقات | يتم إجراء مراحل الاختبارات للتأكد من تنفيذ الضوابط الأمنية اللازمة.<br>الر جاء مراجعة النموذج رقم ( IT_F005) | | | لا يوجد |
| ٥. | قسم التطبيقات | يقوم الموظف المختص بنقل التطبيق إلى بيئة الإنتاج تحديد أولويات طلب التغيير. | | | لا يوجد |
| ٦. | قسم التطبيقات | يقوم الفريق بالتنسيق مع المورد الخارجي بعقد دورات تدريب للمستخدمين النهائيين. | | | ورش العمل للتدريب على النظام |
| ٧. | قسم التطبيقات | يقوم الفريق بالتنسيق مع مزود خدمه لعمل الصيانة الدورية للتطبيق. | | | خطة الصيانة |

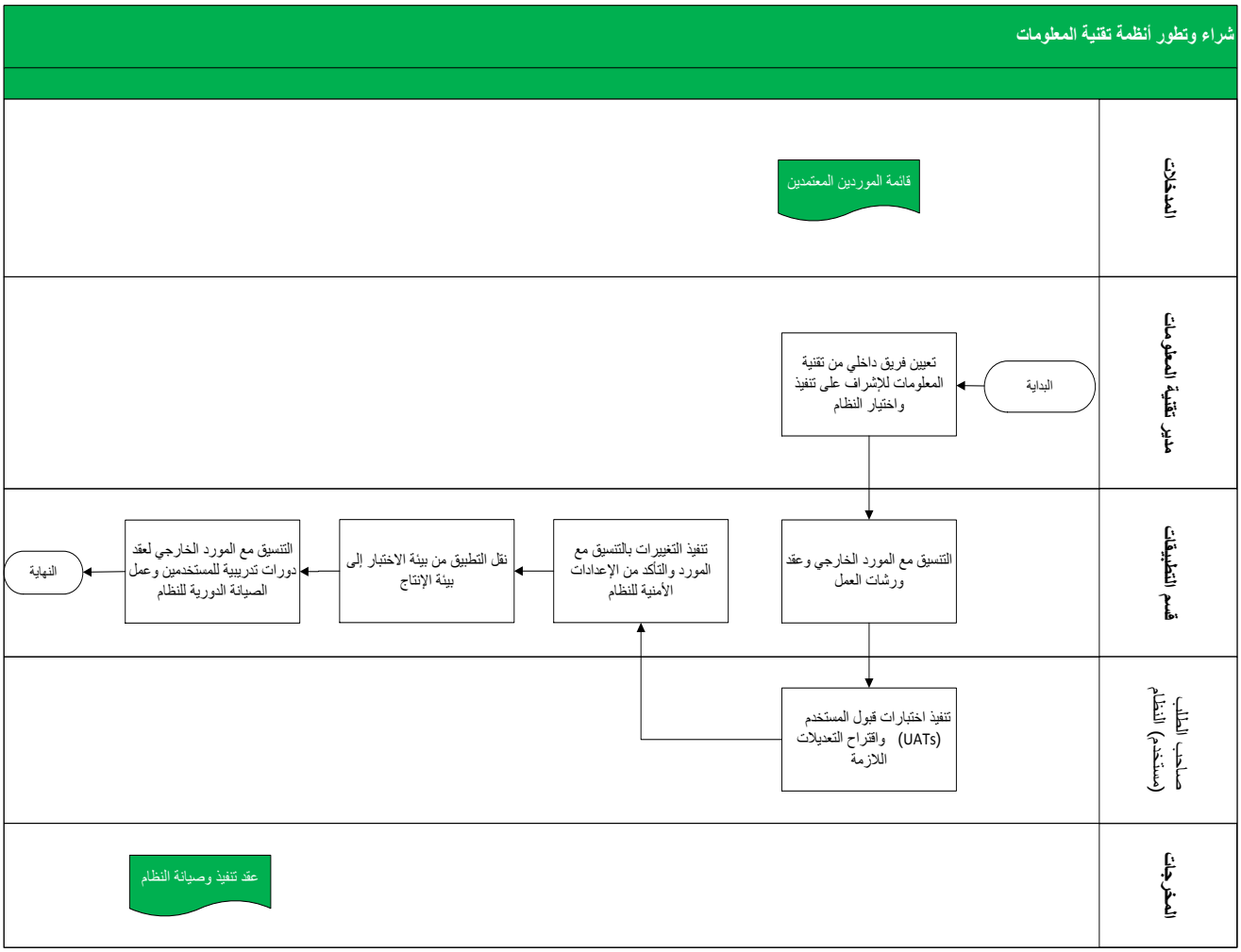
## ٢.٣.٦ شراء عناصر البنية التحتية

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | مدير قسم البنية التحتية وأمن المعلومات | تطوير المتطلبات الفنية للبنى التحتية وفقاً لمتطلبات الأنظمة | | | لا يوجد |
| ٢. | مدير قسم البنية التحتية وأمن المعلومات | تطوير كراسات الشروط والمقاييس (RFPs) من أجل توريد عناصر البنى التحتية | | | كراسة الشروط والمقاييس |

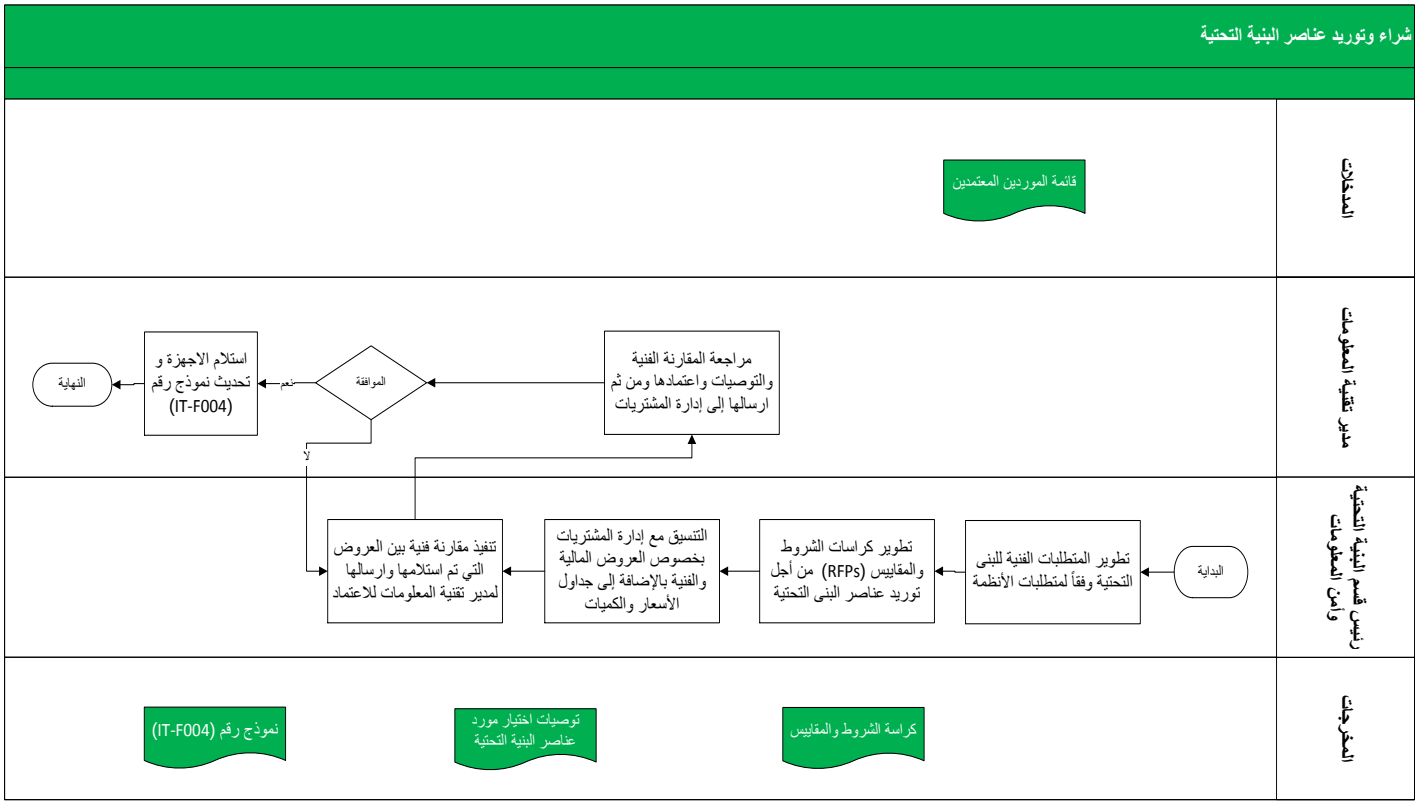
| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ٣. | مدير قسم البنية التحتية وأمن المعلومات | التنسيق مع إدارة المشتريات من أجل الحصول على العروض المالية والفنية بالإضافة إلى جداول الأسعار والكميات | | | لا يوجد |
| ٤. | مدير قسم البنية التحتية وأمن المعلومات | تنفيذ مقارنة فنية بين العروض التي تم استلامها وارسالها لمدير تقنية المعلومات للاعتماد | | | لا يوجد |
| ٥. | مدير تقنية المعلومات | يقوم مدير تقنية المعلومات بمراجعة المقارنة الفنية والتوصيات واعتمادها ومن ثم ارسالها إلى إدارة المشتريات | | | توصيات اختيار مورد البنية التحتية |
| ٦. | مدير قسم البنية التحتية وأمن المعلومات | استلام الاجهزة و تحديث نموذج رقم (IT-F004) | | | |

## ٤.٦ دورات العمل

### ١.٤.٦ شراء وتطوير أنظمة تقنية المعلومات



## ٢.٤.٦ شراء وتوريد عناصر البنية التحتية لتقنية المعلومات



# التقديم والدعم

## ٧. سياسة إدارة التغيير

### ١.٧ المقدمة والأهداف

١.١.٧ الغرض من هذه السياسة هو التأكد من التحكم الفعال بجميع التغييرات التي تطرأ على أنظمة المعلومات الرئيسية أو البنية التحتية لتقنية المعلومات كي يتسنى الحد من احتمالات انقطاع أو توقف خدمات تقنية المعلومات أو الغش والتحايل الناشئ عن التغييرات غير المصرح بها.

### ٢.٧ السياسات

١.٢.٧ يجب أن تتأكد جمعية مراكز الأحياء من القيام بالإدارة والسيطرة على جميع التغييرات بشكل رسمي بما في ذلك التغييرات الاعتيادية أو التغييرات الطارئة على أنظمة المعلومات والبنية التحتية لتقنية المعلومات لدى الجمعية. كما ينبغي أن يتم تسجيل وتقييم التغييرات واعتمادها قبل تنفيذها، ومراجعتها بعد تنفيذها و مقارنتها بالنتائج التي قد تم التخطيط المسبق لها.

٢.٢.٧ ينبغي على جمعية مراكز الأحياء أن تحدد فئات طلبات التغيير لديها بناءً على مدى أهميتها وحسب هو موضح أدناه:

أ. التغيير الاعتيادي: وهي التغييرات على أنظمة المعلومات أو البنية التحتية التي تتطلب فترة مسبقة للمراجعة واعتماد طلب التغيير قبل تنفيذها.

ب. التغيير الطارئ: وهي التغييرات التي يوجد لها أولوية نظراً لأهمية إجرائها بشكل مستعجل وبدون توثيق، مما قد يؤدي الى أثر سلبي على خدمات تقنية المعلومات الرئيسية. وهذا النوع من التغييرات يعطى الأولوية على التغييرات العادية ولا يخضع لمعاييرها نظراً لضيق الوقت ووجوب إجرائه بأسرع ما يمكن.

٣.٢.٧ يتم إجراء جميع التغييرات العادية على أنظمة المعلومات والبنية التحتية لدى جمعية مراكز الأحياء وفقاً لإجراءات إدارة التغيير.

٤.٢.٧ يتعين على جمعية مراكز الأحياء أن تأخذ في اعتبارها آثار التغيير على أمن المعلومات، وأن تتخذ الإجراءات المناسبة للحد من الآثار المترتبة على التغيير وتأثيره على سلامة وأمن المعلومات.

٥.٢.٧ قبل اعتماد وتنفيذ أي تغيير على أنظمة المعلومات، فإنه يجب التأكد من تحديد نظام/ أنظمة المعلومات الأخرى التي قد تتأثر جراء التغيير، وأنه يتم إشراك المسؤولين او الراعين لتلك الأنظمة في العملية، والحصول على الاعتماد المناسب منهم على تنفيذ التغيير/التغييرات.

٦.٢.٧ يسمح فقط بإجراء التغييرات المصرح بها على إعدادات أنظمة المعلومات لدى جمعية مراكز الأحياء.

٧.٢.٧ يتم اعتماد التغييرات العادية على البنية التحتية للتقنية من قبل مدير إدارة تقنية المعلومات.

٨.٢.٧ عند موافقة مدير تقنية المعلومات يفضل اختبار التغييرات في بيئة الفحص أولا قبل التصريح بالموافقة بتطبيق التغيير إلى بيئة الإنتاج.

٩.٢.٧ في حال الحاجة الى إجراء تغييرات واستجابة طارئة على مهمات حرجة، يمكن أن يتم التجاوز مؤقتاً عن إجراءات إدارة التغيير العادي إلى الحد الذي يعتبر ضرورياً لضمان استمرارية الأعمال الأساسية لدى جمعية مراكز الأحياء.

١٠.٢.٧ يجب أن تتم مراجعة واعتماد التغييرات الطارئة من قبل صاحب الصلاحية الذي يعتمد طلب التغيير الطارئ، وهو مدير إدارة تقنية المعلومات او من ينوب عنه

١١.٢.٧ يتم إجراء التغييرات الطارئة بشكل فعال وبالسرعة الواجبة وفقاً لإجراءات التغييرات الطارئة.

١٢.٢.٧ يتم استكمال إغلاق طلب التغيير وتوثيقه وذلك بعد الانتهاء من التغييرات الطارئة، على غرار الإجراءات المتبعة في حالة التغييرات العادية.

١٣.٢.٧ يتم تبليغ طالب التغيير وأصحاب المصلحة المعنيين بآخر المستجدات بشأن حالة التغيير في أنظمة المعلومات

١٤.٢.٧ تقوم إدارة تقنية المعلومات بإعداد وصيانة "سجل متابعة التغييرات" لطلبات التغيير على أنظمة المعلومات والتغييرات المنفذة على أنظمة المعلومات لدى جمعية مراكز الأحياء.

## ٣.٧ الإجراءات

### ١.٣.٧ إنشاء طلب التغيير وتحليله واعتماده

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | مقدم الطلب | **إنشاء طلب التغيير وتحليله واعتماده:**<br>• يقوم مقدم الطلب بتوثيق المعلومات ذات العلاقة عن التغييرات التي يرغب أن تجرى على نظام المعلومات أو البنية.<br>• على مقدم الطلب أن يرسل الطلب الذي وثقه إلى إدارة تقنية المعلومات | | | لا يوجد |
| ٢. | رؤساء أقسام تقنية المعلومات | **تقييم طلب التغيير و اعتماده:**<br>• يجري رئيس قسم البنية التحتية او رئيس قسم التطبيقات تقييماً لطلب التغيير.<br>• إذا كان طلب التغيير عاجلاً (طارئ)، يقوم رئيس فريق الدعم الفني والتقني بإرساله على الفور إلى رئيس الفريق المعني لمراجعته واعتماده.<br>• تعد التغييرات الأخرى تغييرات عادية. وعندها وبناءً على التقييم الأولي، يحدد رئيس قسم البنية التحتية او رئيس قسم التطبيقات أثر التغيير، و بناء عليه يرسل | | | لا يوجد |

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| | | التغييرات إلى مدير إدارة تقنية ونظم المعلومات لمراجعتها واعتمادها (وخصوصاً لمكونات النظم المترابطة *Cross Modules*). | | | |
| ٣. | رؤساء أقسام تقنية المعلومات | **تخطيط وجدولة طلبات التغيير:**<br>• يتم القيام بهذا النشاط لطلبات التغيير المعتمدة.<br>• بناء على الطبيعة المحددة لطلب التغيير المعتمد، يقوم رئيس قسم البنية التحتية او رئيس قسم التطبيقات بالأعمال التالية لطلب التغيير:<br>أ. تحديد أولويات طلب التغيير<br>ب. تحديد وتخصيص الموارد الرئيسية المطلوبة لتنفيذ التغيير<br>ج. بناءً على ما تقدم، يتم تحديد جدول زمني مبدئي لتنفيذ طلب التغيير<br>د. تحديد الأشخاص / الإدارات الأخرى المعنية الذين يمكن أن يتأثروا بالتغيير، ويتعين إبلاغهم بذلك التغيير<br>• يتم توثيق المعلومات أعلاه وتبليغها بصورة رسمية للأطراف التالية:<br>أ. مقدم الطلب<br>ب. الجهات المعنية والذين سيكونون مسئولين عن تنفيذ | | | طلب التغيير |

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| | | التغيير (إدارات الأعمال/ التطبيقات/<br>ج. الأشخاص الآخرين المعنيين المسئولين عن البنية التحتية لتقنية المعلومات التي يمكن أن تتأثر من التغيير<br>الر جاء مراجعة النموذج رقم ( IT_F006) | | | |

٢.٣.٧ تنفيذ التغيير

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | رئيس القسم المختص | **التخطيط التفصيلي لتنفيذ طلب التغيير:**<br>• يتم اسناد طلب التغيير المعتمد إلى رئيس الفريق المعني(الشبكات، نظم المعلومات، البنية التحتية وأمن المعلومات)<br>استناداً إلى طبيعة التغيير.<br>• يعتبر الشخص الذي تم تكليفه بمثابة "المسؤول عن التغيير"، ويجب أن يكون مسؤولاً عن تنفيذ التغيير.<br>• يقوم المسؤول عن التغيير بإعداد | | | لا يوجد |

