1

سياسة الأمن المادي والبيئي

م/ سيف السياغي

بنود السياسة

يجب تأمين المعدات والتحكم في الوصول المادي والبيئة الفيزيائية المحيطة بالأصول الخاصة لكل جهة حكومية وبما يضمن الاستخدام الآمن والأمثل لهذه الأصول، وبما يشمل:

- حماية أماكن المنظومات المعلوماتية التابعة للجهة والتي يتم فيها معالجة وحفظ المعلومات من الاختراق والكوارث الطبيعية أو الصناعية أو الدخول غير المصرح به.
- حماية كافة التجهيزات وجميع نظم المعلومات ووضعها في بيئة آمنة والسماح بالنفاذ/الوصول للموظفين المخولين فقط لمنع الوصول غير المسموح به.
- حماية وسائط حفظ البيانات ووسائط النسخ الاحتياطي التي تحتوي على معلومات أساسية أو حساسة على مسافة آمنة من الموقع الرئيسي لتفادي الأضرار التي قد تنجم عن كارثة في الموقع الرئيسي.
- اختيار مكان آمن للمعدات والتجهيزات التقنية بحيث تكون مؤمنة جيداً من ناحية الأمن المادي ومحمية من الكوارث والتهديدات الأمنية سواء طبيعية أو غيرها، وذلك لتقليل حجم الخسائر ومدة خروجها عن الخدمة وأن تكون في مستوى أمني مناسب.

بنود السياسة

- في حال وجود أي معدات تابعة للجهة وتحتوي على معلومات خاصة بها في عهدة أي من الموظفين فيجب تطبيق المعايير الأمنية للحفاظ على هذه المعدات وسلامة المعلومات المتواجدة بها.
- يجب أن تحدد أسماء الموظفين وتوصيفهم الوظيفي المخولين بالوصول إلى مواقع البيانات والمعدات، على أن يتم مراجعة هذه الأسماء بشكل دوري.
- يجب توفير تجهيزات وأنظمة أمنية خاصة بإدارة الدخول والإغلاق لمواقع البيانات وغرف المعدات وما شابه، مثل انظمة البصمة والبطائق الممغنطة وأن تكون ضمن إجراءات أمنية محددة وصارمة.
- تركيب أنظمة تسجيل ومراقبة لمواقع البيانات وغرف المعدات وأن تكون على مدار الساعة.
- يجب تفعيل خاصية الحماية التلقائية في السيرفرات واجهزة الحاسوب والحواسيب المحمولة وغيرها بحيث يتم إغلاق هذه الأجهزة تلقائياً في حال عدم الاستخدام لفترة قصيرة ومحددة.
- يجب أن توضع شاشات العرض الخاصة بطريقة لا تسمح لغير المصرح لهم برؤيتها.

عناصر السياسة

- المقدمة
- الاهداف
- النطاق
- البنود الخاصة بالجهة الحكومية لسياسة الأمن المادي والبيئي
- الأدوار والمسئوليات

مقدمة

الأمان المادي هو مجموعة من الإجراءات الأمنية التي يتم تبنيها لضمان عدم وصول غير المصرح لهم إلى مواد ومعدات الأصول المعلوماتية كافة وخاصة بمركز البيانات، إذ يمكن أن تتألف إجراءات الأمان المادي من طرق واسعة لردع وإحباط الدخلاء بما في ذلك اللجوء لطرق تعتمد على التقنية.

يجب أن يكون مركز البيانات وغرفة معدات تقنية المعلومات والاتصالات في مناطق محمية مادياً ضد الوصول غير المصرح ويجب أن تمتثل لسياسات الأمن المادي لحماية الأصول والأنظمة المعلوماتية من الدخول الغير مصرح به وصونها من المخاطر.

