سياسة أمن وسرية المعلومات

المؤسسة العامة للغذاء والدواء

Ver 1.0

Preparation Date	**15.03.2026**
Implementation Date	**09.04.2026**

Prepared by	Checked by
Dr. Maha Jaghbeer **Eng. Salam Otoum**	

1. الهدف

تهدف هذه السياسة إلى وضع إطار مؤسسي متكامل لحماية المعلومات والأصول المادية والرقمية في المؤسسة العامة للغذاء والدواء، بما يضمن:

1. الحفاظ على **سرية المعلومات وسلامتها وتوافرها**.
2. حماية الأصول المادية والرقمية والوثائق والسجلات من الوصول غير المصرح به أو الفقد أو التلف أو التسريب أو العبث.
3. ضبط الوصول إلى المعلومات والأنظمة والمواقع الحساسة وفق مبدأ الحاجة إلى المعرفة وطبيعة المهام الوظيفية.
4. تنظيم تصنيف المعلومات والأصول وتطبيق وسائل الحماية المناسبة لكل مستوى.
5. حماية البيانات في جميع مراحل **دورة حياتها** من الإنشاء أو الجمع، مرورًا بالتخزين والاستخدام والنقل والمشاركة، وصولًا إلى الإتلاف الآمن.
6. تعزيز الوعي والمسؤولية الفردية والمؤسسية تجاه أمن المعلومات والأمن السيبراني والأمن المادي وأمن الأفراد.
7. دعم استمرارية الأعمال وتقليل المخاطر المرتبطة بالتهديدات الداخلية والخارجية.
8. ضمان وجود ضوابط واضحة للنسخ الاحتياطي، والاستعادة، والاستجابة للحوادث، والتوثيق، والتدقيق، والمتابعة.

---

2. نطاق التطبيق

تطبق هذه السياسة على:

1. جميع موظفي المؤسسة، والمستخدمين المفوضين، وأعضاء اللجان والخبراء الخارجيين، والمتعاقدين والموردين والشركاء الذين يطلعون على معلومات المؤسسة أو يتعاملون مع أصولها.
2. جميع المعلومات والبيانات الورقية والإلكترونية والسجلات والوثائق وقواعد البيانات والمراسلات الرسمية.
3. جميع الأصول المادية والرقمية، بما في ذلك الأجهزة، الخوادم، الشبكات، الأنظمة، البرمجيات، وسائط التخزين، غرف الأرشفة، ومراكز البيانات.
4. جميع مراحل دورة حياة البيانات.
5. جميع المواقع والمرافق الحساسة ذات العلاقة بحفظ أو معالجة أو نقل المعلومات أو الأصول.

---

3. المرجعيات

تُقرأ هذه السياسة بالاقتران مع:

1. سياسة إدارة وأمن المباني وبيئة العمل.
2. سياسة إدارة المرافق والصيانة الوقائية والدورية.
3. سياسة تصنيف وإدارة البيانات.
4. سياسة النسخ الاحتياطي والتعافي من الكوارث، إن وجدت.
5. سياسات وإجراءات الأمن السيبراني المعتمدة في المؤسسة.
6. التشريعات الوطنية والتعليمات النافذة ذات العلاقة.
7. متطلبات أنظمة الجودة وإدارة المخاطر واستمرارية الأعمال المعتمدة في المؤسسة.
8. متطلبات WHO GBT ذات العلاقة بالحوكمة، وإدارة الوثائق والسجلات، والموارد، واستمرارية أداء الوظائف التنظيمية.

4. المبادئ العامة

تعتمد هذه السياسة على المبادئ الآتية:

1. **السرية :(Confidentiality)** عدم إتاحة المعلومات إلا للمخولين.
2. **السلامة/التكامل :(Integrity)** حماية المعلومات من التغيير أو العبث أو الإتلاف غير المصرح به.
3. **التوافر :(Availability)** ضمان إتاحة المعلومات والأنظمة للمخولين عند الحاجة.
4. **الحاجة إلى المعلومة**.
5. **الحد الصلاحيات والمسؤوليات**.
6. **المساءلة والتتبع** لجميع عمليات الوصول أو التعديل أو النقل أو الإتلاف.
7. **الحماية المبنية على تقييم المخاطر**.
8. **التكامل بين الأمن المعلوماتي والأمن السيبراني والأمن المادي وأمن الأفراد**.