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| | | خطة بأنشطة محددة للطلبات ، كي يتم القيام بها لتنفيذ طلب التغيير المعتمد، ويقوم كذلك بترتيب الموارد المطلوبة. | | | |
| ٢. | رؤساء أقسام تقنية المعلومات | **بناء التغييرات من أجل تطبيقها:**<br>• يقوم المسؤول عن التغيير مع فريق العمل التابعة له بتطوير / شراء عناصر البنية التحية المطلوبة لطلب التغيير المعتمد.<br>• ويتم تطبيق الخطوات ذات العلاقة لدورة تطوير الأنظمة أو شراؤها لدى إدارة تقني ونظم المعلومات وذلك حسب طلب التغيير المعتمد للطلبات. | | | لا يوجد |
| ٣. | | **فحص التغييرات التي سيتم تطبيقها ، وتطوير خطة التراجع عن التغيير المعتمد:**<br>• يفضل أن يتم فحص التغييرات في بيئة الفحص باستخدام الأساليب المناسبة.<br>• يتم تطوير خطة التراجع عن التغيير، لتنفيذها في حال عدم نجاح تنفيذ التغيير. | | | لا يوجد |
| ٤. | رئيس القسم المختص | **تنفيذ التغييرات:**<br>• يتم ادخال التغيير للطلبات في بيئة الانتاج. ويتم اختيار فترة مناسبة للحد من أثر التغيير على خدمات تقنية المعلومات.<br>• يتم إبلاغ جميع الأطراف ذات | | | لا يوجد |

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| | | العلاقة التي قد تتأثر من التغيير للطلبات وذلك قبل تطبيق التغيير في بيئة الانتاج.<br>• يتم تطبيق التغيير المعتمد والمفحوص في بيئة الانتاج من قبل الأشخاص المصرح لهم بذلك.<br>• يتم فحص التغيير المنفذ للتأكد من تأديته لوظائفه بشكل ملائم.<br>• في حال ظهور مشاكل ناتجة عن التغيير، يتم عكس العملية وفقاً لخطة التراجع المحددة. | | | |
| ٥. | رئيس القسم المختص | **إغلاق طلب التغيير:**<br>• تتم مراجعة جميع التغيرات المنفذة من قبل رئيس قسم البنية التحتية او رئيس قسم التطبيقات بتحديث حالة التغييرات المنفذة بنجاح بأنها "أغلقت".<br>• يتم تبليغ مقدم طلب التغيير رسمياً بشأن إغلاق طلب التغيير. | | | التغيير المنفذ |

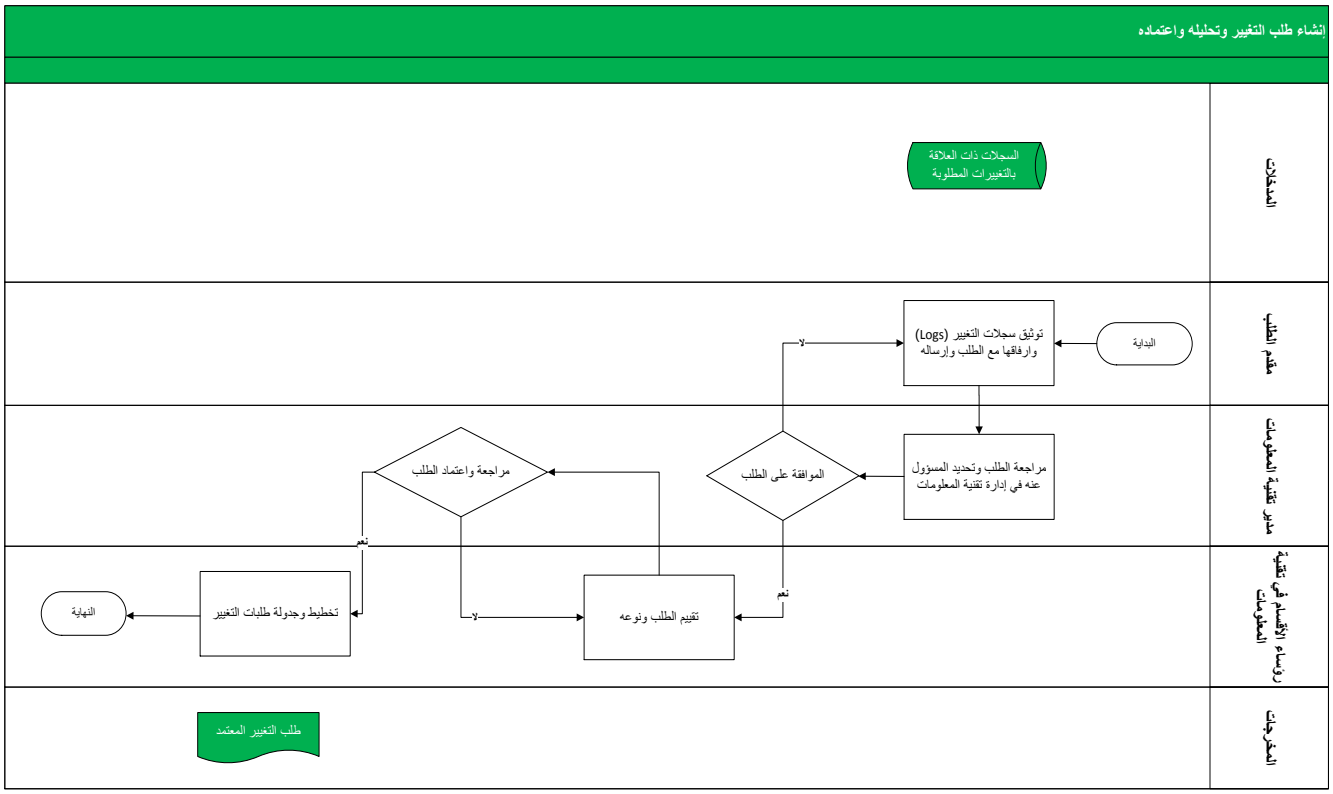
### ٣.٣.٧ تنفيذ التغييرات الطارئة

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | مدير تقنية المعلومات | يقوم مدير تقنية المعلومات او من ينوب عنه باعتماد طلبات التغيير الطارئة بمراجعة طلب التغيير في | | | لا يوجد |

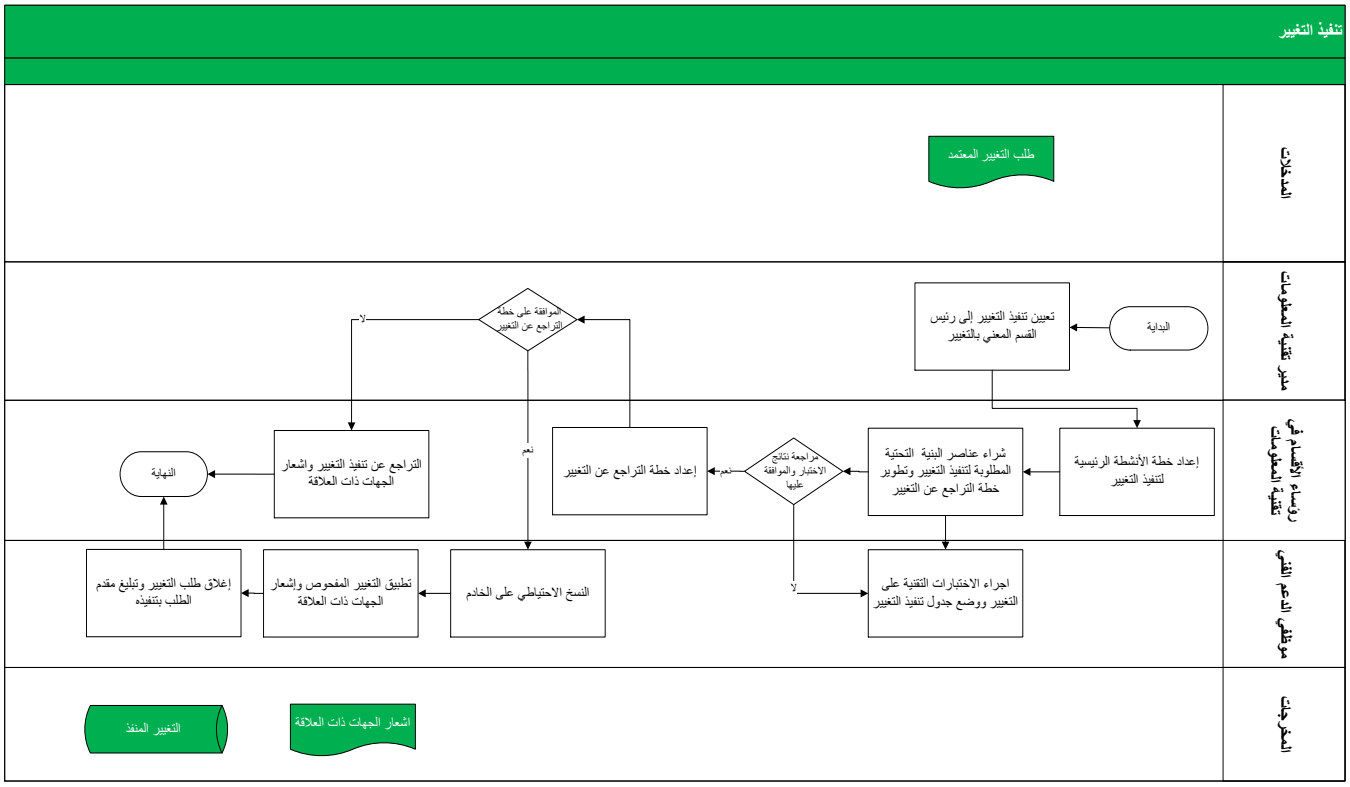
| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| | | ضوء المعلومات المقدمة له، والتشاور مع الأشخاص الآخرين المعنيين، ومن ثم يوافق على طلب التغيير أو يرفضه. | | | |
| ٢. | رؤساء الأقسام في تقنية المعلومات | يجب تنفيذ طلب التغيير الطارئ المعتمد وفقاً لإجراء تنفيذ التغيير. غير أن ثمة أنشطة تتطلب وثائق تفصيلية يمكن تجاوزها مؤقتاً عند تنفيذ التغييرات المستعجلة. | | | لا يوجد |
| ٣. | رؤساء الأقسام في تقنية المعلومات | بعد تنفيذ التغيير الطارئ، يقوم المسئول عن ذلك التغيير بالتأكد من اتمام عملية التوثيق المطلوبة. | | | لا يوجد |
| ٤. | رؤساء الأقسام في تقنية المعلومات | بعد احتواء الوضع الطارئ الذي استدعى التغيير المستعجل، يقوم رئيس قسم البنية التحتية او رئيس قسم التطبيقات بمراجعة التغييرات الطارئة التي تمت، وتقرر فيما إذا كان سيتم الإبقاء على تلك التغييرات بشكل دائم، أو إجراء تعديلات / تحسينات إضافية عليها. | | | التغيير الطارئ المنفذ |

## ٤.٧ دورات العمل

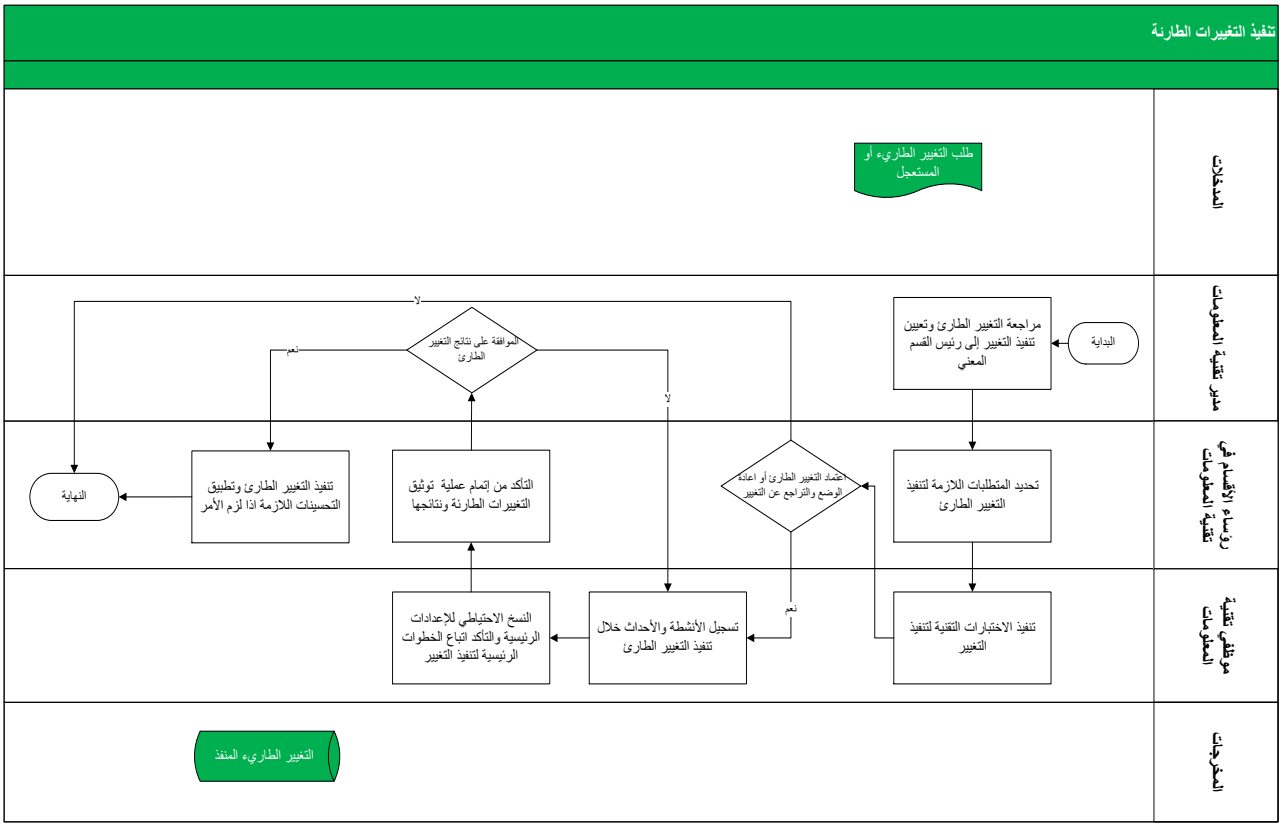
### ١.٤.٧ إنشاء طلب التغيير وتحليله واعتماده



## ٢.٤.٧ تنفيذ التغيير



## ٣.٤.٧ تنفيذ التغييرات الطارئة



## ٨. سياسة إدارة عمليات التشغيل في تقنية المعلومات

### ١.٨ المقدمة والأهداف

١.١.٨ الغرض من هذه السياسة هو تحديد جدول فعال لإدارة عمليات تقنية المعلومات بما يتضمن الدعم الفني والصيانة.

### ٢.٨ السياسات

١.٢.٨ الصيانة:

أ. يجب أن تخضع البنية التحتية والنظم في جمعية مراكز الأحياء للصيانة الوقائية والدورية لضمان استمرارية عملها وتحسين مستوى الخدمة في ادارة تقنية المعلومات.

ب. يجب أن تتم جدولة أعمال الصيانة الدورية بحيث لا تعطل الأنظمة ، وعدم جدولتها بالتزامن مع تنفيذ أنشطة تقنية المعلومات مثل النسخ الاحتياطي(backup) أو الاسترجاع(restoration).

٢.٢.٨ الدعم الفني/ وتقديم خدمات تقنية المعلومات:

أ. أن تحل القضايا المتعلقة بنظم المعلومات بطريقة منظمة وفعاله من خلال اعتماد نقطة اتصال موحدة لاستقبال ومتابعة البلاغات.

ب. القدرة على متابعة وتحديث الحالات (طلبات الخدمة/ البلاغات) الكترونيا.

ج. القدرة على عمل التقارير الدورية لمعرفة أداء الدعم الفني.

د. القدرة على أرشفة وحفظ الحالات الخاصة الكترونيا ليتم الاستعانة بها مستقبلا

هـ. انشاء قائمة معرفة لجميع خدمات تقنية المعلومات التي تقدمها للمستخدمين وتحديد متطلبات الحصول على كل خدمة

## ٣.٨ الإجراءات

### ١.٣.٨ الصيانة:

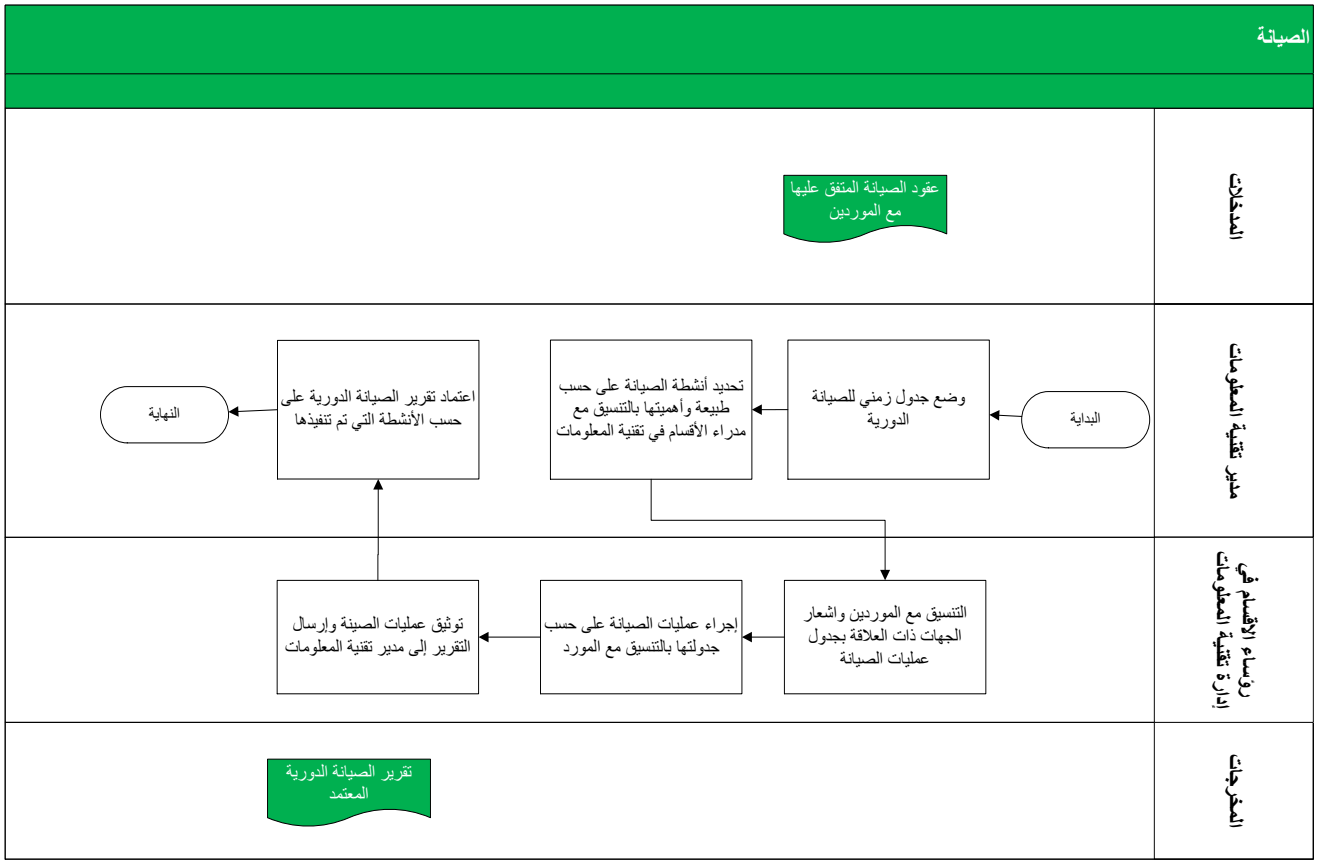
| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | مدير تقنية المعلومات | وضع جدول زمني للصيانة الدورية (تتناسب مع طبيعة وحساسية كل أصل يستخدم لدعم الأنظمة). | | | جدول الصيانة |
| ٢. | رؤساء الأقسام في تقنية المعلومات | تحديد أنشطة الصيانة التي سوف تؤثر على الأعمال اليومية بالتنسيق مع رؤساء الاقسام والتوجيه من خلال مدير ادارة تقنية المعلومات. | | | لا يوجد |
| ٣. | رؤساء الأقسام في تقنية المعلومات | إعلام الأطراف المعنية بأوقات الصيانة مسبقاً بحث يتم التحضير لذلك | | | لا يوجد |
| ٤. | موظفي تقنية المعلومات | إجراء الصيانة للأصول استنادا إلى جدول الصيانة الدورية. | | | لا يوجد |
| ٥. | موظفي تقنية المعلومات | توثيق تفاصيل أعمال الصيانة ، وحالة الأجهزة، والإضافات إلى الأصول وغيرها، ويقدم تقريراً إلى مدير ادارة تقنية المعلومات. | | | تقرير الصيانة |