إجراءات أولية

على الجهة الحكومية تحديد الأصول المادية والبيئية التي يجب حمايتها: يمكن أن تشمل هذه الأصول:

- البنية التحتية المادية، مثل المباني والمرافق .
- المعدات والأنظمة، مثل أجهزة الكمبيوتر والخوادم والشبكات.
- المعلومات الحساسة، مثل البيانات المالية والشخصية.
- وغيرها من الاصول حسب احتياج وطبيعة عمل الجهة.

تحديد المخاطر المحتملة التي تواجه هذه الأصول: يمكن أن تشمل هذه المخاطر:

- السرقة أو التخريب أو الضياع.
- الكوارث الطبيعية أو الصناعية.
- الهجمات الارهابية .

تحديد الإجراءات والضوابط اللازمة للحماية من هذه المخاطر: يمكن أن تشمل هذه الإجراءات والضوابط:

- أنظمة التحكم في الوصول المادي.
- أنظمة مكافحة الحريق.
- أنظمة الإنذار الأمني وكامرات المراقبة.
- وضع بنود وإجراءات أمنية مناسبة
- أنظمة التحكم في الوصول المادي.

الاهداف

منع الوصول المادي لغير المصرح لهم، وضمان حماية موارد المعلومات من خلال تدابير الأمن المادي والبيئي التي تمنع التلاعب المادي أو التلف أو السرقة أو الوصول المادي غير المصرح به.

حماية الموارد التقنية والمعدات والبيانات من السرقة والعبث والكوارث الطبيعية والتخريب والهجمات السيبرانية وغيرها من الأفعال المؤذية وبالتالي الحفاظ على استمرار الخدمات والاعمال.

نموذج لتقسيم (الجهة الحكومية) من الناحية الأمنية

نموذج لتقسيم (الجهة الحكومية) من الناحية الأمنية الى ثلاث مناطق :

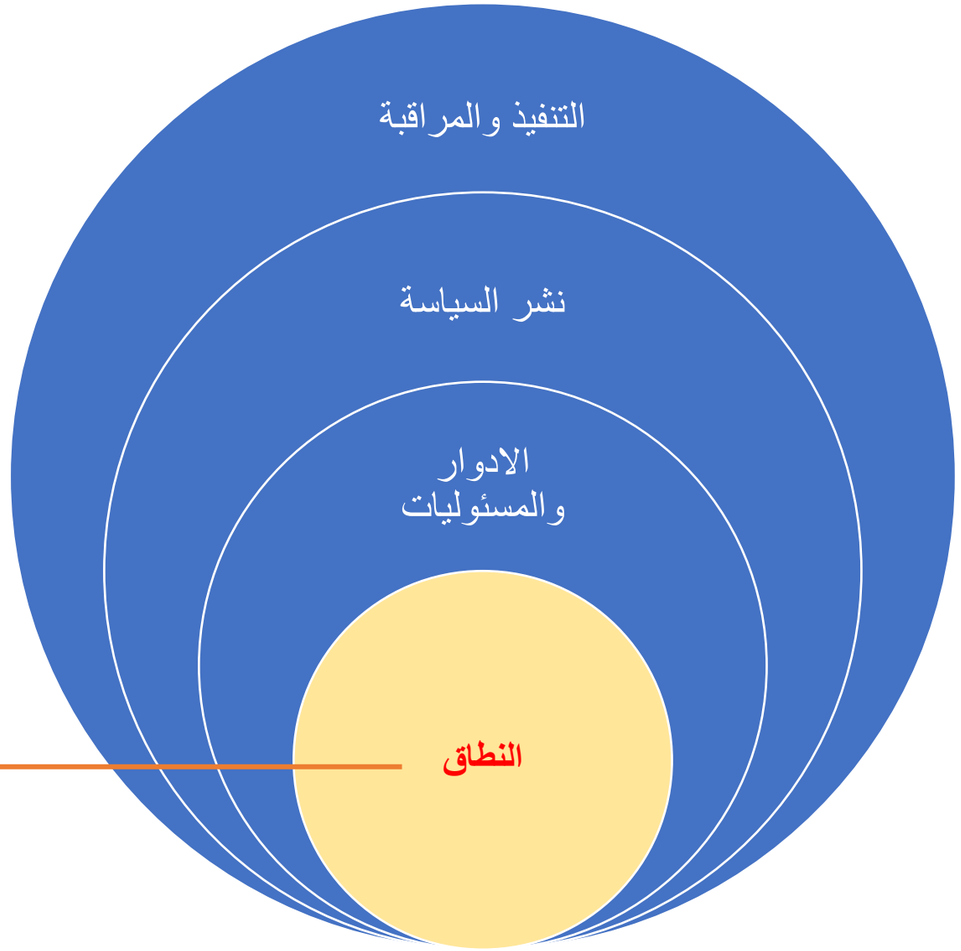
1. المناطق العامة وهي المناطق التي يسمح لأي شخص بالتواجد فيها داخل الوزارة .
2. المناطق المحدودة وهي المناطق الخاصة بموظفي الجهة الحكومية ولا يسمح لأي زائر خارجي دخولها إلا ببطاقة زائر.
3. المناطق الآمنة وهي المناطق التي لا يسمح بتواجد أي شخص أو موظف فيها إلا للمصرح لهم فقط أو بموافقة مسبقة .

