﷽



**جامعة القدس المفتوحة**

**تقرير لمقرر ضبط أنظمة المعلومات و أمنها 1485**

**إعـــــــــــــــــداد :هديل فؤاد فاروق حرب**

**الرقم الجامعي:0123012110056**

**المشــــــــــــرف :أ.د.يوسف صالح يوسف أبو زر**

**المقدمة:**

في العصر الرقمي الحالي، تعتمد المطاعم بشكل متزايد على التكنولوجيا لإدارة عملياتها اليومية وتحقيق تواصل فعال مع العملاء. أصبحت الحلول الرقمية جزءاً أساسياً من نجاح الأعمال في قطاع المطاعم، سواء عبر أنظمة الحجوزات الإلكترونية، أو تطبيقات التوصيل، أو أنظمة الدفع الإلكترونية، أو إدارة المخزون. وعلى الرغم من هذه الفوائد، فإن هذا الاعتماد على التكنولوجيا يجعل المطاعم عرضة لمجموعة واسعة من المخاطر الأمنية التي تهدد سرية وسلامة وتوافر المعلومات الحساسة.

تشمل البيانات التي يحتفظ بها المطعم معلومات حساسة تتعلق بالزبائن، مثل الأسماء وأرقام الهواتف والعناوين، وكذلك تفاصيل المعاملات المالية التي تتطلب حماية صارمة. إضافة إلى ذلك، يمتلك المطعم معلومات سرية تتعلق بالوصفات، وتفاصيل المخزون، والبيانات التشغيلية التي يمكن أن تشكل ميزة تنافسية في السوق. هذه البيانات تُعتبر من الأصول التي يجب تأمينها ضد التهديدات الإلكترونية المتزايدة مثل الهجمات السيبرانية، البرمجيات الخبيثة، والتسريبات غير المقصودة.

يعد وضع سياسة شاملة لأمن المعلومات ضرورةً لضمان حماية هذه البيانات وضمان استمرار العمليات بأمان. سياسة أمن المعلومات تهدف إلى وضع إطار تنظيمي وتحديد إجراءات وقائية تمنع وتقلل من المخاطر، وتحافظ على ثقة العملاء وتعزز سمعة المطعم في السوق. كما تضمن السياسة أن الموظفين على دراية تامة بأهمية حماية المعلومات، وتوفر لهم التوجيهات اللازمة للتصرف بشكل صحيح عند التعامل مع البيانات الحساسة.

يهدف هذا التقرير إلى استعراض سياسة أمن المعلومات للمطاعم وتوضيح كيفية تطبيق هذه السياسة وفقاً للمراحل الستة الرئيسية، التي تشمل: التقييم التمهيدي، التوعية الإدارية، تحليل الاحتياجات، السياسات والإجراءات، التنفيذ والتطبيق، والصيانة. يركز التقرير على كل مرحلة بشكل مفصل، مع تقديم الخطوات الأساسية اللازمة لحماية المعلومات الحساسة وضمان إدارة فعالة وآمنة للعمليات في المطعم.

**1.التقييم التمهيدي:**

**1.1 تحديد الأصول المطلوب حمايتها**

يجب تحديد البيانات والأصول التي تحتاج إلى حماية، والتي تشمل:

* **بيانات الزبائن**: وتشمل الأسماء، عناوين الاتصال، ومعلومات الحجز، ومعلومات التوصيل.
* **المعاملات المالية**: بيانات الدفع الإلكتروني المرتبطة ببطاقات الائتمان، تفاصيل الفواتير، وسجلات الدفع.
* **النظم التقنية**: وتشمل نظام إدارة الطلبات، ونظام نقاط البيع (POS)، وأجهزة الكمبيوتر والخوادم المستخدمة لتخزين البيانات.
* **المخزون والوصفات**: معلومات حول المنتجات والمكونات المستخدمة، وهي ضرورية لحفظ السرية التنافسية.

**1.2 تحديد المخاطر المحتملة**

تشمل المخاطر التي قد تهدد أصول المطعم ما يلي:

* **الهجمات السيبرانية**: قد يستهدف المخترقون الأنظمة لجمع معلومات الزبائن أو التلاعب بالمعاملات المالية.
* **تسريب البيانات**: قد يؤدي الوصول غير المصرح به إلى أنظمة البيانات إلى كشف معلومات حساسة.
* **البرمجيات الخبيثة**: تشمل البرمجيات الضارة التي قد تهاجم النظام، مثل الفيروسات وبرمجيات الفدية.
* **فقدان البيانات**: سواء نتيجة لحادث سيبراني أو عطل فني، مما يؤدي إلى خسارة البيانات الهامة.

**1.3 تحديد وسائل الحماية**

يجب تحديد وسائل الحماية لضمان أمان الأصول، والتي قد تشمل:

* **التشفير**: لتأمين البيانات المخزنة والمنقولة، خاصة بيانات الدفع.
* **جدران الحماية**: لمنع الدخول غير المصرح به إلى الشبكات.
* **التحقق المتعدد العوامل**: لضمان أن جميع الأنظمة المالية وبيانات العملاء لا يمكن الوصول إليها إلا من قبل الأفراد المصرح لهم.

**1.4 الإجراءات عند حدوث خطر**

يجب إعداد خطط للتعامل مع الحوادث الأمنية تشمل:

* **خطة استجابة للحوادث**: يتم تدريب الموظفين على كيفية التعامل مع الحالات الطارئة من الهجمات أو تسريب البيانات.
* **الإبلاغ والتوثيق**: يشمل تقديم تقرير فوري للإدارة الأمنية والمساعدة في التحقيق حول الحادثة.
* **التواصل مع الأطراف الخارجية**: قد يشمل ذلك البنوك ومزودي الخدمة لإيقاف المعاملات غير الآمنة.