## ٢.٣.٨ الدعم الفني وتقديم خدمات تقنية المعلومات:

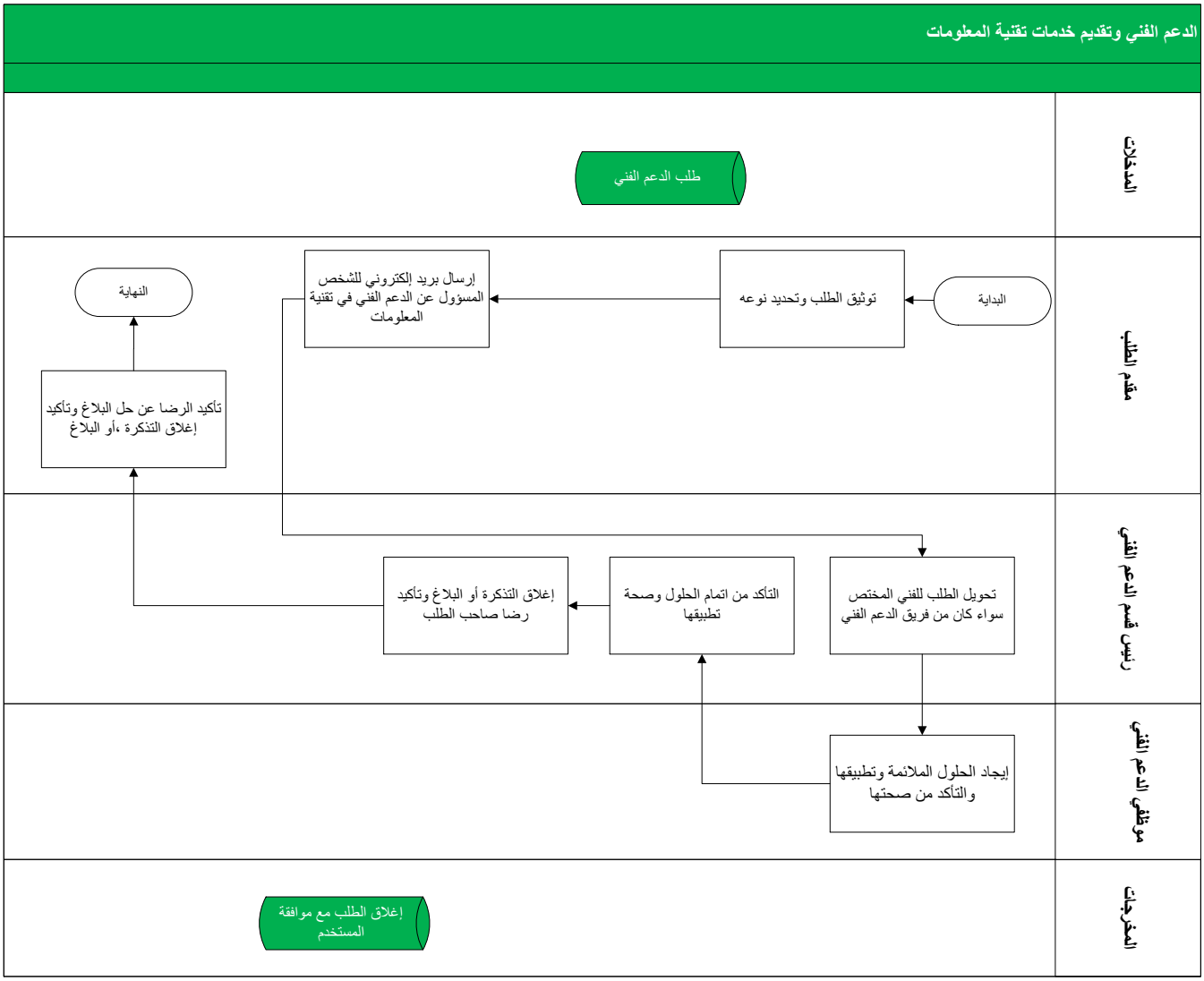
| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | مقدم الطلب | عند الحاجة لخدمات الدعم الفني (حدوث عطل، طلب أجهزة ...الخ) يقوم المستخدم إما بالدخول إلى نظام الدعم الفني لتسجيل طلب الخدمة/ أو البلاغ أو يقوم بالاتصال بالمنسق المسؤول. | | | طلب الدعم |
| ٢. | موظفي الدعم الفني | يقوم المنسق المسئول بتحويل طلب الخدمة/ أو البلاغ إلى الفنيين المختصين لدراسة الحالة والوقوف على مسبباتها وكيفية المضي قدما. | | | لا يوجد |
| ٣. | الدعم | يقوم الفني المختص بإيجاد الحلول الملائمة وتطبيقها والتأكد من صحتها. | | | لا يوجد |
| ٤. | الدعم | يقوم منسق الدعم الفني بإبلاغ المستخدم بإتمام الخدمة/ أو البلاغ وحل العطل والطلب منه التأكد من أن العطل قد تم حله ومن ثم إغلاق الخدمة/ أو البلاغ. | | | لا يوجد |
| ٥. | الدعم | يقوم المستخدم من التأكد ومن ثم إغلاق الخدمة/ أو البلاغ<br><br>الر جاء مراجعة النموذج رقم ( IT_F001) | | | لا يوجد |

## ٤.٨ دورات العمل

### ١.٤.٨ الصيانة:



## ١.٤.٨ الدعم الفني وتقديم خدمات تقنية المعلومات:



## ٩. سياسة ضمان استمرارية الأعمال

### ١.٩ المقدمة والأهداف

١.١.٩ الغرض من هذه السياسة هو تحديد الإجراءات المناسبة الواجب اتخاذها لتخفيف آثار حدوث أي توقف أو انقطاع لأنشطة العمل، وحماية عمليات/ أنشطة العمل من الآثار الناجمة عن إخفاق/ تعطل أنظمة المعلومات أو الكوارث، والتأكد من استعادة الأنظمة بأسرع ما يمكن.

### ٢.٩ السياسات

١.٢.٩ استمرارية النشاط وتقييم المخاطر:

أ. ينبغي على جمعية مراكز الأحياء أن تطبق إطاراً مناسباً لإدارة استمرارية النشاط للحد من التأثير التي قد تتعرض له الجمعية ، واسترجاع خسارة المعلومات التي فقدت أثناء الكوارث الرئيسية مثل الحريق، الفيضان، الهزات الأرضية، العواصف، الأعطال الرئيسية لنظام تقنية المعلومات (الأجهزة)، فقد سجلات البيانات (البرامج)، فقد خدمات المنافع لفترة طويلة، الاضطرابات المدنية والإضرابات، فقد الموارد، إلخ.

ب. يجب أن يستند تخطيط استمرارية النشاط على المخاطر المحددة التي من شأنها أن تسبب انقطاع عمليات/ خدمات النشاط، وعلى تحليل المخاطر وتأثيرها، لتحديد إمكانية وأثر تلك الانقطاعات من حيث الفترات الزمنية، ونطاق الضرر الواقع، وفترة الاستعادة.

ج. تقوم جمعية مراكز الأحياء ، بمشاركة كاملة من المسئولين عن العمليات/ الخدمات، وموارد العمل الأخرى المرتبطة ببيئة أنظمة المعلومات بإجراء تقييم

للمخاطر المترتبة على التوقف أو التغيير في بيئة أنظمة المعلومات، يتبعه تحليل آثار التغيير.

د. يجب أن يشتمل تقييم المخاطر المترتبة على توقف أنظمة المعلومات على تحديد المخاطر وأولوياتها مقابل معايير وأهداف جمعية مراكز الأحياء، وأن يتضمن الموارد الهامة ، أثر انقطاع/ توقف العمل بأنظمة وتقنية المعلومات ، والفترات المسموح بها لانقطاع الخدمة، وأولويات الاستعادة.

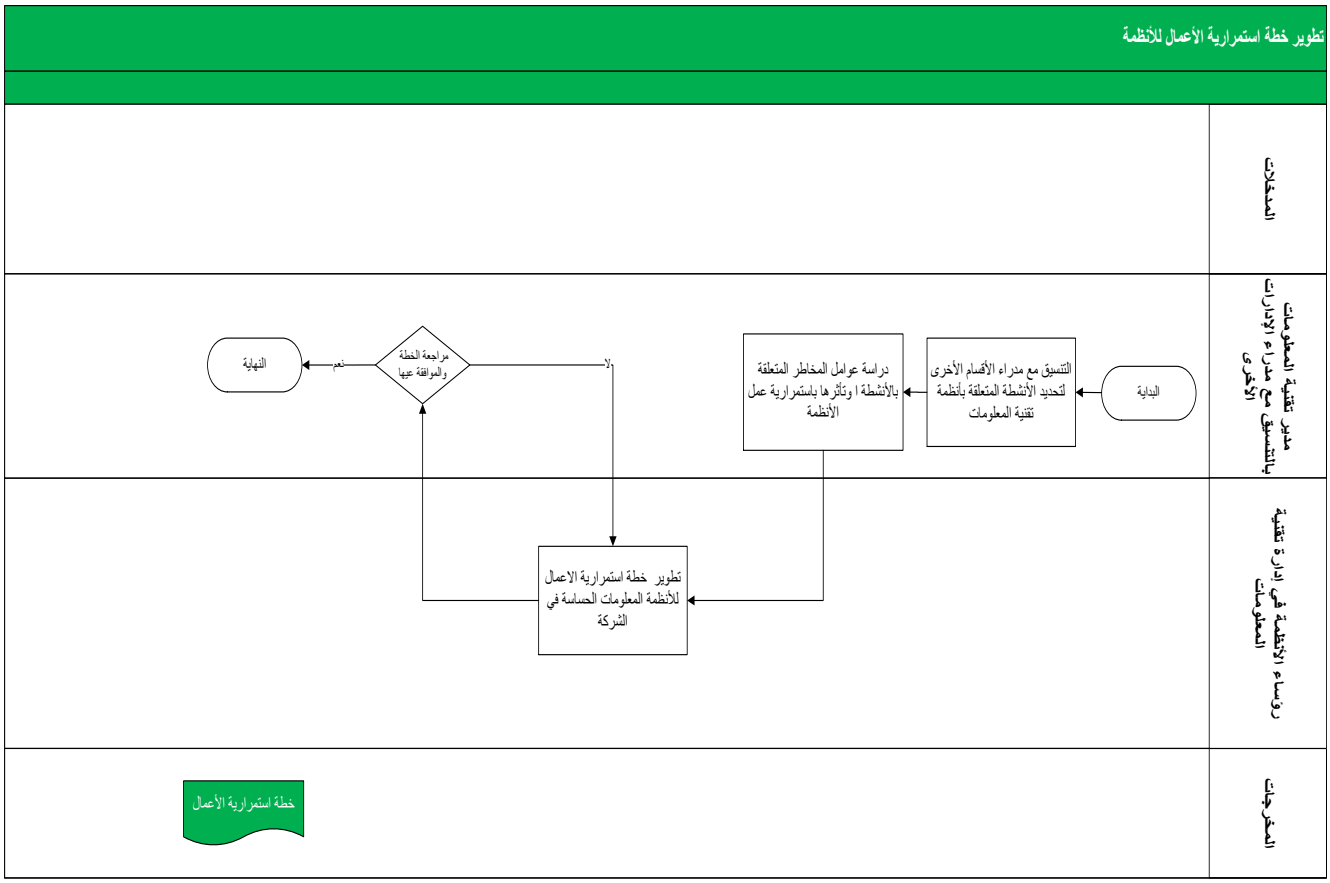
## ٣.٩ الإجراءات

### ١.٣.٩ تطوير خطة استمرارية الأعمال

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | مدير تقنية المعلومات<br>مدراء الإدارات الأخرى | التنسيق مع مدراء الأقسام الأخرى لتحديد الأنشطة المتعلقة بأنظمة تقنية المعلومات | | | |
| ٢. | مدير تقنية المعلومات | دراسة عوامل المخاطر المتعلقة بالأنشطة ا وتأثرها باستمرارية عمل الأنظمة | | | |
| ٣. | رؤساء الأقسام (البنية التحتية ، والتطبيقات) | تطوير خطة استمرارية الاعمال للأنظمة المعلومات الحساسة في الشركة | | | |
| ٤. | مدير تقنية المعلومات | مراجعة خطة استمرارية الأعمال والموافقة عيها | | | خطة استمرارية الأعمال |

## ٤.٩ دورات العمل

### ١.٤.٩ تطوير خطة استمرارية الأعمال



## ١٠. سياسة معدل الاستخدام الأمثل للأنظمة

### ١.١٠ المقدمة والأهداف

١.١.١٠ الغرض من هذه السياسة هو وضع قواعد الاستخدام المقبول لأنظمة المعلومات لدى جمعية مراكز الأحياء.

### ٢.١٠ السياسات

١.٢.١٠ الاستخدامات العامة ومسؤولية الائتمان:

أ. يصرح للمستخدمين باستخدام مصادر المعلومات لدى جمعية مراكز الأحياء فقط لأغراض العمل المصرح لهم القيام بها. وسيتعرض المستخدم الذي يخالف ذلك للإجراءات التأديبية و/أو القانونية المناسبة.

ب. تؤول ملكية كافة بيانات الحاسب الآلي التي تم إنشاؤها أو استلامها أو إرسالها باستخدام أنظمة المعلومات لدى جمعية مراكز الأحياء لملكية جمعية مراكز الأحياء ولا تعتبر مملوكة من قبل المستخدم. وتحتفظ جمعية مراكز الأحياء بحقها بفحص كافة البيانات لأي سبب ودون إخطار، ومثال ذلك عندما تكون هناك شبهات بمخالفة هذه القواعد أو أية سياسات وإجراءات لدى جمعية مراكز الأحياء.

ج. ينبغي على الموظفين والمقاولين و المستخدمين من طرف ثالث الذين يستخدمون أو الذين لديهم إمكانية الوصول إلى معلومات جمعية مراكز الأحياء أن يكونوا على دراية بالحدود الحالية لاستخدامهم لأنظمة المعلومات لدى جمعية مراكز الأحياء، وهم مسئولون عن استخدامهم لأنظمة المعلومات وأي استخدام يتم تحت مسئوليتهم.

٢.٢.١٠ حقوق الملكية الفكرية والترخيص:

أ. جمعية مراكز الأحياء تقدر وتحترم حقوق الملكية الفكرية (التي تشمل حقوق النسخ، وحقوق التصميم، وحقوق براءة الاختراع وتراخيص الشفرات المصدرية للبرامج والوثائق) المرتبطة بأنظمة المعلومات لديها.

ب. يمنع انتهاك أي حقوق لأي شخص أو جمعية محمية بحقوق النسخ أو براءة الاختراع أو حقوق الملكية الفكرية الأخرى، أو الأنظمة واللوائح المشابهة، بما في ذلك، ودون حصر، تركيب البرامج غير المصرح بها أو غير القانونية على أنظمة جمعية مراكز الأحياء، أو الأنظمة الأخرى غير التابعة إلى جمعية مراكز الأحياء لكنها موصولة مع بيئة تقنية المعلومات لدى جمعية مراكز الأحياء.

ج. يجب أن تحتفظ إدارة تقنية المعلومات بمعلومات مناسبة عن التراخيص والأحكام والشروط المتعلقة بأنظمة المعلومات الهامة التي لديها.

د. يمنع منعاً باتاً استخدام برمجيات أو حقوق ملكية فكرية غير مرخصة.

٣.٢.١٠ الاستخدام غير المقبول للأنظمة والشبكة:

أ. يمنع إدخال برامج خبيثة (مثل الفيروسات، الشيفرات الخبيثة، أحصنة طروادة، إلخ) إلى أنظمة المعلومات لدى جمعية مراكز الأحياء.

ب. يمنع إدخال البرامج المجانية أو المشتركة في شبكة الجمعية سواء تم تحميلها من الإنترنت أو تم الحصول عليها من وسائط أخرى، دون تفويض من إدارة تقنية المعلومات.

ج. يمنع تقديم عروض أو منتجات أو بنود أو خدمات تنطوي على الغش والخداع باستخدام موارد الأنظمة لدى جمعية مراكز الأحياء.

د. يمنع الكشف عن كلمات المرور التي يستخدمها الآخرون للدخول إلى حساباتهم أو السماح باستخدام تلك الحسابات من قبل أطراف أخرى.

