سياسة أمن المعلومات

المقدمة:

تلتزم شركة فيرست جارد للحراسات الأمنية بحماية معلوماتها ومعلومات عملائها وشركائها من أي تهديدات قد تؤثر على سريتها أو سلامتها أو توافرها. تهدف هذه السياسة إلى وضع الإرشادات والإجراءات اللازمة لضمان أمن المعلومات ودعم أهداف الشركة.

---

1 - الأهداف:

1. حماية بيانات الشركة من الوصول أو الكشف غير المصرح به.
2. ضمان سرية وسلامة وتوافر المعلومات.
3. الالتزام بالقوانين والمعايير الدولية ذات الصلة بأمن المعلومات.
4. رفع الوعي بين الموظفين حول أهمية أمن المعلومات.

---

1 - نطاق السياسة:

تُطبق هذه السياسة على:

- جميع المعلومات الإلكترونية والمطبوعة والشفهية الخاصة بالشركة.
- جميع الموظفين والشركاء والموردين الذين يتعاملون مع بيانات الشركة.

---

3 - المبادئ الأساسية:

أ. السرية:(Confidentiality)

- حماية المعلومات الحساسة من الوصول غير المصرح به.
- ضمان أن تكون البيانات متاحة فقط للأشخاص المصرح لهم.

ب. السلامة:(Integrity)

- ضمان دقة واكتمال البيانات.
- حماية البيانات من أي تعديل أو تدمير غير مصرح به.

ج. التوافر:(Availability)

- ضمان أن تكون المعلومات متاحة عند الحاجة للمستخدمين المصرح لهم.

---

4 - الالتزامات:

4.1 حماية البيانات:

- تطبيق التدابير التقنية والإدارية لحماية البيانات من التهديدات.
- استخدام تقنيات التشفير لحماية البيانات أثناء نقلها.

4.2 الوصول المصرح به:

- منح الوصول إلى المعلومات بناءً على مبدأ "الحاجة إلى المعرفة."
- مراجعة صلاحيات الوصول دوريًا.

4.3 التوعية والتدريب:

- تقديم دورات تدريبية دورية لجميع الموظفين حول:
  - حماية البيانات.
  - التعرف على التهديدات السيبرانية (مثل التصيد الإلكتروني).
  - الامتثال للسياسات والإجراءات.

4.4 أمن الجهات الخارجية:

- تقييم الموردين والشركاء لضمان التزامهم بمعايير أمن المعلومات.
- توقيع عقود تضمن التزام الجهات الخارجية بحماية البيانات.

4.5 الإبلاغ عن الحوادث:

- إنشاء نظام للإبلاغ الفوري عن أي حوادث تتعلق بأمن المعلومات.
- ضمان السرية وعدم الانتقام عند الإبلاغ.

---

5 - إجراءات أمن المعلومات :

5.1 إدارة المخاطر:

- تحديد وتقييم المخاطر المحتملة التي تهدد أمن المعلومات.
- وضع خطط لتخفيف هذه المخاطر.

5.2 إدارة الحوادث:

- تطبيق خطة استجابة للحوادث تتضمن:
  - تحديد الحوادث.
  - تقييم الأضرار.
  - اتخاذ الإجراءات التصحيحية.

5.3 حماية الأنظمة والشبكات:

- تطبيق جدران حماية لحماية الأنظمة من التهديدات الخارجية.
- استخدام برامج مكافحة الفيروسات وتحديثها بانتظام.

5.4 الاحتفاظ بالسجلات:

- وضع جدول زمني للاحتفاظ بالسجلات والمستندات الرقمية.
- التخلص الآمن من البيانات عند انتهاء صلاحيتها.

---

6 - مراجعة وتحديث السياسة:

- تتم مراجعة سياسة أمن المعلومات بشكل دوري (مرة واحدة على الأقل سنويًا) لضمان:
  - توافقها مع التغيرات في البيئة التشغيلية والقوانين.
  - تحسين الإجراءات بناءً على المراجعات والتقييمات.

---

7 - المسؤوليات:

7.1 فريق أمن المعلومات:

- تطوير وتطبيق سياسات وإجراءات أمن المعلومات.
- إدارة الحوادث الأمنية وضمان الاستجابة السريعة.

7.2 الموظفون:

- الالتزام بسياسات أمن المعلومات.
- الإبلاغ الفوري عن أي حوادث أو انتهاكات.

7.3 الإدارة العليا:

- دعم تطبيق سياسة أمن المعلومات وتوفير الموارد اللازمة.

---

8 - الامتثال:

- يُعتبر عدم الالتزام بسياسة أمن المعلومات انتهاكًا خطيرًا قد يؤدي إلى:
  - إجراءات تأديبية.
  - إنهاء التعاقد مع الجهات الخارجية المخالفة.

الخلاصة :

سياسة أمن المعلومات الخاصة بشركة فيرست جارد للحراسات الأمنية تضمن حماية المعلومات والبيانات الحساسة من التهديدات المحتملة مع تعزيز ثقافة الوعي الأمني داخل الشركة وخارجها.

شركة فيرست جارد للحراسات الأمنية