5. المسؤوليات

5.1 الإدارة العليا

1. اعتماد السياسة والتحديثات المتعلقة بها.
2. دعم توفير الموارد اللازمة لتنفيذها.
3. الإشراف العام على الامتثال المؤسسي لمتطلبات أمن المعلومات وسريتها.

5.2 المديريات والإدارات المعنية

1. تطبيق هذه السياسة ضمن نطاق اختصاصها.
2. تحديد المعلومات والأصول الحساسة التابعة لها.
3. ضمان التزام الموظفين بالإجراءات المعتمدة.
4. الإبلاغ عن الحوادث أو نقاط الضعف أو حالات عدم الامتثال.
5. التأكد من توقيع نماذج وتضارب المصالح والمحافظة على سرية المعلومات حيثما يلزم

5.3 وحدة تكنولوجيا المعلومات

1. إدارة الصلاحيات والوصول إلى الأنظمة والشبكات.
2. حماية الشبكات والخوادم والأنظمة وقواعد البيانات.
3. تطبيق ضوابط الحماية التقنية مثل التشفير والجدران النارية والمراقبة والتحديثات.
4. تنفيذ وإدارة النسخ الاحتياطي والاستعادة.
5. الاستجابة للحوادث السيبرانية وتوثيقها.
6. حماية غرف مراكز البيانات وغرف الأجهزة الحساسة بالتنسيق مع الجهات المعنية.
7. اعداد طرق العمل القياسية المتعلقة بالتعامل مع البيانات والمعلومات لضمان امنها وتدريب العاملين في المؤسسة عليها دوريا.

5.4 الجهة المعنية بالمخاطر والجودة/الحوكمة

1. تطوير وتحديث السياسات والإجراءات ذات العلاقة.
2. تقييم ومتابعة المخاطر المرتبطة بالمعلومات والأصول.
3. متابعة الامتثال ورفع التقارير والتوصيات التحسينية.
4. دعم برامج التوعية والتدريب.

5.5 مديرية الموارد البشرية والادارية المعنية بالمباني والمرافق

1. تأمين المواقع المادية والمرافق المرتبطة بالأصول والمعلومات.
2. ضبط الدخول إلى المواقع الحساسة.
3. حماية الأرشيفات وغرف الملفات والأصول المادية الحساسة.
4. اعداد طرق العمل القياسية المتعلقة بالتعامل مع المباني والمرافق لضمان امنها وتدريب العاملين في المؤسسة عليها دوريا.
5. إدماج التزامات السرية وأمن المعلومات ضمن إجراءات التوظيف والتعيين.
6. التأكد من توقيع العاملين في المؤسسة للتعهدات ومدونة قواعد السلوك الوظيفي.
7. التنسيق لسحب أو تعديل الصلاحيات عند النقل أو إنهاء الخدمة

5.6 لجان الاتلاف للوثائق

1. . توفير وسائل الإتلاف المادي الآمن للوثائق وفق الإجراءات المعتمدة.

5.7جميع الموظفين والمستخدمين

1. المحافظة على سرية المعلومات والبيانات والأصول التي تقع في عهدتهم.
2. استخدام الأنظمة والبريد الإلكتروني والإنترنت والأجهزة لأغراض العمل الرسمي فقط.
3. الإبلاغ الفوري عن أي حادث أو اشتباه أو ضعف أمني.
4. عدم إفشاء كلمات المرور أو مشاركة الوصول أو تجاوز الصلاحيات.