ه. يمنع إجراء مسح للمنافذ أو مسح أمني لشبكة معلومات الجمعية أو نظام معلوماتها إلا إذا كان ذلك مصرحاً به من قبل مدير تقنية المعلومات ويتم إرسال إشعارات مسبقة بذلك للأشخاص المعنيين.

و. يمنع تنفيذ أي شكل من أشكال مراقبة الشبكة والتي يتم خلالها اعتراض البيانات التي لا تعني الجهاز المضيف لحساب الموظف، إلا إذا كان هذا النشاط جزءاً من الوظيفة/ المهمة المصرح بها للموظف او بطلب من الادارة المعنية وبموافقة ادارة تقنية و نظم المعلومات

ز. يمنع التحايل أو الالتفاف حول تعريف هوية المستخدم أو أمن أي مضيف أو شبكة أو حاسوب.

ح. يمنع استخدام أي برنامج/ لغة/ أمر، أو إرسال الرسائل من أي نوع، بغرض التداخل مع أو تعطيل طرفيه أي مستخدم، من خلال أية وسائل، محلياً أو عبر الإنترنت/ الإنترانت/ الإكسترانت.

ط. يمنع تزويد معلومات تتعلق بموظفي جمعية مراكز الأحياء أو قوائم بأسمائهم إلى أي أطراف خارج الجمعية.

٤.٢.١٠ استخدام البريد الإلكتروني والاتصالات:

أ. يمنع إرسال أية رسائل بريد إلكتروني غير مطلوبة (طوعية unsolicited) بما في ذلك إرسال "البريد غير النافع Junk" أو المواد الإعلانية الأخرى إلى الأشخاص الذي لم يطلبوا تلك المواد بصفة محددة (رسائل البريد الإلكتروني الاقتحامية).

ب. تمنع المضايقة عبر البريد الإلكتروني سواء من حيث اللغة أو بتكرار أو حجم الرسائل.

ج. يمنع منعاً باتاً الاستخدام غير المصرح به أو تزوير معلومات ترويسة البريد الإلكتروني أو محتوياتها.

د. يمنع إنشاء أو تحرير "الرسائل التسلسلية chain letters" أو "Ponzi" أو برامج "هرمية pyramid schemes" من أي نوع.

ه. يجب أن لا يتوقع موظفو جمعية مراكز الأحياء أية خصوصية لأي شيء يقومون بتخزينه أو إرساله أو استلامه عبر نظام البريد الإلكتروني للجمعية . ويجوز لجمعية مراكز الأحياء مراقبة الرسائل دون سابق إشعار و بعد اخذ موافقة الإدارة المعنية وإدارة تقنية المعلومات.

و. ينبغي على موظفي جمعية مراكز الأحياء توخي الحذر عند إرسال أي بريد إلكتروني من داخل جمعية مراكز الأحياء إلى شبكات خارجها.

٥.٢.١٠ إبداء العناية الواجبة:

أ. يكون كل مستخدم مسئولاً عن منع الوصول غير المصرح به، بما في ذلك المشاهدة، إلى مصادر المعلومات الواقعة تحت مسئوليته أو تحكمه (مثل المعلومات

المتوفرة في الأجهزة المحمولة، أجهزة سطح المكتب، طرفيات الدخول، الطابعات، أو وسائط الأشرطة، إلخ).

ب. يكون كل مستخدم مسئولاً عن إبلاغ إدارة تقنية المعلومات بأي سلوك يشتبه بأنه ناتج عن الفيروسات أو أي أنشطة مشبوهة في أنظمتهم.

ج. من المقبول تصفح النطاق العام لإجراء بعض البحث شريطة التزام المستخدمين بسياسات ومعايير وإجراءات جمعية مراكز الأحياء فيما يتعلق بهذا الاستخدام. كما أن على المستخدمين في هذه الحالة الالتزام بسياسات ومعايير وإجراءات المواقع التي يبحثون فيها.

٦.٢.١٠ سياسة استخدام الإنترنت:

أ. تقوم ادارة تقنية المعلومات بتوعية المستخدمين عن الاستخدام الامثل للأنترنت و ان الجمعية لن تقف مكتوفة الأيدي نحو إساءة استخدام الإنترنت، وخصوصاً الأنشطة التي قد تعرضها للملاحقة القضائية أو إجراءات قانونية (ويشمل ذلك الإباحية، ومضايقة الأشخاص). وستتخذ الجمعية الإجراءات التأديبية المناسبة والتي قد تصل إلى فصل الموظف، في حالة قيام المستخدم بأي أنشطة غير قانونية، فإن جمعية مراكز الأحياء تحتفظ بحقها بالتبليغ عن هذه الأنشطة إلى السلطات التنظيمية أو الحكومية أو القانونية ذات العلاقة.

ب. تقوم جمعية مراكز الأحياء بحجب فئات محددة من المواقع الإلكترونية تحددها الجمعية. و. وإذا ما تم الدخول إلى أي موقع إلكتروني غير قانوني أو لا يتعلق بالعمل، فإن ذلك لا يعني أن جمعية مراكز الأحياء قد صرحت بالدخول إليه أو

اعتبرته مقبولاً. بالتالي، فعلى المستخدمين عدم زيارة مثل تلك المواقع الإلكترونية التي قد تعتبر غير قانونية أو غير أخلاقية أو تتنافى مع مبادئ الجمعية.

ج. على المستخدم فهم الوقت الذي يقضيه في الاستخدام الشخصي للإنترنت والذي يمكن اعتباره مقبولاً. وللمستخدم استشارة مدير إدارته لاستيضاح هذه المتطلبات.

د. يجب عدم استخدام عناوين البريد الإلكتروني العامة أو الشخصية لإرسال رسائل إلكترونية تتضمن معلومات تتعلق بالعمل الا في الحالات الاستثنائية.

ه. على المستخدم ملاحظة أن رسائل البريد الإلكترونية المرسلة من أجهزة الكمبيوتر الخاصة بالعمل باستخدام حسابات البريد الإلكترونية العامة مثل ياهو(Yahoo) وجي ميل(Gmail) وغيرهما يمكن أن يتم تتبعها من قبل المستلم كونها مرسلة من جمعية مراكز الأحياء. وبالتالي، فإن أية إساءة استخدام يمكن أن تعرض الجمعية إلى الإجراءات القضائية.

و. إذا كان هناك مواقع معينة تم حجبها وكان واجباً ألا يتم حجبها (أو بالعكس)، فعلى المستخدم إشعار إدارة أمن المعلومات بذلك.

ز. إذا قام المستخدم بشكل عرضي بزيارة موقع غير لائق، أو إذا تم توجيهه آلياً إلى ذلك الموقع، فإن عليه مغادرة ذلك الموقع فوراً.

ح. على المستخدمين الامتناع عن تنزيل أي برمجيات لا علاقة لها بالعمل.

ط. أثناء تنزيل المعلومات المتعلقة بالعمل، ينبغي على المستخدم التأكد من عدم مخالفة أي حقوق ملكية فكرية مما قد يعرض الجمعية لمخاطر الإجراءات القضائية.

ي. على جمعية مراكز الأحياء بأن المعلومات المتاحة على موقعها الإلكتروني قد تم التحقق منها والتأكد من صحتها بشكل ملائم.

## ٣.١٠ الإجراءات

١.٣.١٠ لا تحتاج هذه السياسة لإجراءات تشغيلية بموجب هذا الإطار. وقد تم تحديد الخطوات العملية المطلوب اتباعها ضمن السياسة.

## ١١. سياسة إدارة الخدمات المقدمة من طرف ثالث

### ١.١١ المقدمة والأهداف

١.١.١١ الغرض من هذه السياسة هو التأكد من أن جمعية مراكز الأحياء تدير مخاطر أمن المعلومات التي قد تنجم عن أنشطة الأطراف الثالثة التي تقدم خدماتها للجمعية والتي قد تسبب خطر للأنظمة.

### ٢.١١ السياسات

١.٢.١١ إدارة العقود:

أ. يجب توقيع اتفاقية رسمية بين جمعية مراكز الأحياء وكافة الأطراف الثالثة التي تقدم خدماتها إلى جمعية مراكز الأحياء.

ب. يتم تقديم الضوابط المتعلقة بسياسات وإجراءات أمن معلومات جمعية مراكز الأحياء إلى المقاولين / الموردين الذي يتعين عليهم قراءة وفهم سياسات وإجراءات أمن المعلومات وإقرارهم بقبولها.

ج. تحتفظ جمعية مراكز الأحياء بحقها في رفض خدمات أي موظفين تابعين لأي طرف ثالث بناءً على كفاءتهم الفنية وقدراتهم التنفيذية والاعتبارات الأمنية وأي جوانب أخرى متعلقة بهذا الصدد و التي أن تسبب ضرر لجمعية مراكز الأحياء.

٢.٢.١١ تبادل المعلومات:

أ. على جمعية مراكز الأحياء أن تفرض على جميع الأطراف الثالثة توقيع اتفاقية رسمية لعدم الإفصاح قبل مشاركتهم في معلوماتها السرية.

٣.٢.١١ إدارة أداء الأطراف الثالثة:

أ. يقوم مدير تقنية المعلومات بمراقبة أداء الطرف الثالث والتأكد من التزامه بما تم النص عليه في اتفاقية الخدمة (Service Level Agreement) ، في حالة إخلال الطرف

الثالث للعقد، لإدارة تقنية المعلومات اتخاذ الإجراء اللازم وذلك بموجب اتفاقية العقد الموقعة مع ذلك الطرف.

ب. تضطلع الإدارات المعنية لدى جمعية مراكز الأحياء والتي تحصل على الخدمات التي تم إسنادها إلى أطراف الثالثة مسؤولة عن مراقبة وتقديم تقارير لأداء تلك الأطراف مقارنة بمتطلبات العقد، وذلك بهدف توفير مرئيات بناءة لتحسين مستوى الخدمات المقدمة من الأطراف الثالثة.

## ٣.١١ الإجراءات

١.٣.١١ لا تحتاج هذه السياسة لإجراءات تشغيلية بموجب هذا الإطار. وقد تم تحديد الخطوات العملية المطلوب اتباعها ضمن السياسة.

## ١٢. سياسة النسخ الاحتياطي والاسترجاع في حال الكوارث

### ١.١٢ المقدمة والأهداف

١.١.١٢ الهدف من هذه السياسة هو التأكد من أن يتم عمل نسخ احتياطية مساندة للمعلومات الإلكترونية و استرجاعها من قبل جمعية مراكز الأحياء بشكل مخطط وسريع وفعال وآمن بناء على متطلبات العمل.

### ٢.١٢ السياسات

١.٢.١٢ متطلبات النسخ الاحتياطية

أ. يتم اخذ نسخ احتياطية من البيانات الإلكترونية المخزنة في أنظمة المعلومات لدى جمعية مراكز الأحياء بناءً على احتياجات العمل ووفقاً لإجراءات معرفة في خطة النسخ الاحتياطية والمعتمدة لدي إدارة تقنية المعلومات.

ب. تكون إدارة تقنية المعلومات مسؤولة عن أخذ النسخ الاحتياطية لجميع أنظمة تقنية المعلومات التي تديرها، وذلك وفقاً لخطط النسخ الاحتياطية التي تم تطويرها لتلك الأنظمة.

ج. يكون جميع موظفي جمعية مراكز الأحياء مسؤولين عن أخذ النسخ الاحتياطية الخاصة بهم على خوادم ملفات الشبكة أو الوسط المختار للنسخ الاحتياطية.

٢.٢.١٢ وسائط النسخ الاحتياطية

أ. يجب استخدام وسائط مناسبة لتخزين النسخ الاحتياطية، بحيث التأكد من أنها خالية من الأخطاء وصالحة للاستخدام.

ب. يجب استبدال وسائط تخزين النسخ الاحتياطية بعد مواجهة أي خطأ أو على فترات زمنية محددة مسبقاً أيهما يقع أولاً.

ج. يتم وضع ملصقات الباركود المناسبة على وسائط تخزين النسخ الاحتياطية وترقيمها آلياً حسب متطلبات نظام النسخ الاحتياطية.

د. يتوجب على رئيس قسم البنية التحتية متابعة استخدام وسائط النسخ الاحتياطية، على أن يتم استبدال تلك الوسائط بعد استخدامها حسب نظام النسخ الاحتياطية.

٣.٢.١٢ الاحتفاظ بالبيانات

أ. تقوم إدارة تقنية المعلومات بالتأكد من الاحتفاظ بنسخ احتياطية للبيانات الخاصة بأنظمة المعلومات، للمدة المطلوبة من قبل جمعية مراكز الأحياء، أو حسب متطلبات النظام.

٤.٢.١٢ استرجاع النسخ الاحتياطية:

- يتم استرجاع النسخ الاحتياطية على أساس الحاجة، وبناءً على تفويض مناسب من مدير إدارة تقنية المعلومات.
- يتم استرجاع النسخ الاحتياطية وفقاً لإجراءات استرجاع النسخ الاحتياطية.

٥.٢.١٢ فحص استرجاع النسخ الاحتياطية:

أ. تقوم إدارة تقنية المعلومات بإجراء اختبارات على استرجاع النسخ الاحتياطية على عينة من البيانات المخزنة في النسخ الاحتياطية بشكل دوريً للتأكد من قابليتها للاسترجاع.

ب. يتم إجراء اختبارات استرجاع النسخ الاحتياطية وفقاً لإجراءات فحص استرجاع النسخ الاحتياطية.

## ٣.١٢ الإجراءات

### ١.٣.١٢ اجراءات النسخ الاحتياطية

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | رؤساء الأقسام في تقنية المعلومات | تحديد الانظمة و المعلومات المراد حفظ النسخ الاحتياطية لها | | | لا يوجد |
| ٢. | رؤساء الأقسام في تقنية المعلومات | تحديث وثيقة استراتيجية النسخ الاحتياطي | | | وثيقة استراتيجية النسخ الاحتياطي |
| ٣. | رؤساء الأقسام في تقنية المعلومات | تطبيق الاعدادات على برنامج النسخ الاحتياطي للقيام بنسخ هذه المعلومات حسب و وثيقة استراتيجية النسخ الاحتياطي | | | لا يوجد |
| ٤. | رؤساء الأقسام في تقنية المعلومات | مراجعة سجلات النسخ الاحتياطي و التأكد من تنفيذها بالشكل الصحيح<br>الر جاء مراجعة النموذج رقم ( IT_F003 ) | | | لا يوجد |
| ٥. | مدير تقنية المعلومات | يقوم مدير تقنية المعلومات بمراجعة هذه السجلات و حفظها لغايات المراجعة | | | سجل النسخ الاحتياطية |

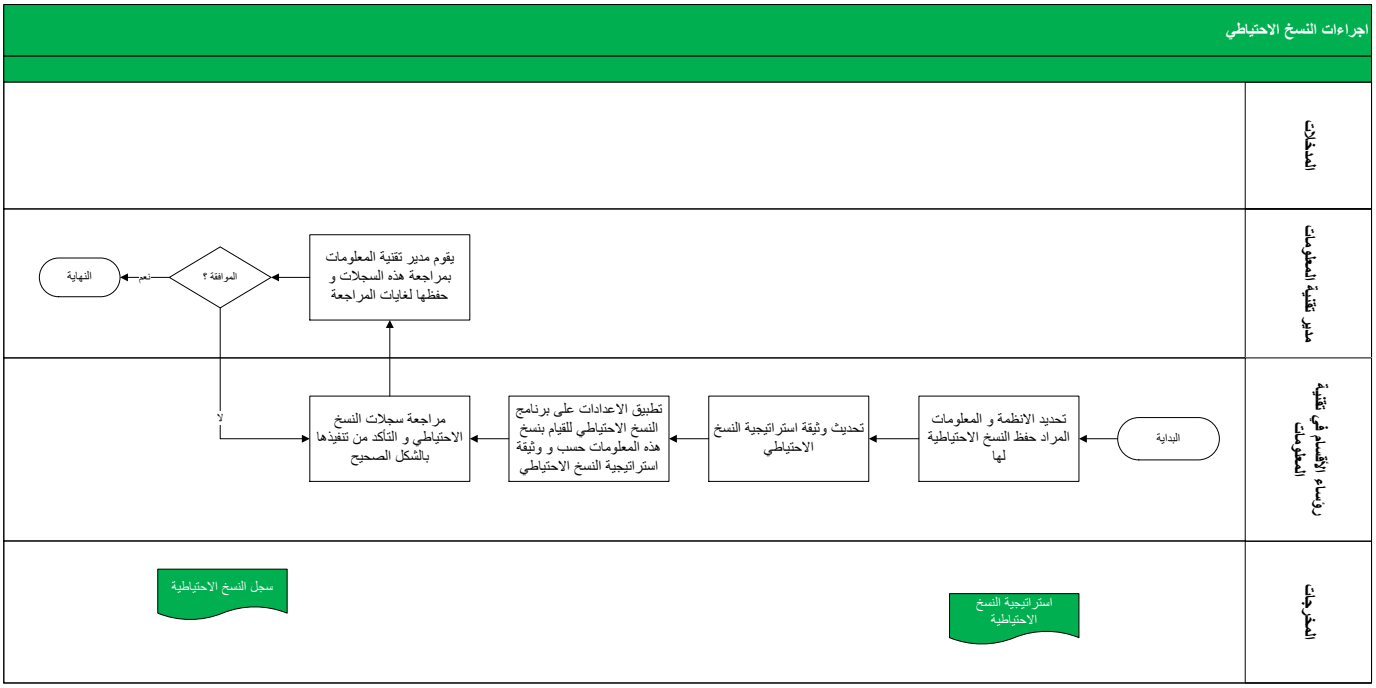
## ٢.٣.١٢ استرجاع النسخ الاحتياطية

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | رؤساء الأقسام في تقنية المعلومات | يرجع رئيس قسم البنية التحتية او رئيس قسم التطبيقات إلى خطط النسخ الاحتياطية لنظم المعلومات ليحدد متطلبات استرجاع وفحص تلك النسخ، ويعين مسئوليات الفحص للأشخاص المعنيين. | | | لا يوجد |
| ٢. | رؤساء الأقسام في تقنية المعلومات | عند تنفيذ عملية فحص استرجاع النسخ الاحتياطية لأنظمة المعلومات (أو مجموعة من أنظمة المعلومات) حسب الخطة، يتم استرجاع بيانات النسخ الاحتياطية على خادم الفحص، ومن ثم يتم توثيق النتائج على سجل متابعة. | | | لا يوجد |
| ٣. | رؤساء الأقسام في تقنية المعلومات | يقوم رئيس قسم البنية التحتية او رئيس قسم التطبيقات بالتحقق من نتائج الفحص ونهاية عملية الاسترجاع الاختبارية، | | | لا يوجد |
| ٤. | رؤساء الأقسام في تقنية المعلومات | يتم حذف البيانات المسترجعة من خادم الفحص بعد اكتمال عملية الاسترجاع بنجاح. | | | لا يوجد |
| ٥. | رؤساء الأقسام في تقنية المعلومات | يتم تحديث جدول فحص استرجاع النسخ الاحتياطية بحيث يظهر تواريخ فحص الاسترجاع التالية. | | | لا يوجد |
| ٦. | مدير تقنية المعلومات | عند اكتمال اجراءات استرجاع النسخ الاحتياطية المجدولة لأنظمة المعلومات، يتم إعداد تقرير استرجاع النسخ الاحتياطية، و من ثم إرسالها إلى مدير إدارة تقنية المعلومات.<br>(الرجاء مراجعة نموذج رقم IT_F002) | | | تقرير استرجاع النسخ الاحتياطية المحدث |
| ٧. | مدير تقنية المعلومات | يقوم مدير إدارة تقنية المعلومات، بمراجعة التقرير واتخاذ الإجراءات | | | لا يوجد |