البنود الخاصة بالجهة الحكومية لسياسة الأمن المادي والبيئي

على سبيل المثال :

- لا يسمح بتركيب أو نقل أو صيانة الأجهزة بجميع أنواعها إلا بإتباع الإجراءات المحددة في سياسات (إدارة الأصول المعلوماتية ، الاستخدام المقبول للأصول ،ضبط التغيير ، أمن الشبكات والاتصال)
- يجب على مسئولي البنية التحتية عدم الإفصاح عن محتويات مركز البيانات ونشاطاته.
- يمنع دخول أي شخص ليس له علاقة في عمل مركز/مراكز البيانات الا بتصريح ومبرر للدخول وبرفقة مسئول البنية التحتية مع إشعار مسئول أمن المعلومات بذلك.
- يمنع تصوير داخل أو خارج مركز البيانات بأي وسيلة من وسائل التصوير، ويتم وضع لافتة تحذيرية بذلك.
- يمنع الأكل أو التدخين أو الشرب داخل المناطق المؤمنة .
- وغيرها.....الكثير

تنطبق هذه السياسة على جميع الاصول المعلوماتية وجميع الموظفين العاملين بالجهة الحكومية والجهات الخارجية المتعاقد معها



القيادة العليا: **امثلة**

- وضع التعليمات الخاصة بتحديد المناطق المؤمنة والصلاحيات الممنوحة للأشخاص المخولين .
- توفير جميع المتطلبات الخاصة بتحقيق الأمن المادي .
- وضع التعليمات الخاصة بالزوار

مسؤول أمن المعلومات :