5.8الموردون والشركاء والمتعاقدون

1. الالتزام بشروط السرية وأمن المعلومات المعتمدة من المؤسسة.
2. توقيع تعهدات بعدم الإفصاح حيثما ينطبق.
3. الالتزام بالضوابط الأمنية أثناء الوصول إلى معلومات المؤسسة أو أنظمتها أو مواقعها.

---

6. التعريفات

تشمل هذه السياسة، لغايات التطبيق، التعريفات الآتية:

1. **أمن المعلومات :**مجموعة السياسات والإجراءات والضوابط الهادفة إلى حماية سرية المعلومات وسلامتها وتوافرها.
2. **الأمن السيبراني :**الإجراءات المتخذة لحماية الأنظمة والشبكات والبنية التحتية الرقمية من التهديدات والحوادث السيبرانية.
3. **الأمن المادي :**الإجراءات المتخذة لحماية المواقع والمرافق والأصول المادية من الوصول غير المصرح به أو التلف أو الأخطار البيئية.
4. **أمن الأفراد :**الضوابط المتعلقة بسلوك الأفراد، والتحقق من خلفياتهم، وامتثالهم، وتقليل المخاطر الداخلية.
5. **الأصول :**جميع الممتلكات المادية والرقمية وغير الملموسة التي تستخدمها المؤسسة لتحقيق أهدافها.

6. **تصنيف المعلومات/البيانات :**تقسيم المعلومات والبيانات إلى مستويات وفق حساسيتها وتأثير فقدانها أو إفشائها أو العبث بها.
7. **دورة حياة البيانات :**المراحل التي تمر بها البيانات من الإنشاء أو الجمع إلى الإتلاف الآمن.
8. **الحادث الأمني/السيبراني :**أي واقعة تؤثر أو قد تؤثر على سرية أو سلامة أو توافر المعلومات أو الأصول أو الأنظمة.
9. **العلامات الوقائية :**إشارات أو وسوم أو ملصقات مادية أو رقمية تبين مستوى الحساسية ومتطلبات الحماية.

---

7. تصنيف المعلومات والأصول

1. يجب تصنيف المعلومات والبيانات والأصول بحسب حساسيتها وتأثير فقدانها أو إفشائها أو إساءة استخدامها.
2. يعتمد تصنيف المعلومات والأصول وفق السياسة أو التعليمات المعتمدة في المؤسسة.
3. تُطبَّق وسائل الحماية المناسبة لكل مستوى تصنيف.
4. تُستخدم العلامات الوقائية أو وسوم التصنيف على الوثائق الورقية والإلكترونية والأصول الحساسة حيثما يلزم.
5. تشمل المعلومات عالية الحساسية، على سبيل المثال لا الحصر:
    - ملفات الموظفين.
    - البيانات التنظيمية أو الفنية غير المعلنة.
    - الملفات المقدمة من المراجعين أو الشركات أو المتعاملين.
    - السجلات الرقابية أو القانونية أو الفنية المقيدة.
    - كلمات المرور ومفاتيح الوصول والإعدادات الحرجة.

---

8. التحكم بالوصول والصلاحيات

1. يمنح الوصول إلى المعلومات والأنظمة والمواقع الحساسة وفق طبيعة العمل والحاجة الفعلية.
2. تُمنح الصلاحيات وتحجب وتراجع بشكل دوري وفق الوصف الوظيفي ومصفوفة الصلاحيات المعتمدة.
3. يُمنع استخدام حسابات الآخرين أو مشاركة الحسابات أو كلمات المرور.
4. يجب سحب أو تعديل الصلاحيات فور نقل الموظف أو تغيير مهامه أو انتهاء خدمته أو انتهاء حاجة المستخدم الخارجي للوصول.
5. يخضع الدخول إلى المواقع الحساسة وغرف الخوادم والأرشيف والمستودعات وغرف المراقبة لضوابط دخول خاصة.