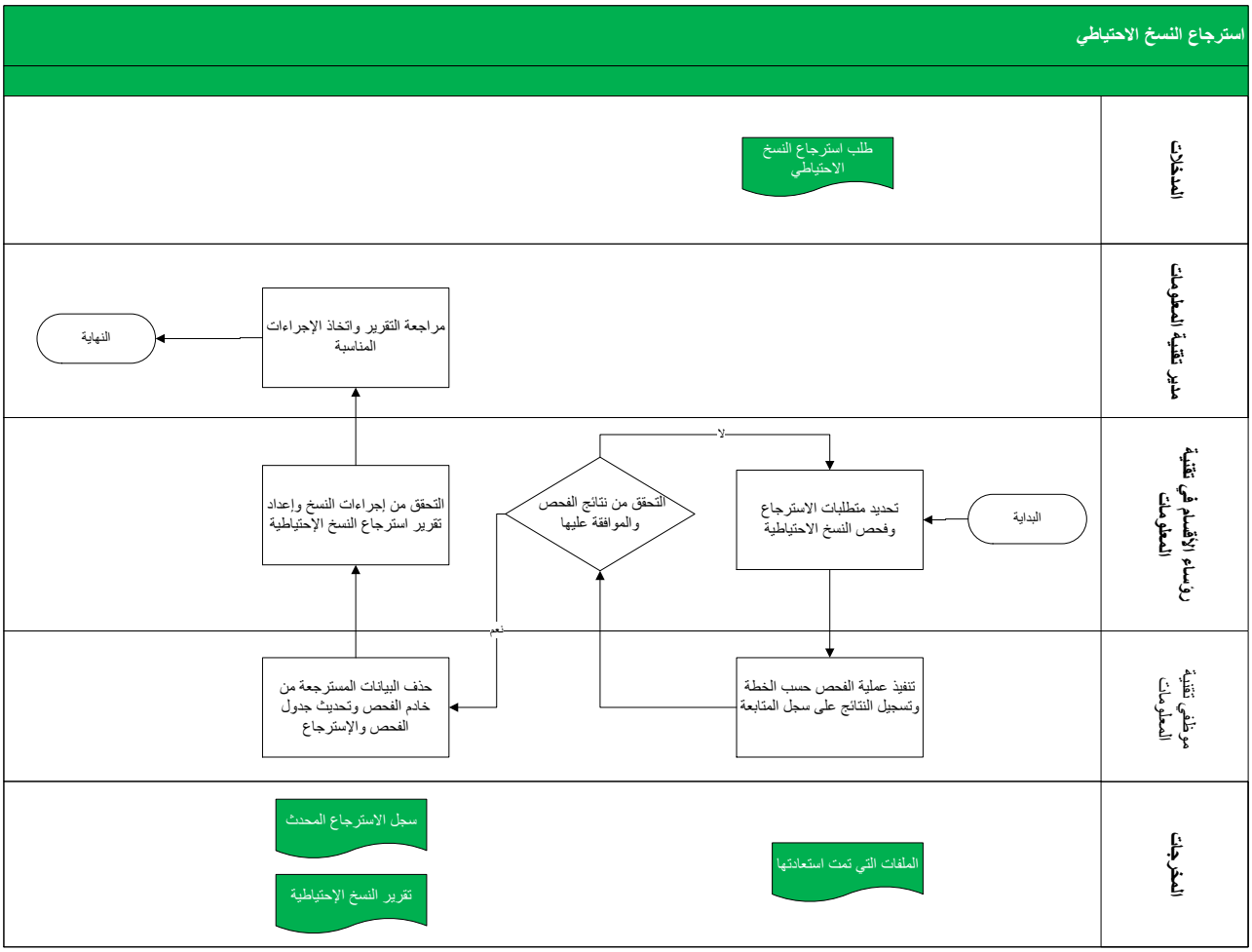
| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| | | المناسبة. | | | |

## ٤.١٢ دورات العمل

### ١.٤.١٢ اجراءات النسخ الاحتياطي



## ٢.٤.١٢ استرجاع النسخ الاحتياطي



# الرقابة والتقييم

## ١٣. سياسة تقييم أداء تقنية المعلومات

### ١.١٣ المقدمة والأهداف

١.١.١٣ الغرض من هذه السياسة هو وضع معايير لقياس أداء تقنية المعلومات ومتابعة هذه المعايير بشكل دوري لضمان التحسين المستمر لأداء هذه الإدارة.

### ٢.١٣ السياسات

١.٢.١٣ يجب تعريف معايير قياس الأداء في بداية كل سنة مالية لدى الجمعية على أن يتم مراجعة هذه المعايير كل ٦ أشهر.

٢.٢.١٣ يجب أن تشمل معايير قياس الاداء النطاقات التالية كحد أدنى على أن يتم إضافة نطاقات جديدة حسب الحاجة وحسب خطط التوسع لدى الجمعية:

أ. معايير قياس خدمات تقنية المعلومات والدعم الفني

- زمن تقديم الخدمة/ البلاغ
- سهولة تقديم الطلب والحصول على الخدمة
- حل مشاكل المستخدمين فور استلامها
- مدى رضى المستخدم عن الخدمة المقدمة له

ب. معايير مراقبة أداء البنية التحتية لتقنية المعلومات ووضع مؤشرات قياس الأداء (KPIs) ، مثل:

- توافريه شبكة وأنظمة المعلومات في الجمعية

- كفاية السعة التخزينية مقارنة بمتطلبات المعلومات في الجمعية
- السرعة في معالجة ونقل المعلومات وتوفيرها بالوقت المناسب
- المرونة في تطوير البنية التحتية وشبكة المعلومات
- مواكبة التطوير والتحديث في عناصر البينة التحتية والأنظمة التابعة لها

ج. معايير تقييم أمن المعلومات في الجمعية

- عدد حوادث أمن المعلومات المؤثرة على توافريه وسرية المعلومات في شبكة الجمعية
- مدى الالتزام بضوابط تقنية المعلومات (مثل عدم مشاركة كلمات السر بين الموظفين ، الابلاغ عن البرامج والفيروسات الضارة في شبكة الجمعية)
- تحديث برامج مكافحة الفيروسات والتأكد من أنها تغطي جميع الأجهزة داخل شبكة الجمعية
- التأكد من وجود مراقبة لصلاحيات المستخدمين بشكل دوري في الجمعية
- التأكد من وجود خطة لاستمرارية الأعمال واختبارها بشكل دوري

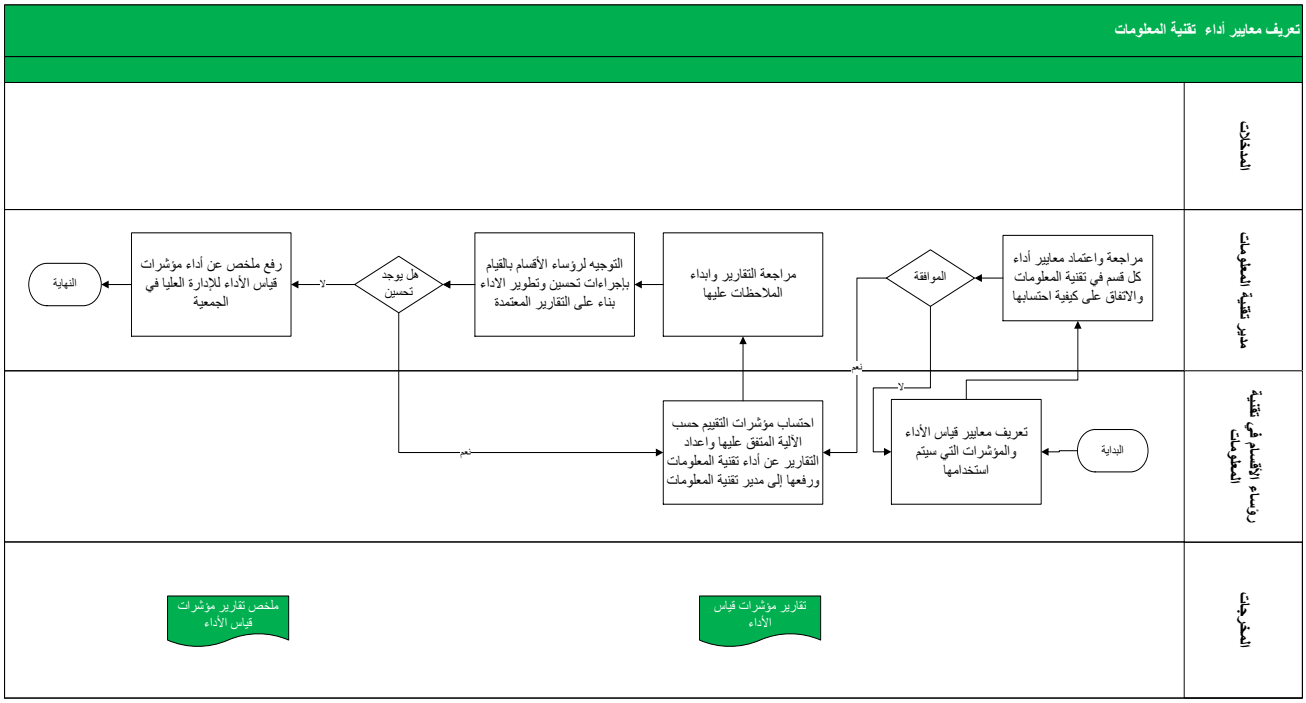
## ٣.١٣ الإجراءات

### ١.٣.١٣ تعريف معايير أداء تقنية المعلومات

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| .١ | رؤساء الأقسام في تقنية المعلومات | تعريف معايير قياس الأداء والمؤشرات التي سيتم استخدامها | | | لا يوجد |
| .٢ | مدير تقنية المعلومات | مراجعة واعتماد معايير أداء كل قسم في تقنية المعلومات والاتفاق على كيفية احتسابها | | | لا يوجد |
| .٣ | رؤساء الأقسام في تقنية المعلومات | احتساب مؤشرات التقييم حسب الآلية المتفق عليها واعداد التقارير عن أداء تقنية المعلومات ورفعها إلى مدير تقنية المعلومات | | | لا يوجد |
| .٤ | مدير تقنية المعلومات | مراجعة التقارير وابداء الملاحظات عليها | | | تقارير مؤشرات قياس الأداء |
| .٥ | مدير تقنية المعلومات | التوجيه لرؤساء الأقسام بالقيام بإجراءات تحسين وتطوير الاداء بناء على التقارير المعتمدة | | | لا يوجد |
| .٦ | مدير تقنية المعلومات | رفع ملخص عن أداء مؤشرات قياس الأداء للإدارة العليا في الجمعية | | | ملخص تقارير مؤشرات الأداء |

## ٤.١٣ دورات العمل

### ١.٤.١٣ تعريف معايير أداء تقنية المعلومات



# أمن المعلومات

## ١٤. سياسة أمن المعلومات

### ١.١٤ المقدمة والأهداف

١.١.١٤ الغرض من هذه السياسة هو التأكد من أن مراقبة حالة أمن المعلومات المتعلقة بأنظمة المعلومات لدى جمعية مراكز الأحياء تتم بشكل دائم من خلال تخطيط ونشر أساليب أمنية ملائمة بما يتوافق مع مخاطر ومدى حساسية وأهمية أنظمة المعلومات.

### ٢.١٤ السياسات

١.٢.١٤ مراقبة أمن المعلومات بناء على المخاطر:

أ. يتم تخطيط وتنفيذ مراقبة أمن المعلومات لأنظمة المعلومات بناءً على حساسية وأهمية وتصنيف المخاطر المتعلقة بأنظمة المعلومات في الجمعية

ب. يجب أن تحدد في وثيقة خطة المراقبة الأمنية المبنية على المخاطر والأشخاص الرئيسيين المعنيين بتنفيذ هذه الأنشطة والعمليات المطلوب تنفيذها والضوابط المتعلقة بالتقنية الواجب مراقبتها.

٢.٢.١٤ إدارة التحديثات وملفات التحديثات الطارئة:

أ. عند عدم وجود ضرر على انظمة المعلومات الحالية تقوم ادارة تقنية المعلومات بالتأكد من أنه تم تحديد وفحص وتطبيق كافة الإصلاحات السريعة أو التحديثات الأمنية لأنظمة المعلومات المحددة.

٣.٢.١٤ تسجيل ومراقبة أحداث النظام

أ. ينبغي على إدارة تقنية المعلومات أن تتأكد من وجود آليات مناسبة في أنظمة معلوماتها والتي تدعم تسجيل الحوادث الأمنية حسب ما تقتضيه خطط المراقبة الأمنية لتلك الأنظمة، ويشمل ذلك دون حصر:

- سجلات محاولات دخول النظام الناجحة والمرفوضة

- سجلات المحاولات الناجحة والمرفوضة للوصول للبيانات والموارد الأخرى
- استخدام الصلاحيات
- سجلات جدار الحماية
- سجلات أخطاء النظام
- النسخ الاحتياطية من البيانات وسجلات الاسترجاع
-

## ٣.١٤ الإجراءات

### ١.٣.١٤ إجراءات المراقبة العامة لأمن المعلومات

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | مدير تقنية المعلومات | يقوم مدير إدارة تقنية المعلومات بتحديد جميع أنظمة المعلومات التي سيتم تطوير خطط مراقبة خاصة بها. | | | خطة مراقبة أمن المعلومات |

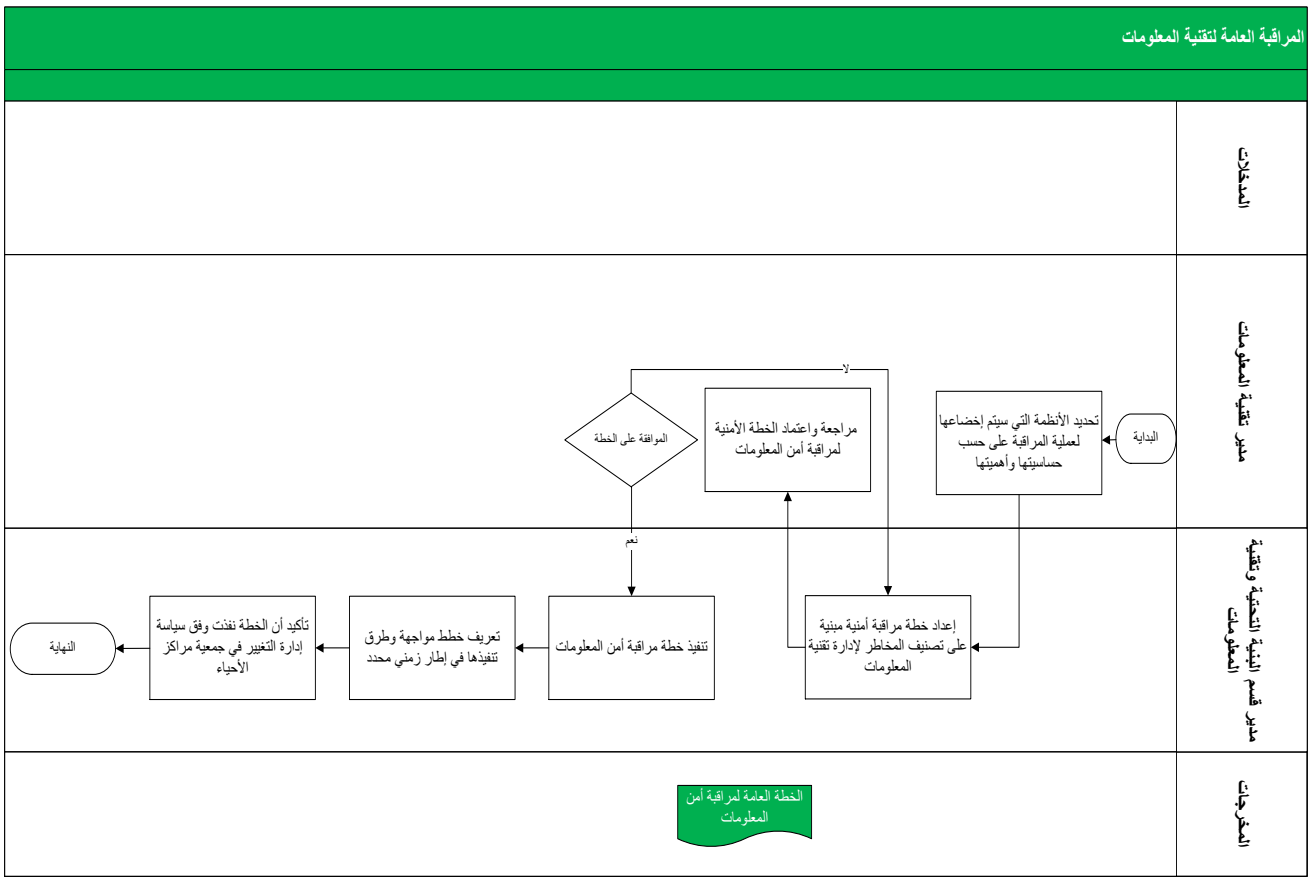
| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ٢. | رؤساء الأقسام في تقنية المعلومات | لكل نظام من أنظمة المعلومات المختارة (أو مجموعة أنظمة المعلومات)، يقوم رئيس قسم البنية التحتية ورئيس قسم التطبيق بإعداد خطة مراقبة أمنية مبنية على تصنيف المخاطر باستخدام نموذج المراقبة والتقييم الأمني المعتمد من إدارة تقنية المعلومات بحيث تشمل الأنشطة التالية :<br>• تحديد ما سيتم مراقبته في الأنظمة المختارة تحديد كيفية المراقبة<br>• تحديد عدد مرات عملية المراقبة | | | لا يوجد |
| ٣. | رؤساء الأقسام في تقنية المعلومات | يرسل رئيس قسم البنية التحتية خطة المراقبة الأمنية إلى مدير إدارة تقنية المعلومات للمراجعة والاعتماد. | | | لا يوجد |
| ٤. | مدير تقنية المعلومات | يقوم مدير إدارة تقنية المعلومات بمراجعة واعتماد خطة مراقبة أمن المعلومات والتوجيه إلى الموظفين المعنيين للعمل بموجبها. | | | خطة مراقبة أمن المعلومات |