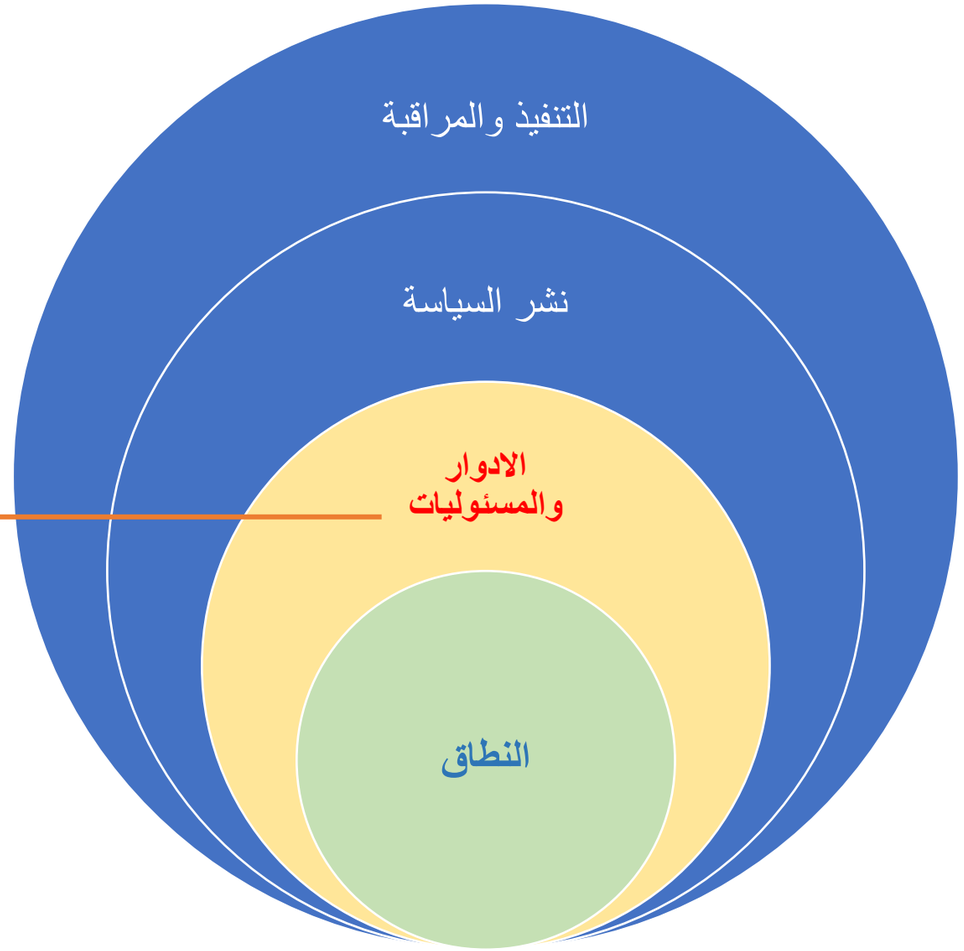
- تطوير إجراءات وضوابط الأمن المادي والبيئي.
- مراقبة تنفيذ إجراءات وضوابط الأمن المادي والبيئي.
- إجراء التدقيقات الأمنية.

الموظفين:

- اتباع الإجراءات والضوابط المحددة في سياسة الأمن المادي والبيئي.
- الإبلاغ عن أي حوادث أو تهديدات للأمن المادي والبيئي.

ضابط الأمن :

-التحقق من هويات الزوار وتوثيق بياناتهم وغرض الزيارة.