---

9. ضوابط استخدام الأجهزة والبرمجيات

1. تثبت البرمجيات وتحدث من خلال الجهة المختصة فقط.
2. يمنع تحميل أو تثبيت أي برامج غير معتمدة.
3. تستخدم الأجهزة والبرمجيات لأغراض العمل الرسمي فقط.
4. يمنع فتح أو صيانة أو فك أجهزة المؤسسة إلا من قبل الجهة الفنية المخولة.
5. يمنع تخزين ملفات شخصية أو غير مرتبطة بالعمل على أجهزة المؤسسة.
6. تُطبق ضوابط الحماية على الأجهزة المحمولة ووسائط التخزين والأجهزة المتصلة بالشبكة.

10.ضوابط استخدام الإنترنت والشبكات

1. يستخدم الإنترنت وشبكات المؤسسة لغايات العمل الرسمي فقط.
2. تخضع الشبكات والاتصالات للفلترة والمراقبة والتسجيل وفقًا للضوابط المعتمدة.
3. يمنع استخدام شبكات أو وسائل اتصال خارجية غير معتمدة على أجهزة المؤسسة أو لربطها بأنظمة المؤسسة.
4. يمنع إدخال برامج خبيثة أو أدوات اختراق أو استخدام أدوات قرصنة أو تجاوز ضوابط الحماية.
5. يحق للمؤسسة تطبيق وسائل الحجب والفلترة والمراقبة وحفظ السجلات وفق التشريعات والتعليمات النافذة.
6. تُدار صلاحيات الوصول إلى الشبكات السلكية واللاسلكية والشبكات الافتراضية وفقًا للضوابط المعتمدة.

---

11. البريد الإلكتروني والاتصالات الإلكترونية

1. يستخدم البريد الإلكتروني المؤسسي لغايات العمل الرسمي فقط.
2. يمنع إرسال رسائل عشوائية أو رسائل تنتحل الهوية أو تحتوي محتوى مخالفًا أو غير مشروع.
3. يجب عدم فتح الروابط أو الملفات من مصادر مشبوهة.
4. في حال الاشتباه برسالة أو مرفق أو رابط، يجب التحقق من الجهة المرسلة أو إبلاغ الجهة المختصة فورًا.
5. يجب مراعاة التسلسل الإداري والمهنية والدقة عند استخدام البريد الإلكتروني.
6. يجب أرشفة الرسائل المهمة وفق الإجراءات المعتمدة.

---

12 .كلمات المرور والمصادقة

1. تعد كلمات المرور معلومات حساسة ويمنع إفشاؤها أو مشاركتها.
2. يجب أن تكون كلمات المرور قوية ومعقدة ومحدثة دوريًا وفق الضوابط الفنية المعتمدة.
3. يمنع استخدام كلمات مرور شخصية أو يسهل تخمينها.
4. يجب تغيير كلمة المرور فور الاشتباه بكشفها أو إساءة استخدامها.
5. يجوز تطبيق متطلبات إضافية مثل:
    - الحد الأدنى لطول كلمة المرور.
    - استخدام الرموز الخاصة والأرقام والأحرف.
    - تحديد عمر الصلاحية.
    - منع إعادة استخدام كلمات المرور السابقة.
6. تعتمد المؤسسة وسائل مصادقة إضافية حيثما لزم ذلك.

---

13. الحماية من البرمجيات الخبيثة

1. يجب تشغيل وتحديث برامج الحماية من الفيروسات والبرمجيات الخبيثة على الأجهزة المعتمدة.
2. يجب فحص الملفات والوسائط والبيانات قبل تنزيلها أو تشغيلها أو نقلها.
3. يجب الإبلاغ فورًا عن أي بطء غير طبيعي أو سلوك مشبوه أو رسائل غير مألوفة أو مؤشرات اختراق.
4. تتولى الجهة المختصة التوعية والإجراءات الفنية والاستجابة اللازمة.