## ٢.٣.١٤ تحديثات أمن المعلومات / وملفات التعديل الطارئة

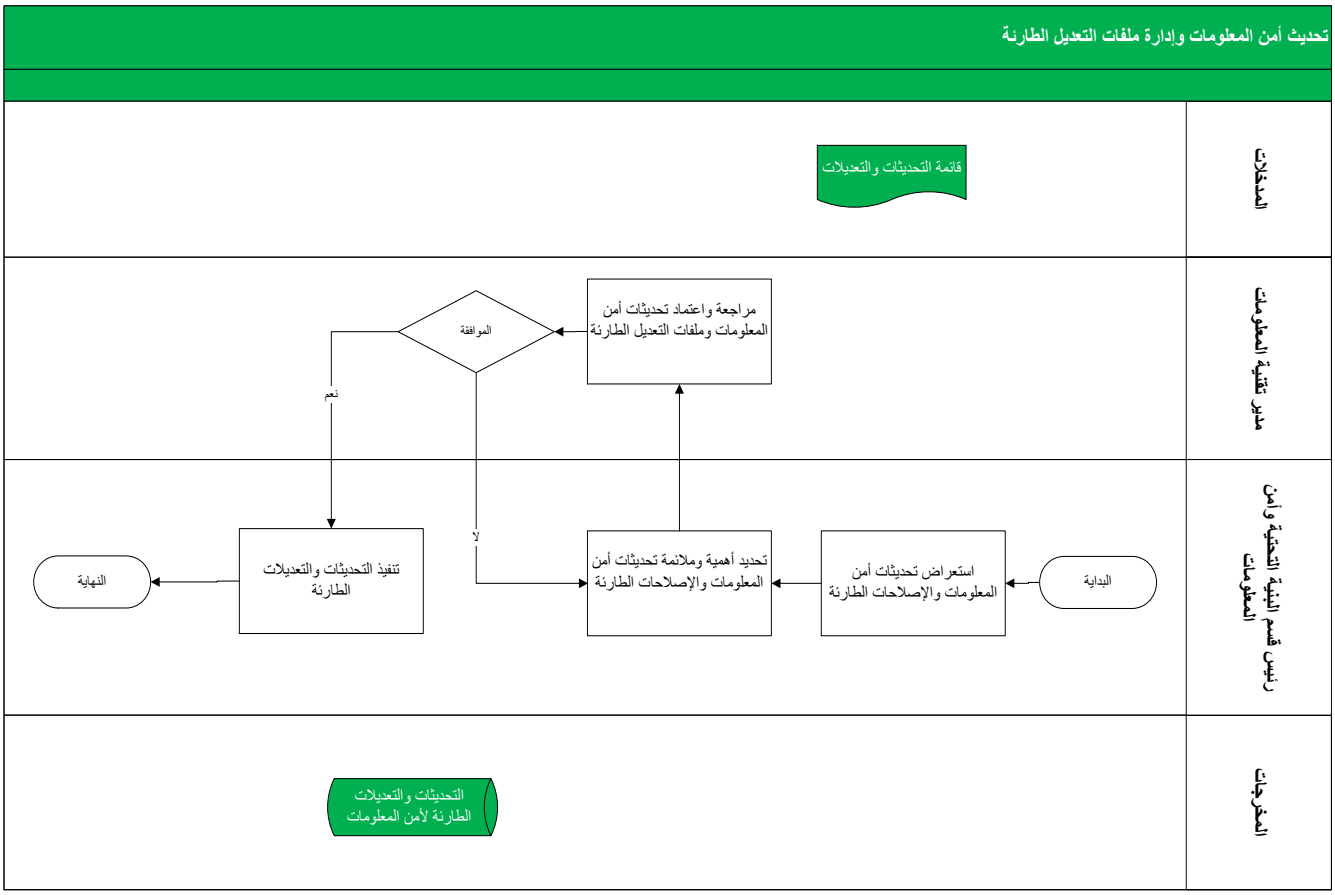
| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | رؤساء الأقسام في تقنية المعلومات | يتم استعراض تحديثات أمن المعلومات / الإصلاحات السريعة (Security Updates/Patches) من قبل الموظفين المعنيين في إدارة تقنية المعلومات (رئيس قسم البنية التحتية أو رئيس قسم التطبيقات أو من ينوب عنهما) لضمان صحتها وعدم وجود ضرر على أنظمة المعلومات الحالية. | | | لا يوجد |
| ٢. | رؤساء الأقسام في تقنية المعلومات | يقوم رئيس قسم البنية التحتية أو رئيس قسم التطبيقات بتحديد مدى أهمية التحديث الأمني / التعديلات الطارئة والتأكد من عدم تعارضها مع متطلبات الانظمة الحالية. | | | لا يوجد |
| ٣. | رؤساء الأقسام في تقنية المعلومات | يقوم رئيس قسم البنية التحتية أو رئيس قسم التطبيقات بإعلام مدير تقنية المعلومات بالتحديثات أو التعديلات الطارئة وينبغي أخذ الموافقة منه لتطبيقها. | | | لا يوجد |
| ٤. | رؤساء الأقسام في تقنية المعلومات | يقوم رئيس قسم البنية التحتية أو رئيس قسم التطبيقات بتنفيذ التحديث الأمني / التعديلات حسب أولويات العمل في الجمعية وحسب إجراءات التغيير. | | | التحديثات والتعديلات الطارئة |

## ٤.١٤ دورات العمل

### ١.٤.١٤ إجراءات المراقبة العامة لأمن المعلومات



## ٢.٤.١٤ تحديثات أمن المعلومات / وملفات التعديل الطارئة



## ١٥. سياسة الأمن المادي والبيئي

### ١.١٥ المقدمة والأهداف

١.١.١٥ الغرض من هذه السياسة هو تحديد القواعد الأساسية لمنع الدخول غير المصرح له والتداخل مع مرافق وأنظمة أمن المعلومات لدى جمعية مراكز الأحياء وكذلك الحماية والحفاظ على أمن المعلومات والموظفين من التعرض إلى التهديدات المادية المختلفة، والتي من شأنها التأثير سلبياً على خدمات أنظمة المعلومات أو توقفها عن العمل.

### ٢.١٥ السياسات

١.٢.١٥ ضوابط الأمن المادي بناء على المخاطر للمنشآت المادية التي تحتوي على أنظمة معلومات:

أ. يجب أن تتأكد جمعية مراكز الأحياء من أن جميع منشآتها المادية التي تحتوي على أنظمة معلومات تتمتع بعوامل الأمان بما يتوافق مع مخاطر أنظمة المعلومات في تلك المنشآت.

ب. يتم تحديد جميع هذه المنشآت المادية لدى الجمعية وتعين تصنيف أمني لها.

ج. يتم تخطيط الأمن المادي والبيئي لهذه المنشآت مع الأخذ بعين الاعتبار درجة تصنيف أمن المعلومات والمعايير المتعلقة بالنوع المحدد من البنية التحتية المادية لدى جمعية مراكز الأحياء.

د. تعنى الموارد البشرية(الشئون الإدارية) وإدارة تقنية المعلومات بمسئولية التنسيق فيما بينهما للتأكد من تصميم وتنفيذ ومراقبة الضوابط المحددة لهذه المنشآت القائمة على المخاطر.

٢.٢.١٥ التحكم بالدخول المادي:

أ. يسمح لموظفي وموردي ومقاولي جمعية مراكز الأحياء بالدخول إلى مرافق معالجة المعلومات، و ذلك فقط بناءً على التعريف بأنفسهم والتحقق من هويتهم وفقاً لإجراءات الموافقة على طلب الدخول للجهة او بموافقة مدير تقنية المعلومات .

ب. يمنع منعاً باتاً مشاركة الموظفين بعضهم باستخدام بطاقة الدخول إلى مرافق أنظمة المعلومات.

ج. يجب مرافقة جميع الزوار أثناء تجوالهم في المناطق الآمنة من قبل موظفي تقنية المعلومات في جمعية مراكز الأحياء.

٣.٢.١٥ صيانة البنية التحتية للأمن المادي والبيئي:

أ. ينبغي أن تتم صيانة وإصلاح معدات تقنية المعلومات من قبل موظفين مصرح لهم من قبل إدارة تقنية المعلومات.

ب. ينبغي أن تتأكد إدارة تقنية المعلومات من أنه يتم فحص وصيانة أجهزة ومعدات البنية التحتية للأمن المادي والبيئي المتعلقة بأنظمة المعلومات حسب جدول الصيانة الوقائية المعتمد من قبل إدارة تقنية المعلومات لهذه المعدات.

د. يتعين على إدارة تقنية المعلومات التصريح والتحكم ومراقبة أية أنشطة صيانة وأنشطة تشخيصية يتم تنفيذها محلياً أو عن بعد.

٤.٢.١٥ الحماية من الحريق بمنشآت نظم المعلومات:

أ. تشترك إدارتا تقنية المعلومات والموارد البشرية(الشئون الإدارية) بمسئولية الاستجابة لحوادث الحريق الطارئة وإجراء تمارين للتعامل مع الحريق.

ب. ينبغي إجراء تمارين التعامل مع الحريق بشكل سنوي. كما ينبغي مراقبة تلك التمارين، وتزويد جميع المشاركين بإفادات تتعلق بمساهمتهم وأدائهم.

ج. تقوم إدارتا تقنية المعلومات والموارد البشرية(الشئون الإدارية) بتحديد المواقع الحرجة الخاصة بتقنية المعلومات التي سيتم تجهيزها بطفايات حريق يدوية. وعليه فإنه يتعين وضع بطاقات واضحة على تلك المناطق.

٧.٢.١١ مراقبة الأمن المادي والبيئي:

أ. يجب أن تتأكد إدارة تقنية المعلومات بالتنسيق مع إدارة الموارد البشرية من مراقبة ضوابط الأمن المادي والبيئي لمنشآت أنظمة المعلومات بما يتوافق مع مستويات تصنيف المخاطر.

### ٣.١٥ الإجراءات

١.٣.١٥ لا تحتاج هذه السياسة لإجراءات تشغيلية بموجب هذا الإطار. وقد تم تحديد الخطوات العملية المطلوب اتباعها ضمن السياسة.

## ١٦. سياسة إدارة المعلومات الشخصية والإفصاح

### ١.١٦ المقدمة والأهداف

الغرض من هذه السياسة هو الحفاظ على سرية وسلامة وصحة المعلومات التي تتعامل معها جمعية مراكز الأحياء.

### ٢.١٦ السياسات

١.٢.١٦ أمن المعلومات الشخصية المخزنة في انظمة معلومات الجمعية (هذه السياسة تنطبق على المعلومات المخزنة في انظمة معلومات الجمعية و لدى ادارة تقنية المعلومات):

أ. تلتزم ادارة تقنية المعلومات بحماية المعلومات الشخصية المرتبطة بمنسوبي جمعية مراكز الأحياء و التي يتم تخزينها في انظمة معلومات الجمعية.

ب. تحتفظ جمعية مراكز الأحياء بحقها بالكشف عن المعلومات الشخصية السرية حسبما يقتضي النظام ولمساعدة السلطات في تحديد الأنشطة التي تنطوي على غش وخداع.

ج. على جمعية مراكز الأحياء حصر الوصول إلى المعلومات (الالكترونية) الشخصية السرية عن موظفيها على "أساس الحاجة إلى المعرفة (need to know basis)". ويتم إلزام هؤلاء الأشخاص بالتزامات سياسة عدم الإفصاح، ويتعرضون لإجراءات نظامية في حالة المخالفة قد تصل إلى فصلهم من العمل والملاحقة القضائية.

د. يجب التأكد من عدم جمع أية معلومات شخصية عن أي فرد دون موافقة المسبقة.

٢.٢.١٦ سياسة نشر المعلومات المخزنة في انظمة معلومات الجمعية (هذه السياسة تنطبق على المعلومات المخزنة لدى انظمة معلومات الجمعية و لدى ادارة تقنية المعلومات) :

٣.٢.١٦ :

أ. ينبغي على جمعية مراكز الأحياء عدم نشر أية معلومات شخصية بأية صيغة أو شكل دون التفويض الواضح المسبق من المسؤول عن تلك المعلومات الشخصية. ويجب الحصول على التفويض بالإفصاح عن المعلومات من قبل المسئولين عنها قبل وضعها في النطاق العام.

ه. يطلب من مدير الادارة المعنية او من ينوب عنه بمراجعة المعلومات الشخصية المزمع نشرها وذلك قبل نشرها لوصول الجمهور إليها بشكل عام، وذلك من أجل

تقييم المسئوليات والتبعات الممكنة جراء ذلك. وتقوم الإدارة القانونية بتقييم تلك المعلومات وتشير إلى مخاطر المسئولية التي قد تؤثر بصورة مباشرة أو غير مباشرة على جمعية مراكز الأحياء.

و. على جمعية مراكز الأحياء حماية عملائها ومعلوماتهم السرية في جميع الأوقات من إساءة الاستخدام، وأن تتأكد من عدم بيع تلك المعلومات أو إعطاؤها لأي أطراف ثالثة دون الموافق الصريحة المسبقة والواضحة من المسؤول عن معلومات التعريف الشخصية للعملاء.

## ٣.١٦ الإجراءات

١.٣.١٦ لا تحتاج هذه السياسة لإجراءات تشغيلية بموجب هذا الإطار. وقد تم تحديد الخطوات العملية المطلوب اتباعها ضمن السياسة.

## ١٧. سياسة أمن الوسائط الإلكترونية

### ١.١٧ المقدمة والأهداف

١.١.١٧ الهدف من هذه السياسة حماية الوسائط الإلكترونية لدى جمعية مراكز الأحياء مثل (أجهزة الذاكرة الموصولة على منافذ USB، الأقراص الصلبة المتنقلة، وسائط بيانات المدخلات/المخرجات مثل دي في دي، والأقراص المدمجة، خدمات التخزين على السحب الإلكترونية وغيرهما) من الاستخدام والسرقة والوصول إليها بشكل غير مصرح به.

### ٢.١٧ السياسات

١.٢.١٧ تخزين الوسائط الإلكترونية:

أ. يتم خزن الوسائط الإلكترونية في بيئة آمنة تتوفر فيها شروط السلامة.

ب. يجب استخدام بطاقات الباركود لتعريف الوسائط في الـ "Tape Library".

٢.٢.١٧ أمن الوسائط الإلكترونية أثناء نقلها:

ج. على جمعية مراكز الأحياء أن تتأكد من حماية أنظمة معلومات العمل أثناء نقل الوسائط.

د. منع تخزين معلومات الجمعية على وسائط تخزين خدمات السحب الإلكترونية المجانية مثل (Google Drive, DropBox, SugarSync, Skydrive, etc.).

٣.٢.١٧ الوسائط القابلة لإعادة الاستخدام:

أ. يجب أن يتم المسح التام للمحتويات المحفوظة على الوسائط الإلكترونية القابلة لإعادة الاستخدام والتأكد من عدم إمكانية استرجاع تلك المحتويات.

ب. يجب فحص جميع الأجهزة المحتوية على وسائط خزن بيانات (الأقراص الصلبة الثابتة) للتأكد من إزالة أي أنظمة معلومات تتعلق بالعمل، وكذلك إزالة البرامج

المرخصة عنها، وأنه يتم الكتابة فوقها بأمان أو إتلافها قبل التخلص منها أو إعادة استخدامها.

٤.٢.١٧ الوسائط القابلة للإزالة:

ج. يجب إعادة تهيئة الوسائط التي لم تعد مستخدمة والقابلة للإزالة وإعادة الكتابة وذلك للحيلولة دون الكشف بشكل خاطئ عن المعلومات التي تحتويها أثناء تبادلها بين الموظفين أو الأطراف الأخرى.

٥.٢.١٧ التخلص من الوسائط:

أ. يجب إتلاف الوسائط المادية التي تحتوي على معلومات بشكل آمن عندما لا تعود هناك حاجة لها وذلك وفقاً لإجراءات التخلص من الوسائط الإلكترونية.

ب. يتم الاحتفاظ بسجل عمليات إتلاف/ تدمير أجهزة الوسائط وتوثيق الأشخاص المسئولين عن الإتلاف.