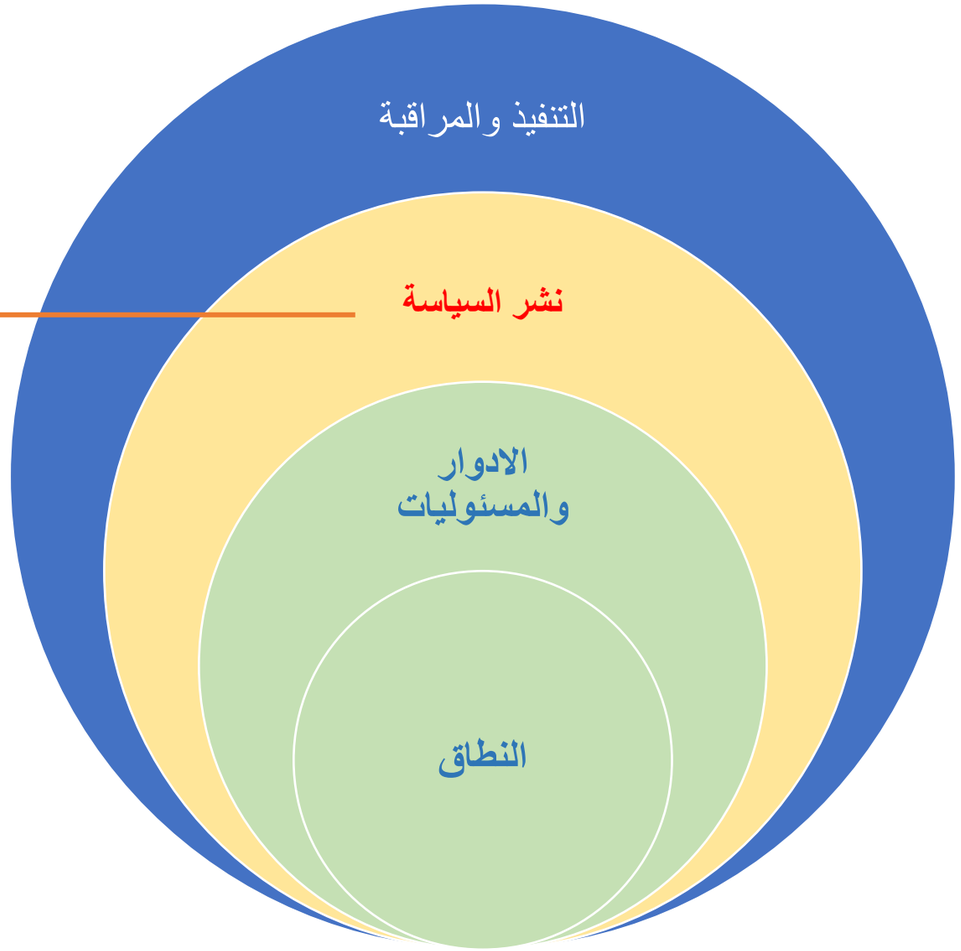


اعتماد السياسة .

نشر السياسة .

التوعية للموظفين بها وتدريبهم عليها

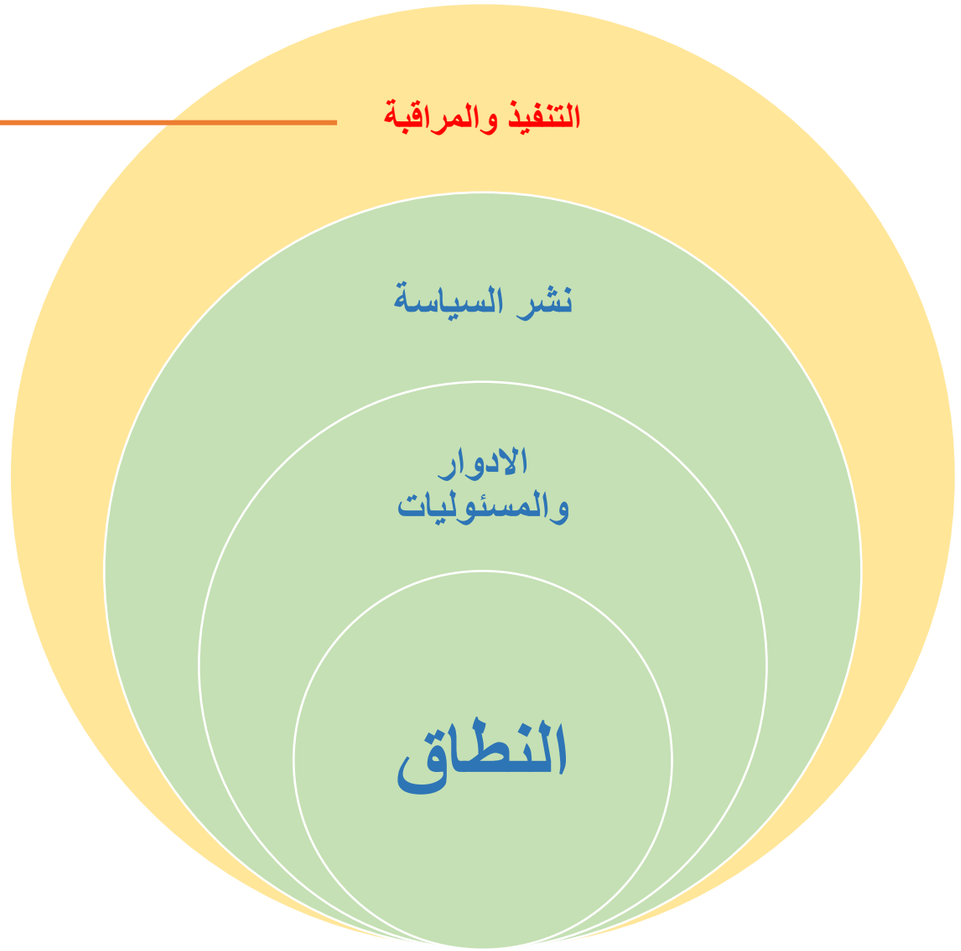
اخذ اقرارات الموظفين بالالتزام بها .