---

14. النسخ الاحتياطي والاستعادة

1. تحفظ نسخ احتياطية منتظمة للبيانات والأنظمة الحرجة وفق خطة معتمدة.
2. يحدد نطاق النسخ الاحتياطي وأولوياته بناءً على أهمية البيانات والأصول.
3. تحفظ النسخ الاحتياطية في مواقع مناسبة وآمنة مع مراعاة الفصل الجغرافي عندما يلزم.
4. تخضع وسائط النسخ الاحتياطي لضوابط حماية مادية ومنطقية.
5. توثق إجراءات النسخ والاستعادة بوضوح، بما في ذلك المسؤوليات، والمدة الزمنية، وآلية الطلب، وحالات التفعيل.
6. تختبر صلاحية النسخ الاحتياطية وإجراءات الاستعادة دوريًا، وخاصة بعد أي تغيير جوهري.
7. تحفظ النسخ وفق مدد الاحتفاظ المعتمدة، ويتم التخلص منها بطريقة آمنة عند انتهاء الحاجة إليها.

---

15. دورة حياة البيانات

15.1 الإنشاء والجمع

1. تُجمع البيانات وتنشأ وفق الحاجة الفعلية وبالحد الأدنى اللازم.
2. يستخدم الموظفون معرفات فريدة وكلمات مرور قوية.
3. يجب حماية الشاشات والوثائق وعدم ترك المعلومات الحساسة مكشوفة.
4. يمنع مناقشة المسائل الحساسة في أماكن غير مناسبة أو أمام غير المخولين.

15.2 التخزين والحفظ

1. تخزن البيانات الحساسة على أنظمة أو منصات معتمدة وآمنة.
2. تطبق الحماية الفنية والفيزيائية المناسبة على أماكن الحفظ.
3. تضبط صلاحيات الوصول إلى البيانات المخزنة وتراجع دوريًا.

15.3 النقل والمشاركة

1. تستخدم قنوات ووسائل معتمدة وآمنة لنقل البيانات.
2. يمنع استخدام وسائل غير معتمدة أو غير مؤمنة لنقل المعلومات الحساسة.
3. توثق عمليات النقل أو المشاركة عندما تستدعي طبيعة المعلومات ذلك.

15.4 الإتلاف الآمن

1. تتلف الوثائق الورقية الحساسة وفق إجراءات رسمية معتمدة تضمن عدم إعادة بنائها أو استرجاعها.
2. تتلف البيانات الرقمية أو تمحى بوسائل آمنة ومعتمدة تمنع استعادتها.
3. توثق عمليات الإتلاف في سجلات أو محاضر معتمدة.

---

16. أمن الأفراد

1. تُراعى اعتبارات النزاهة والثقة والسرية عند التعيين أو التكليف أو منح الوصول للمعلومات الحساسة.
2. يوقع الموظفون والمستخدمون المعنيون على التعهدات اللازمة المتعلقة بالسرية ومدونة السلوك وعدم تعارض المصالح عند الاقتضاء.

3. يجري تحديث ضوابط الوصول والصلاحيات بشكل فوري عند التغيير الوظيفي أو انتهاء الخدمة.
4. يخضع الموظفون للتوعية المستمرة بشأن الهندسة الاجتماعية، والتصيد الاحتيالي، وواجبات السرية والإبلاغ.

---

17. الموردون والشركاء والمتعاقدون

1. يخضع الموردون والشركاء والمتعاقدون للضوابط الأمنية ذات العلاقة قبل تمكينهم من الوصول إلى المعلومات أو الأنظمة أو المواقع الحساسة.
2. توقيع تعهدات بعدم إفصاح وشروط حماية معلومات عند الحاجة.
3. تُجرى تقييمات أولية ودورية لالتزامهم بمتطلبات الأمن وحماية المعلومات.
4. يحدد الوصول الممنوح لهم ومدته ونطاقه ومسؤوليته بوضوح.