٦.٢.١٧ الهواتف والأجهزة الذكية:

أ. تقوم إدارة تقنية المعلومات بالتوعية بالسياسات الإرشادية التالية لمستخدمي الهواتف والأجهزة الذكية المملوكة للجمعية لأغراض العمل:

- إقفال الجهاز بطريقة تلقائية وتحديد كلمة مرور خاصة بالمستخدم
- تستخدم الاجهزة لأعمال الجمعية فقط
- يجب تفعيل مسح الذكرة و كرت التخزين (SD) في حال السرقة أو فقدان الجهاز

- يجب تشفير المعلومات المخزنة في ذاكرة الجهاز و كرت التخزين (SD)
- تبادل المعلومات مع شبكة الجمعية يتم عبر قنوات آمنة ومشفرة

ب. أما في حال كانت الاجهزة الذكية غير مملوكة للجمعية فيجب على موظفي الجمعية اتباع الارشادات التالية:

- إقفال الجهاز بطريقة تلقائية وتحديد كلمة مرور خاصة بالمستخدم
- فصل المعلومات الشخصية عن معلومات العمل من خلال استخدام دليل منفصل لملفات العمل و وتوخي اقصى دراجات الحذر عند استخدام برامج التواصل الاجتماعي على هذه الاجهزة و خاصة عند مشاركة بعض الملفات مع اطراف اخرى
- يفضل تشفير المعلومات المخزنة في ذاكرة الجهاز و كرت التخزين (SD)
- يفضل أن يتم تفعيل مسح الذكرة و كرت التخزين (SD) في حال السرقة أو فقدان الجهاز

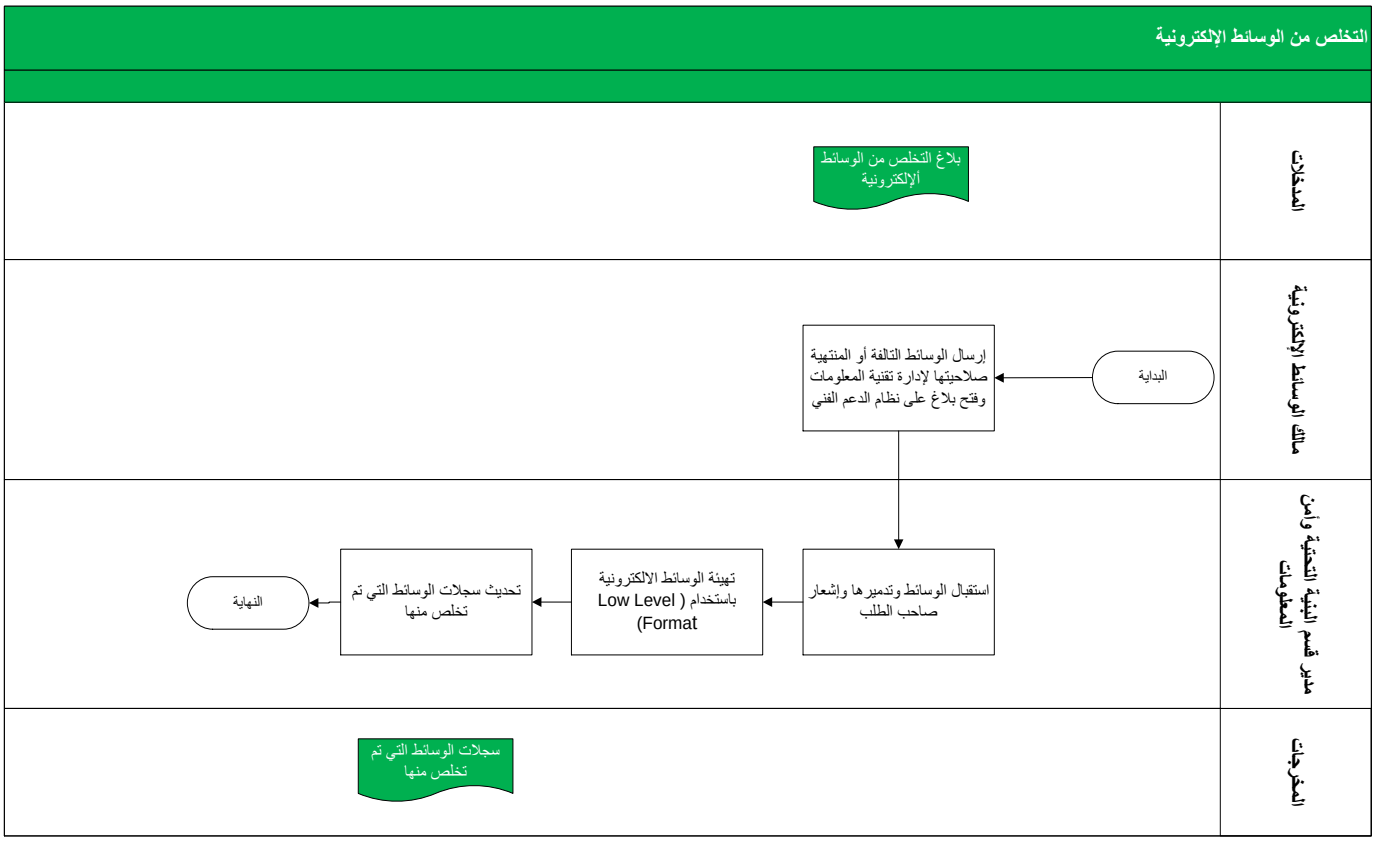
## ٣.١٧ الإجراءات

### ١.٣.١٧ التخلص من الوسائط الإلكترونية

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | رئيس قسم البنية التحتية | يقوم رئيس قسم البنية التحتية بعملية تدمير للوسط الإلكتروني. | | | لا يوجد |
| ٢. | رئيس قسم البنية التحتية | الوسط الذي يحتوي على معلومات الجمعية والذي يمكن تهيئته، فيجب تهيئته باستخدام "Low Level Format". | | | لا يوجد |
| ٣. | رئيس قسم البنية التحتية | يجب الاحتفاظ بسجل للوسائط المادية المهمة التي تم التخلص منها.<br>الر جاء مراجعة النموذج<br>رقم ( IT_F008) | | | السجل المحدث للوسائط التي تم التخلص منها |

## ٤.١٧ دورات العمل

### ١.٤.١٧ التخلص من الوسائط الإلكترونية



## ١٨. سياسة الحماية من الفيروسات والبرامج الضارة

### ١.١٨ المقدمة والأهداف

١.١.١٨ الغرض من هذه السياسة هو حماية أنظمة المعلومات لدى جمعية مراكز الأحياء من البرامج الضارة (مثل الفيروسات، ديدان الحاسب الآلي (computer worm) ، أحصنة طروادة(Trojan Horse) ،برامج التجسس على البريد الإلكتروني، إلخ).

### ٢.١٨ السياسات

١.٢.١٨ استخدام حلول مكافحة الفيروسات المتعارف عليها دولياً:

أ. يجب أن يكون لدى جمعية مراكز الأحياء آلية محددة وواضحة للكشف عن الفيروسات والبرامج الضارة ومنعها وعلاج واستعادة الأنظمة المصابة بطريقة مناسبة.

ب. يجب أن يكون لدى جمعية مراكز الأحياء برنامج مكافحة فيروسات متعارف عليه دولياً ومدار لديها بصورة مركزية ومثبت ومفعّل في جميع الأوقات على كافة أنظمتها المعلوماتية.

٢.٢.١٨ اكتشاف ومنع الفيروسات / البرامج الضارة من التأثير على أنظمة المعلومات لدى جمعية مراكز الأحياء.

أ. يجب أن يتم فحص كافة الأجهزة المملوكة وغير المملوكة من قبل جمعية مراكز الأحياء للتأكد من خلوها من الفيروسات/ البرامج الضارة قبل وصلها مع شبكة جمعية مراكز الأحياء.

ب. يجب تطبيق تقنية مكافحة الفيروسات في النقاط التي يمكن للفيروس/ أو الملفات الغير موثوق بها أن تدخل منها إلى شبكة جمعية مراكز الأحياء.

ج. يجب نشر تعريفات وتحديثات برامج مكافحة الفيروسات عبر وسائل آلية بشكل دوري أو بمجرد اصدارها.

د. يجب إعداد أنظمة المعلومات بحيث تمنع المستخدمين من تعطيل عمل أدوات مكافحة الفيروسات.

ه. يجب أن تشتمل برامج الحماية من الفيروسات/ البرامج الضارة على آلية التثبيت/ التركيب لبرامج مكافحة الفيروسات في أي أنظمة معلومات (أجهزة الحاسب الآلي ، الخادم، إلخ).

ج. يتم تطبيق التدابير الفنية التالية:

- يجب أن يتم– إعداد– برنامج مكافحة الفيروسات للتأكد بأن تطبيق مكافحة الفيروسات (agent) يعمل في جميع الأوقات على أجهزة المستخدمين (أجهزة سطح المكتب، أجهزة الحاسب الآلي المحمول ، إلخ) وذلك من خلال كشف حالة التطبيق في جميع الأوقات.
- يتم ضبط إعدادات برنامج مكافحة الفيروسات لفحص كافة أقراص الوسائط القابلة للإزالة وذاكرات الفلاش الموصولة مع أنظمة المعلومات.
- يتم فحص ملفات ومرفقات البريد الإلكتروني للتأكد من عدم احتواءها على الفيروسات/ البرامج الضارة قبل فتحها أو الدخول إليها.
- يتم ضبط إعدادات برنامج الحماية من الفيروسات/ الشفرات الخبيثة بحيث يقوم بإجراء فحص آلي بشكل دوري لجميع أجهزة الحاسوب، والخوادم على فترات منتظمة، للكشف عن احتمالات وجود أي فيروسات/ شفرات خبيثة.

- يتم ضبط إعدادات سجل الدخول إلى برنامج مكافحة الفيروسات بحيث يتم رصد أقصى حد ممكن من التفاصيل. ويجب عدم السماح بالحذف النهائي لتلك السجلات الا بموافقة مدير تقنية المعلومات.
- يكون رئيس قسم البنية التحتية مسئولاً عن بقاء البنية التحتية للكشف عن الفيروسات/ الشفرات الخبيثة فاعلة.

٣.٢.١٨ مسئوليات المستخدم

أ. يتعين على المستخدم توخي الحذر عند تحميل (إنزال) الملفات من الإنترنت.

ب. يجب أن لا يفتح المستخدم أو يحمل أو ينفذ أي ملفات يستقبلها أو مرفقات بريد إلكتروني يتلقاها من مصدر غير معروف أو مشبوه أو غير موثوق به.

ج. يجب أن لا يقوم المستخدم بمحاولة تغيير الإعدادات، أو حذف، أو إبطال، أو العبث بأي برنامج مخصص لمكافحة أو الكشف عن الفيروسات/ الشفرات الخبيثة يكون قد تم تركيبه على أي نظام معلومات مستخدم من قبلهم.

د. ينبغي على المستخدمين تبليغ إدارة تقنية المعلومات فوراً عن جميع حوادث الفيروسات/ الشفرات الخبيثة (المكتشفة من خلال برنامج مكافحة الفيروسات/ الشفرات الخبيثة المركبة في أجهزتهم) وعن أي سلوك غير اعتيادي / غير طبيعي للنظام (مثل بطء الاستجابة أو تأخر زمن الاستجابة أو غير ذلك).

ه. على المستخدمين أن يتأكدوا من أن الوسائط الإلكترونية المتبادلة مع الإدارات أو المؤسسات الأخرى قد تم فحصها تحسباً لوجود فيروسات / برامج خبيثة وذلك قبل استخدامها في الأنظمة التي لديهم.

٤.٢.١٨ إزالة الفيروسات/ البرامج الضارة من أنظمة معلومات جمعية مراكز الأحياء:

أ. يجب القيام بعزل/إزالة أي فيروسات/ شفرات خبيثة مكتشفة أنظمة معلومات جمعية مراكز الأحياء. ويجب عدم السماح بوصل أنظمة المعلومات التي لم يتم إزالة / تعطيل الفيروسات/ الشفرات الخبيثة المكتشفة فيها مع شبكة جمعية مراكز الأحياء.

و. يتم إعداد برنامج الفيروسات بحيث يكتشف ويعزل آلياً جميع الفيروسات/ الشفرات الخبيثة المكتشفة في أنظمة المعلومات.

ز. يتم التعامل مع جميع هجمات الفيروسات/ الشفرات طبقاً لإجراءات إزالة الفيروسات/ الشفرات الخبيثة من أنظمة المعلومات لدى جمعية مراكز الأحياء.

## ٣.١٨ الإجراءات

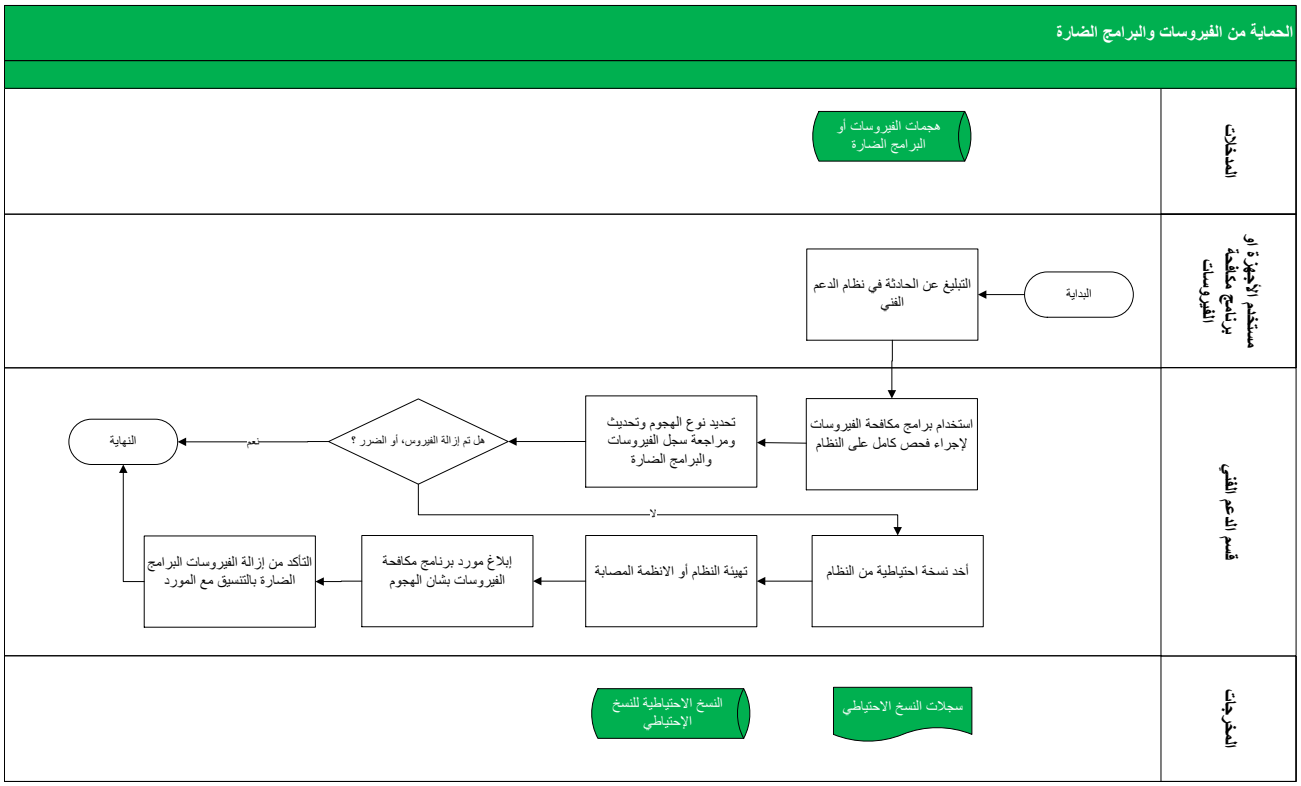
### ١.٣.١٨ اجراءات الحماية من الفيروسات والبرامج الضارة

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | مستخدم الجهاز/ النظام | عندما يشك المستخدم بوجود هجمات بالفيروسات / الشفرات الخبيثة على نظام المعلومات الذي يستخدمه، أو يشير برنامج مكافحة الفيروسات المركب على الأجهزة بوجود ذلك، فإن عليه التبليغ فوراً عن الحادثة إلى فريق الدعم الفني (قسم الشبكات). | | | لا يوجد |
| ٢. | قسم الدعم الفني | يستخدم فريق الدعم الفني (قسم الشبكات) برنامج مكافحة الفيروسات/ برنامج مكافحة الشفرات الخبيثة | | | لا يوجد |

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| | | لإجراء فحص كامل للنظام بما في ذلك قطاع بيانات التشغيل وكافة الملفات المضغوطة، ومكتبات النظام، والأقراص لإزالة / عزل كافة البرامج الخبيثة التي يمكن التعرف عليها. | | | |
| ٣. | قسم الدعم الفني | يراجع فريق الدعم الفني (قسم الشبكات) سجل برنامج مكافحة الفيروسات / أو البرامج الضارة لتحديد طبيعة الهجوم والاحتفاظ بالسجل حتى يمكن الرجوع إليه و استخدامه في التقارير مستقبلا. | | | |
| ٤. | قسم الدعم الفني | إذا تعذر عزل أو إزالة الفيروسات / الشفرات الخبيثة بواسطة برنامج مكافحة الفيروسات، يقوم رئيس البنية التحتية وأمن المعلومات بالتالي إن استدعت الحاجة:<br><br>أ. أخذ نسخة احتياطية من نظام المعلومات.<br><br>ب. تهيئة نظام/ أنظمة أمن المعلومات المصابة.<br><br>ج. إبلاغ مورد برنامج مكافحة الفيروسات بشأن الهجوم، وطلب المزيد من المساعدة.<br><br>د. التأكد من إزالة الفيروس / الشفرة الخبيثة من النسخة الاحتياطية للنظام بمساعدة من مورد برنامج مكافحة الفيروسات . | | | لا يوجد |

## ١.١٨ دورات العمل

### ١.١.١٨ اجراءات الحماية من الفيروسات والبرامج الضارة



## ١٩. سياسة الوصول المنطقي

### ١.١٩ المقدمة والأهداف

١.١.١٩ الغرض من هذه السياسة هو التحكم بالوصول المنطقي إلى أنظمة المعلومات لدى جمعية مراكز الأحياء مما يكفل دقة وسرية وتوفر المعلومات.

### ٢.١٩ السياسات

١.٢.١٩ التحكم بالوصول

أ. يجب أن يسمح للمستخدمين لدى جمعية مراكز الأحياء بالوصول إلى أنظمة المعلومات والعمليات اللازمة لتأدية مهام أعمالهم فقط وفي حالة الاستثناء يجب اخذ موافقة الادارة المعنية.

ب. يجب استخدام (إجراءات إنشاء مجموعات المستخدمين أو مجموعات الصلاحيات) لضبط إعدادات الوصول لأنظمة المعلومات عند تطبيق و إعداد الأنظمة و ذلك باستخدام خاصية مجموعات المستخدمين أو مجموعات الصلاحيات والتي تحدد صلاحيات الوصول لكل مجموعة، ويتم منحهم إمكانية الوصول من خلال عضويتهم في مجموعات المستخدمين أو مجموعات الصلاحيات المحددة مسبقاً.