التنفيذ والمراقبة

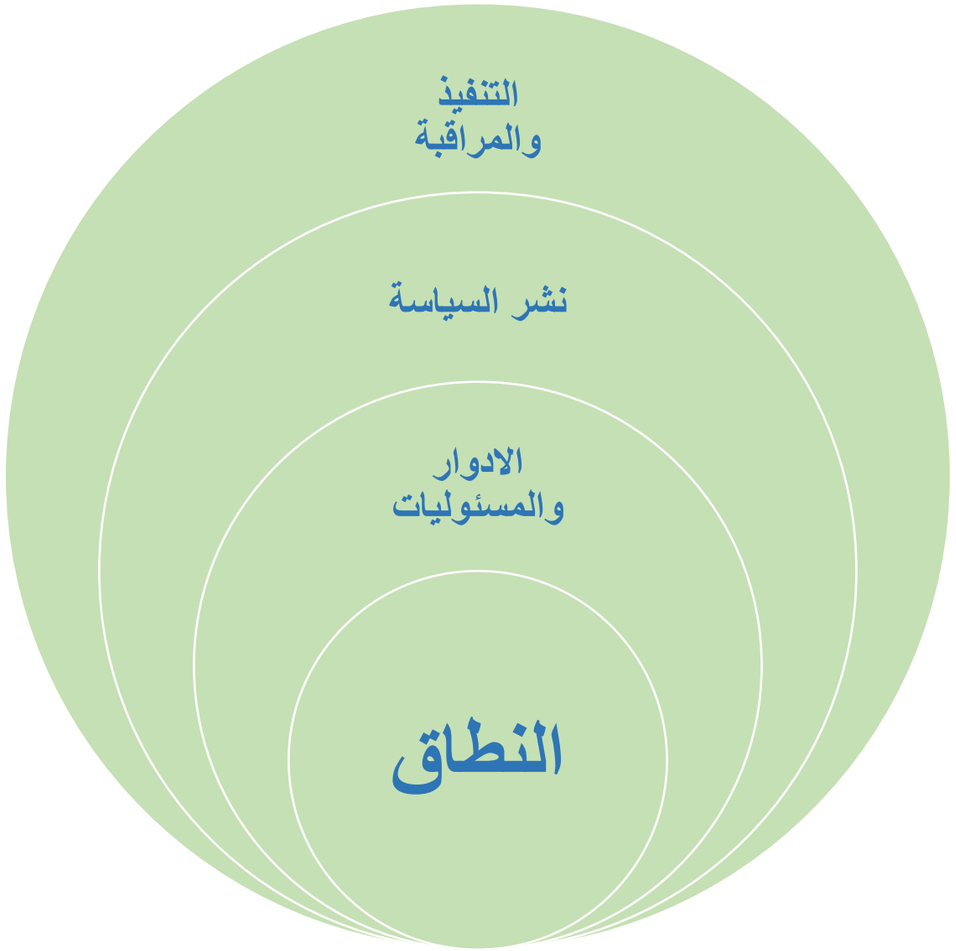
- تنفيذ السياسة وفقًا للإجراءات المحددة:
  يجب تنفيذ السياسة وفقًا للإجراءات المحددة في السياسة نفسها.