---

18. الأمن المادي المرتبط بالمعلومات

1. تحمى المواقع الحساسة التي تحتوي على معلومات أو خوادم أو أرشيفات أو نسخ احتياطية أو أصول تقنية بضوابط مادية مناسبة.
2. يشمل ذلك الأقفال المناسبة، والأنظمة البيومترية، وكاميرات المراقبة، وسجلات الدخول، وضبط الزوار، وحماية البيئة التشغيلية.
3. تُقرأ هذه الأحكام بالاقتران مع سياسة إدارة وأمن المباني وبيئة العمل.

---

19. إدارة الحوادث الأمنية والسيبرانية

1. يجب الإبلاغ الفوري عن أي حادث أو اشتباه أو ضعف أمني قد يؤثر على المعلومات أو الأصول أو الأنظمة.
2. تتولى الجهة المختصة تقييم الحادث واحتواءه والتحقيق فيه ومعالجته والتنسيق مع الجهات ذات العلاقة.
3. توثق الحوادث والإجراءات المتخذة والدروس المستفادة والإجراءات التصحيحية والوقائية.
4. تُرفع الحوادث الجسيمة أو الحرجة إلى الإدارة العليا وفق آلية التصعيد المعتمدة.
5. يجوز استخدام نماذج وسجلات موحدة للإبلاغ عن الحوادث والتحقيق والمتابعة.

---

20. التوعية والتدريب

1. تقوم المؤسسة باعداد برامج لتوعية العاملين في المؤسسة حسب مواقعهم و برامج تدريب دورية لجميع الفئات ذات العلاقة.
2. تشمل التوعية موضوعات مثل:
    - السرية وأمن المعلومات
    - التصنيف
    - كلمات المرور
    - البريد الإلكتروني
    - الهندسة الاجتماعية
    - الحوادث والإبلاغ

- النسخ الاحتياطي
- حماية الوثائق والسجلات والأصول

3. توثق أنشطة التدريب والمشاركة فيها.

---

21. السجلات والتوثيق

يجب الاحتفاظ بالسجلات والنماذج ذات العلاقة، بما في ذلك عند الاقتضاء:

1. سجلات تصنيف المعلومات والأصول.
2. سجلات منح وحجب الصلاحيات.
3. سجلات الدخول إلى المواقع الحساسة.
4. سجلات النسخ الاحتياطي والاستعادة.
5. سجلات الحوادث الأمنية والسيبرانية.
6. تعهدات السرية وعدم الإفصاح.
7. سجلات الإتلاف.
8. سجلات التوعية والتدريب.
9. تقارير التدقيق والمتابعة.

22.مؤشرات القياس

تقاس فعالية تطبيق هذه السياسة من خلال مؤشرات مناسبة، مثل:

1. عدد الحوادث الأمنية والسيبرانية المبلغ عنها.
2. الوقت المستغرق لمعالجة الحوادث الأمنية والسيبرانية
3. نسبة الحوادث التي تمت معالجتها ضمن المدد المحددة.
4. نسبة مراجعة وتحديث الصلاحيات في مواعيدها.
5. نسبة الموظفين الذين أكملوا التوعية والتدريب.
6. نسبة نجاح اختبارات الاستعادة من النسخ الاحتياطي.
7. نسبة الامتثال لتصنيف المعلومات والأصول.
8. عدد حالات عدم الامتثال أو المخالفات المتعلقة بالسرية أو الوصول أو الاستخدام غير المصرح به.

---

23. المخالفات والإجراءات

يعد عدم الالتزام بهذه السياسة مخالفة تستوجب اتخاذ الإجراءات الإدارية أو القانونية أو التأديبية وفق التشريعات والسياسات والأنظمة والتعليمات النافذة.

---

24. الوثائق الداعمة

1. نموذج تعهد سرية المعلومات.
2. نموذج منح/تعديل/سحب الصلاحيات.
3. نموذج الإبلاغ عن حادث أمني/سيبراني.
4. سجل تصنيف الأصول والمعلومات.
5. سجل الدخول إلى المواقع الحساسة.
6. سجل الإتلاف الآمن للوثائق والبيانات.
7. سجل النسخ الاحتياطي والاستعادة.