ج. يجب التحكم بالوصول إلى شبكة أنظمة المعلومات (Network Domain) لدى جمعية مراكز الأحياء باستخدام إجراءات تسجيل دخول المستخدمين فقط.

د. على كل مستخدم من مستخدمي شبكة أنظمة المعلومات الحصول على تفويض رئيس قسم البنية التحتية كي يتسنى له الدخول إلى شبكة أنظمة معلومات لجمعية مراكز الأحياء.

ه. يسمح بالدخول إلى أنظمة المعلومات وتفعيل حسابات المستخدمين لكل من الموظفين، المقاولين، الاستشاريين، العاملين المؤقتين، أو موظفي الموردين في حالة قيام الشخص بتأدية الخدمات لمصلحة جمعية مراكز الأحياء فقط.

٢.٢.١٩ اسم المستخدم وكلمة المرور

أ. يجب أن يتم تخزين والتعامل مع وتوزيع كافة أسماء المستخدمين وكلمات المرور إلى الأنظمة بشكل آمن.

ب. يجب أن يكون لكل مستخدم من مستخدمي أي نظام معلوماتي اسم مستخدم فريد وكلمة مرور خاصة به.

ج. يجب عدم استخدام أسماء المستخدمين العامة مثل حساب (Admin).

د. لا يسمح للمستخدم بمشاركة اسم المستخدم وكلمة المرور الخاصين به مع أشخاص آخرين تحت أي ظرف من الظروف. وعلى المستخدم أن يتحمل المسؤولية المباشرة كاملة عن كافة الأنشطة التي تتم من خلال حساب المستخدم الخاص به على أي من الأنظمة المسموح له استخدامها.

ه. يجب عدم إعادة إصدار نفس اسم المستخدم لمستخدمين آخرين.

و. يجب أن تكون معايير تحديد اسم المستخدم متوافقة مع معايير التسمية المعيارية لدى جمعية مراكز الأحياء بما يضمن أن اسم المستخدم لا يعطي أي انطباع حول مستوى المستخدم أو امتيازاته أو حقوق الدخول التي يتمتع بها، مثل (Verifier) أو (Releaser).

ز. ينبغي على جميع المستخدمين بمن فيهم مدراء الأنظمة الالتزام بالأحكام والشروط المتعلقة باستخدام وإدارة كلمات المرور الخاصة بهم، ويجب تطبيق المعايير التالية من قبل كل نظام

- أدنى طول مسموح به لكلمة المرور يتكون من (٦-١٠ خانات).
- الاحتفاظ بتاريخ كلمة المرور ( يمنع استخدام آخر ثلاث كلمات مرور مسبقة).
- انتهاء صلاحية كلمة المرور للشبكة (مع أول تسجيل دخول باستخدام كلمة المرور، وبعد ذلك بحد أقصى لمدة ٩٠ يوماً منذ آخر تغيير لكلمة المرور).
- يتم الاستخدام لمرة واحدة فقط لكلمة المرور الأولية التي تم انشاءها عند انشاء اسم المستخدم، وبعد ذلك يقوم نظام المعلومات بإجبار المستخدم على تغيير كلمة المرور في أول تسجيل دخول.
- يتم تطبيق تشفير كلمة المرور.
- لا يتم عرض كلمة المرور في الحقل المخصص لإدخال كلمة المرور.
- عند استحداث حساب لمستخدم، يجب إصدار كلمة مرور مؤقتة لاستخدامها في تسجيل الدخول لأول مرة فقط، ويجوز إبلاغ المستخدم بها شفوياً.

ح. يجب تحديد ميزات حجب وانتهاء صلاحية كلمة المرور بناءً على متطلبات النظام، وتصنيفه، وأهميته (كونه من الأنظمة الحرجة) ، والآثار الجانبية في حال الانتهاك.

٣.٢.١٩ تغيير وصول المستخدم

أ. يجب إبلاغ إدارة تقنية المعلومات من قبل الادارة المعنية أو ادارة الموارد البشرية عن إنهاء أو انتهاء عقود الموظفين أو عندما لم يعد لمستخدم معين حاجة عملية للوصول إلى نظام المعلومات لكي يتم الإلغاء الفوري لجميع حسابات المستخدمين أو تغيير وظائفهم و/أو صلاحياتهم.

ب. في حالة انتهاء أو إنهاء عقد الموظف أو انتقاله، يجب على إدارة الموارد البشرية أن تقوم فوراً بإشعار إدارة تقنية المعلومات رسميا وتزويدهم بتفاصيل قرار تغيير الوظيفة أو الانتقال وتاريخ النفاذ.

- في حالة إنهاء أو انتهاء عقد الموظف، يتصرف رئيس قسم البنية التحتية و رئيس قسم التطبيقات لإيقاف وصول ذلك الموظف إلى أنظمة المعلومات إلا إذا أجاب مدير الإدارة بالموافقة على طلب التمديد المؤقت لوصول الموظف المعني إلى الأنظمة وحدد تاريخاً لاحقاً لإيقاف ذلك الوصول.
- في حال انتقال الموظف، ينسق مدير الادارة المعنية مع رئيس قسم البنية التحتية و رئيس قسم التطبيقات لإزالة جميع إمكانيات الوصول الحالية للموظف، ومن ثم يحدد الوصول الجديد وفقاً لأحدث نموذج صلاحيات وصول معتمد للمستخدم.

٣.٢.١٦ مراجعة صلاحيات وصول المستخدم

أ. تقوم إدارة تقنية المعلومات مع الإدارة المعنية بإجراء مراجعة دورية تتعلق بالمخاطر المترتبة عن حقوق وصول المستخدمين للأنظمة.

ب. يطلب رئيس قسم البنية التحتية أو رئيس قسم التطبيقات من مدراء الإدارات المعنية التأكد من أن جميع حقوق وصول المستخدمين قد تمت مراجعتها من قبلهم وفقاً لإجراءات مراجعة حقوق وصول المستخدمين للتأكد من:

- مطابقتها لأوصاف وظائف المستخدمين.
- الاستمرار في الحفاظ على متطلبات الفصل بين المهام.
- الاستمرار في إتباع مبدأ "الحاجة إلى المعرفة"(need-to-know basis)

ج. ينبغي على رئيس قسم البنية التحتية أو رئيس قسم التطبيقات إجراء مراجعة دورية لاكتشاف الحسابات غير المستخدمة، حيث يتعين تعطيل تلك الحسابات أو إزالتها من النظام.

د. عند اكتشاف أي سوء استخدام لحقوق الوصول المميزة، فإن على رئيس قسم البنية التحتية و رئيس قسم التطبيقات تقييد تلك الامتيازات وإشعار الادارة المعنية لاتخاذ الإجراء اللازم حيال ذلك.

٤.٢.١٩ سياسة المكتب النظيف والشاشة النظيفة

أ. تقوم إدارة تقنية المعلومات مع ادارة الموارد البشرية بتوعية المستخدمين بالتالي:

- عدم ترك أجهزة الحاسوب المحمولة وأجهزة سطح المكتب ووحدات الحاسوب الطرفية والطابعات مفتوحة في حالة عدم التواجد بجوارها، وإنما يجب تحصينها بشاشات محمية بكلمات مرور.
- حماية أجهزة تصوير المستندات وأجهزة الفاكس بكلمات مرور.

- رفع المعلومات المصنفة كمعلومات حساسة عند طباعتها فوراً من الطابعات.

٥.٢.١٩ مرافق معالجة المعلومات

أ. لا يسمح لأي مستخدم باستعمال أي أنظمة معلومات شخصية أو مملوكة شخصيا، مثل الحواسيب المحمولة وأجهزة الحاسب الآلي المنزلية والأقراص الصلبة الخارجية وأدوات التخزين الخارجية (flash disks) والأجهزة اليدوية دون موافقة الادارة المعنية و إدارة تقنية المعلومات.

٦.٢.١٩ الوصول عن بعد

أ. يمنح الوصول عن بعد لشبكة جمعية مراكز الأحياء باستخدام إجراءات تسجيل دخول المستخدمين.

ب. يمنح الوصول عن بعد على أساس الحاجة ولأغراض العمل فقط.

ج. تمنح جمعية مراكز الأحياء إمكانية الوصول عن بعد فقط للاحتياجات التشغيلية الضرورية وتوثق مبررات هذا الوصول ضمن إجراءات تسجيل دخول المستخدمين.

د. يتم اعتماد الوصول عن بعد من قبل مدير إدارة المستخدم ومدير ادارة تقنية المعلومات.

ه. يجب أن تتحكم جمعية مراكز الأحياء بجميع حالات الوصول عن بعد عبر عدد محدود من نقاط الوصول لشبكة المعلومات.

و. يتحمل المستخدم المسئولية عن أن أية تبعات أو آثار سلبية ناشئة عن إساءة استخدام الوصول الى عناصر شبكة معلومات الجمعية.

ز. يجب أن يتم اعتماد الدخول عن بعد من قبل إدارة تقنية المعلومات.

ح. يجب تسجيل كافة اتصالات الدخول عن بعد بما في ذلك عنوان بروتوكول الإنترنت واسم المستخدم الخاص بالدخول.

ط. يجب مراقبة النشاطات المنفذة بعد الدخول عن بعد. وفي حالة عدم استخدام الحساب لمدة ثلاثة أشهر يجب إنهاؤه وإيقافه. وإذا تم طلب الوصول مرة أخرى، فعلى المستخدم أن يطلب حساباً جديداً.

ي. يجب أن يكون للوصول عن بعد آليات قوية للتحقق من الهوية مثل التحقق باستخدام كلمة مرور بمقاطع قوية (مثل استخدام الاحرف و الارقام و الاحرف الخاصة).

## ٣.١٩ الإجراءات

### ١.٣.١٩ تسجيل وصول المستخدم

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | المستخدم | على المستخدم الذي يطلب الدخول إلى نظام المعلومات بتعبئة نموذج ورقي او الكتروني وصول المستخدم ذاكراً فيه صلاحيات النظام المطلوب، وتقديمه لمدير إدارته للحصول على الموافقة.<br><br>الر جاء مراجعة النموذج رقم ( IT_F007) | | | لا يوجد |

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| .٢ | مدير الإدارة المعنية | يراجع مدير الإدارة نموذج طلب وصول المستخدم ويعتمده يرسل النموذج المعتمد إلى رئيس الدعم الفني لفحص الطلب و رفعة لمدير تقنية المعلومات لاعتماده | | | طلب وصول المستخدم |
| .٣ | مدير تقنية المعلومات | يقوم مدير تقنية المعلومات بمراجعة الطلب و اعتماده و الايعاز لمدير القسم المعني بتنفيذه، أو رفضة و إعادته لمدير الادارة المعنية للتصحيح. | | | لا يوجد |
| .٤ | رئيس قسم التطبيقات | يتم كذلك مراجعة طلب وصول المستخدم التابع لأي طرف ثالث واعتماده مبدئياً من مدير الإدارة المعنية آخذاً في الاعتبار المبررات الملائمة لصلاحية الوصول المطلوبة، والفترة المطلوبة الوصول خلالها، ومخاطر منح الوصول لذلك الطرف الثالث . | | | |
| .٥ | الدعم الفني | عند استلام نموذج طلب وصول مستخدم إلى نظام المعلومات، يقوم رئيس قسم الدعم الفني بما يلي:<br>• مراجعة طلب وصول المستخدم إلى نظام المعلومات و ويتم اعتماده حسب الصلاحيات الممنوحة المعرفة في إدارة تقنية المعلومات وفي حالة تجاوز الطلب لصلاحياته، يحيله إلى مدير إدارة تقنية المعلومات للموافقة.<br>• تقييم المخاطر المترتبة على منح صلاحية الوصول إلى مستوى محدد في نظام المعلومات.<br>• التأكد بالتنسيق مع الإدارة المعنية من أن مستوى الوصول المطلوب لا يؤدي إلى تعارض يتعلق بفصل المهام أو مخاطر إفشاء معلومات الجمعية السرية إلى أطراف ثالثة.<br>• إنشاء هوية مستخدم جديد وكلمة مرور على نظام المعلومات، حسب | | | اسم المستخدم وكلمة المرور |

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| | | المطلوب.<br>• إبلاغ المستخدم ومدير الإدارة المعنية عن إنشاء الحساب/ منح الصلاحية بالوصول | | | |
| ٦. | رئيس قسم التطبيقات | الاحتفاظ بسجل (نماذج) رسمي لجميع المستخدمين المسجلين، والاحتفاظ بنماذج طلبات وصول المستخدمين في الملف. | | | سجل النماذج المحدث لطلبات وصول المستخدمين |

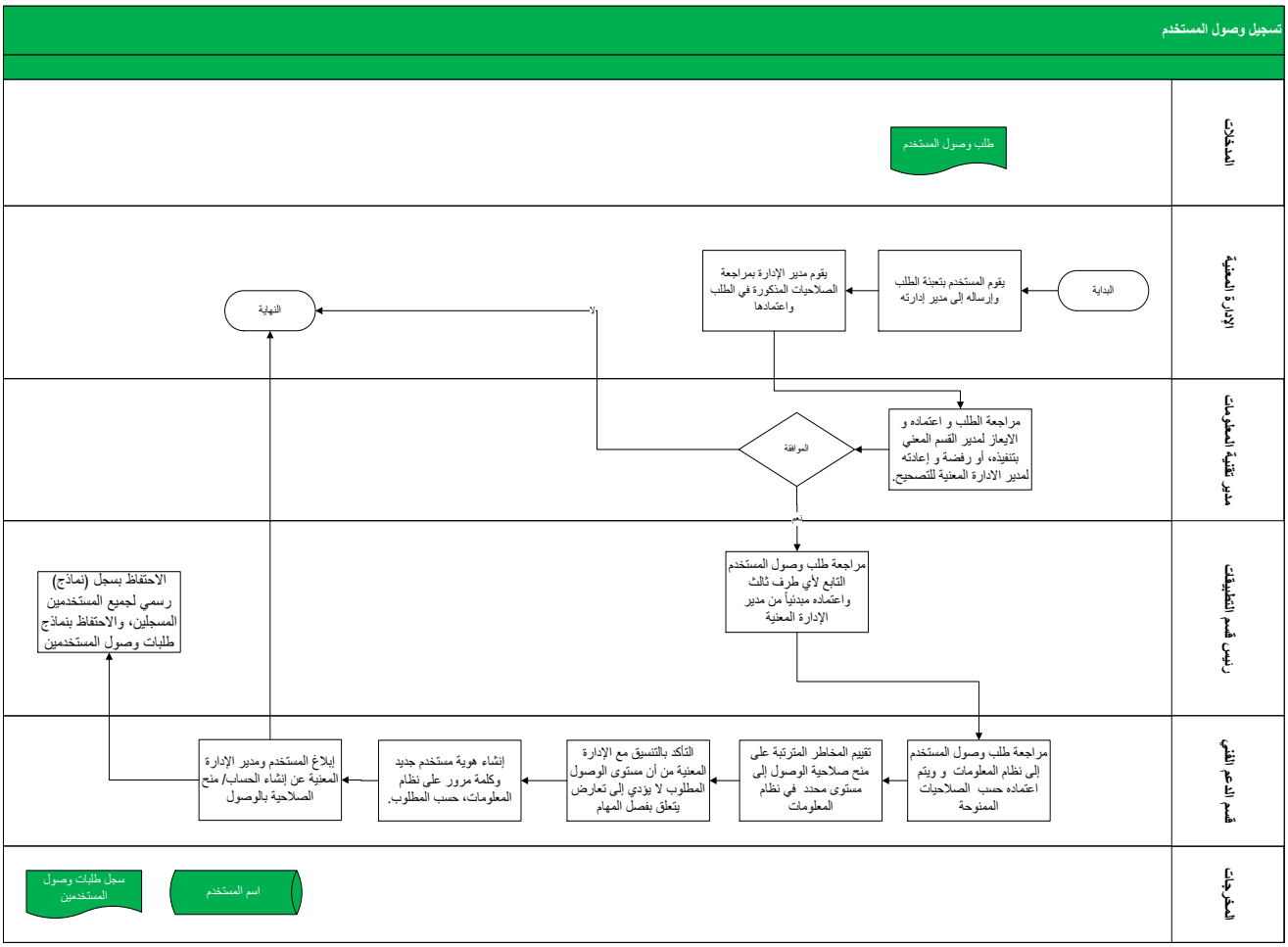
## ٢.٣.١٩ مراجعة صلاحيات وصول المستخدمين

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| ١. | مدير تقنية المعلومات | يقوم مدير إدارة تقنية المعلومات بمراجعة أنظمة المعلومات التي سيتم مراجعة ملفات الوصول فيها. | | | لا يوجد |
| ٢. | مدير تقنية المعلومات | يطور مدير إدارة تقنية المعلومات خطة لمراجعة صلاحيات وصول المستخدمين تتضمن أنظمة المعلومات التي ستتم مراجعتها وتكرار عملية المراجعة. | | | خطة مراجعة الصلاحيات |
| ٣. | مدير تقنية المعلومات | بعد ذلك يقوم مدير إدارة تقنية المعلومات بتعيين المسئولين عن مراجعة صلاحيات دخول المستخدمين (رئيس قسم البنية التحتية ورئيس قسم التطبيقات أو من ينوب عنهما) و عليه يقوم المسئولين بمراجعة ملفات الوصول للمستخدمين بالتنسيق مع الادارات المعنية وتأكيد ما يلي:<br>• فيما إذا كانت الصلاحيات متوافقة مع الأدوار والمسئوليات المعينة للموظفين.<br>• أن الصلاحيات لا تخالف | | | |

| الرقم | المسؤول | العملية | الوقت | الطريقة | المخرج |
|---|---|---|---|---|---|
| | | مبادئ الفصل في المهام. | | | |
| ٤. | مدير الإدارة المعنية | يقوم المسؤولين بالتبليغ عن أي استثناءات إلى مدير تقنية المعلومات.<br>يقوم مدير تقنية المعلومات بالموافقة علي اية الاستثناءات في الصلاحيات بالتنسيق مع الادارات المعنية. | | | تقرير الاستثناءات |
| ٥. | رئيس قسم البنية التحتية<br>رئيس قسم التطبيقات | يتم تحديث صلاحيات الدخول للمستخدمين المعنيين. | | | ملفات التعريف المحدثة للمستخدمين |

## ٤.١٩ دورات العمل

### ١.٤.١٩ تسجيل وصول المستخدم



## ٢.٤.١٩ مراجعة صلاحيات وصول المستخدمين