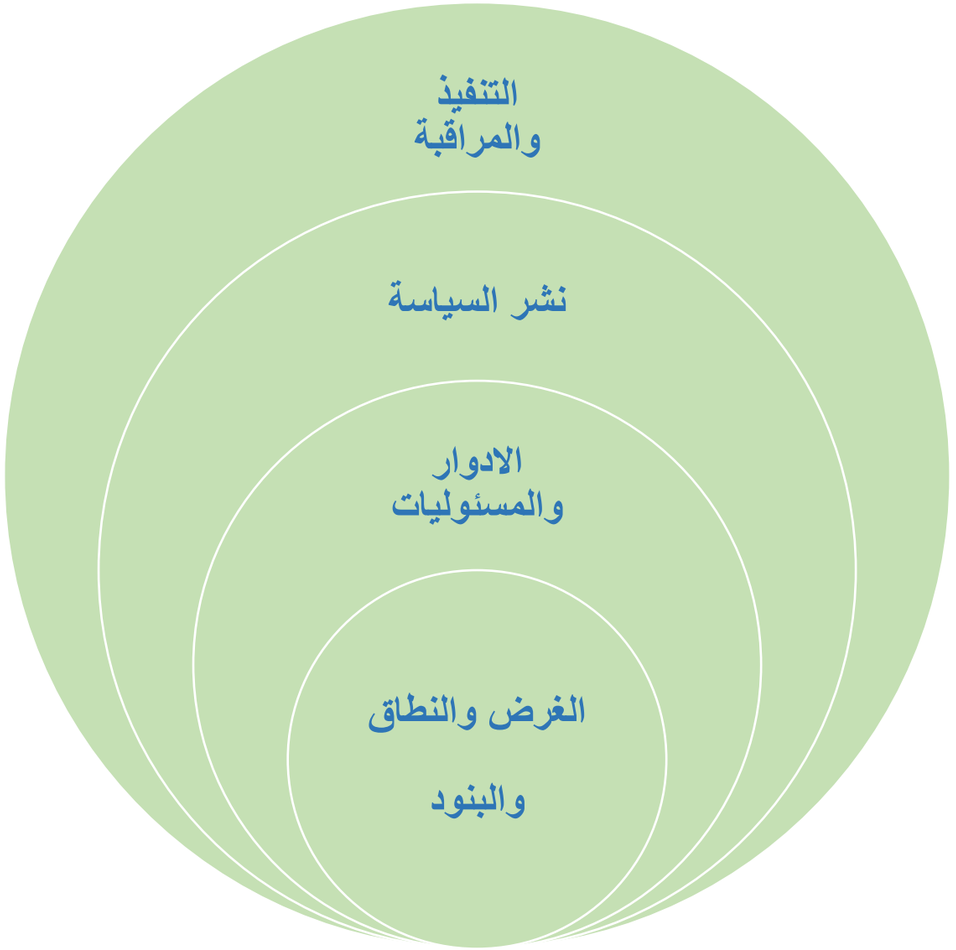
- مراقبة فعالية السياسة وإجراء التعديلات اللازمة:
  يجب مراقبة فعالية السياسة بانتظام وإجراء التعديلات اللازمة لضمان فعاليتها المستمرة.



التوصيات

- يجب أن تكون سياسة الأمن المادي والبيئي شاملة وواسعة النطاق.
- يجب أن تستند السياسة إلى تقييم مخاطر شامل
- ان تكون الادوار والمسئوليات عنصر اساسي في الحد من هذه التهديدات والمخاصر.
- يجب أن تكون السياسة قابلة للتنفيذ من حيث التكلفة والتنفيذ.
- يجب أن تكون السياسة موضوعة للمراجعة والتقييم بانتظام ومحدثة عند مواجهة تهديدات جديدة يتم ادراجها ويمر بنفس المعالجات التي تمت في الاصدار السابق.





التوصيات

- يجب أن تكون سياسة الأمن المادي والبيئي شاملة وواسعة النطاق.
- يجب أن تستند السياسة إلى تقييم مخاطر شامل.
- يجب أن تكون السياسة قابلة للتنفيذ من حيث التكلفة والتنفيذ.
- يجب أن تكون السياسة موضوعة للمراجعة والتقييم بانتظام.