**2.التوعية الإدارية:**

تعتمد حماية المعلومات في المطاعم على وعي الموظفين وأهمية التزامهم بالإجراءات الأمنية:

1. **ورش العمل التدريبية**: تنظم برامج تدريبية مستمرة حول أهمية حماية البيانات، مع إرشادات حول كيفية التعامل الآمن مع الأنظمة.
2. **توزيع مواد توعوية**: كتيبات إرشادية وملصقات حول الأمان السيبراني وأفضل الممارسات للحفاظ على أمان المعلومات.
3. **رفع الوعي حول السياسات**: تعريف الموظفين بسياسة أمن المعلومات وتوضيح مسؤولياتهم تجاه أمن البيانات وخصوصية الزبائن.

**3. تحليل الإحتياجات:**

**3.1 تحديد الثغرات الأمنية**

في هذه المرحلة، يتم فحص الأنظمة والتطبيقات المستخدمة لتحديد أي ثغرات قد تُستغل، مثل:

* **الوصول غير المقيد**: بعض الموظفين قد يكون لديهم إمكانية الوصول إلى بيانات حساسة دون سبب مقنع.
* **عدم تحديث الأنظمة**: يمكن أن تؤدي البرمجيات القديمة إلى ثغرات أمنية كبيرة في النظام.
* **ضعف كلمات المرور**: قد يستخدم الموظفون كلمات مرور ضعيفة، مما يسهل من اختراق الأنظمة.

#### 3.2 تخصيص الموارد

بعد تحديد الثغرات، يتم تخصيص الموارد المتاحة لمعالجتها. يمكن أن يشمل ذلك:

* **تطوير الأمن التقني**: مثل تحديث الأجهزة والبرمجيات الأمنية.
* **تدريب الموظفين بشكل أوسع**: لضمان فهمهم لكيفية حماية المعلومات.
* **استثمار في بنية تحتية آمنة**: بما في ذلك أجهزة حماية الشبكة مثل جدران الحماية وأنظمة كشف التسلل

**4.السياسات و الإجراءات:**

**4.1 وضع السياسات الأمنية**

السياسات هي الإطار الذي يحكم جميع أنشطة حماية المعلومات في المطعم، وتغطي:

* **سياسة الخصوصية**: تحدد كيفية التعامل مع بيانات الزبائن وحمايتها.
* **سياسة الوصول**: تحديد من يمكنه الوصول إلى أنظمة المعلومات والبيانات الحساسة.
* **سياسة النسخ الاحتياطي**: لضمان حماية البيانات من الفقد عبر نسخ احتياطي دوري.

#### 4.2إجراءات التشغيل

الإجراءات هي الأنشطة العملية التي يجب على الموظفين اتباعها، وتتضمن:

1. **الإجراءات الخاصة بتسجيل الدخول والخروج من الأنظمة**: لضمان عدم الوصول غير المصرح به.
2. **تحديث كلمات المرور بانتظام**: للمساعدة في الحماية من اختراق الحسابات.
3. **إجراءات التعامل مع الدفع الإلكتروني**: لضمان حماية بيانات الدفع والحفاظ على أمان المعاملات.

**5. التنفيذ أو التطبيق:**

#### 5.1تنفيذ التدابير الأمنية

يتم تنفيذ التدابير الأمنية على الأنظمة والعمليات اليومية في المطعم، وتشمل:

* **تنصيب وتحديث برامج الأمان**: مثل برامج مكافحة الفيروسات، وبرامج اكتشاف التسلل.
* **التحكم في الوصول إلى البيانات**: عبر ضبط أذونات الوصول بناءً على الوظيفة.
* **اختبار الأنظمة**: من خلال محاكاة حوادث أمنية للتأكد من فعالية السياسات والإجراءات.

#### 5.2 مراقبة التزام الموظفين

يتم التأكد من أن جميع الموظفين يلتزمون بتطبيق السياسات، ويشمل ذلك مراقبة كيفية التعامل مع بيانات العملاء والتأكد من تطبيق إجراءات الأمان المحددة.

**6. الصيانة:**

**6.1 مراجعة دورية للسياسات**

تتطلب السياسة الأمنية مراجعة دورية للتأكد من توافقها مع أحدث التهديدات، بما في ذلك:

* **مراجعة السياسات**: تحديث السياسات لتتوافق مع التغيرات التقنية أو التنظيمية.
* **تحديث الأنظمة**: بما في ذلك البرمجيات والأجهزة التي تحتاج إلى تحديثات أمان دورية.

#### 6.2 اختبارات أمان النظام

يتضمن اختبار النظام إجراء مراجعات أمنية دورية لاكتشاف أي ثغرات محتملة ومعالجتها. يمكن أن تشمل الاختبارات اختبارات الاختراق أو عمليات فحص لنقاط الضعف.

#### 6.3 التدريب المستمر

يجب أن يتم تدريب الموظفين بشكل دوري حول السياسات والإجراءات الأمنية لضمان أنهم على دراية بآخر التحديثات في سياسة أمن المعلومات وأحدث الأساليب للتصدي للهجمات.

### الخاتمة

توفر سياسة أمن المعلومات للمطاعم أساساً لحماية البيانات والعمليات بشكل شامل، مما يساعد في الحفاظ على خصوصية العملاء وضمان استمرارية العمل. توضح المراحل الستة كيفية بناء سياسة أمان قوية وفعالة تلبي احتياجات المطعم وتضمن حماية البيانات والمعلومات من التهديدات المختلفة.