# نموذج اعتماد إطار توجيهي للأمن السيبراني

**بيانات المؤسسة:**

- **اسم الشركة/المؤسسة** .....
- **المقر الرئيسي** .....
- **النشاط التجاري** .....

**نص الإقرار والاعتماد:** إيمانًا منا في **(اسم الشركة)** بأن الأمن السيبراني هو ركيزة أساسية لحماية السيادة الرقمية والبيانات الحساسة، وضمان استمرارية أعمالنا في ظل التحول الرقمي الذي تشهده الدولة الليبية، فإننا نعلن بموجب هذا النموذج عن تبنينا الرسمي لـ **"الإطار التوجيهي للأمن السيبراني للمؤسسات الخاصة"** كمرجع إداري وفني لممارساتنا الرقمية.

**البنود المعتمدة:**

1. **تعيين المسؤولية :** تُعين **)اسم الشركة (** السيد/السيدة: ..... بصفته **مسؤولاً عن الأمن الرقمي (Cybersecurity Lead)**، وتوكل إليه مهام الإشراف على تنفيذ السياسات الأمنية، ومتابعة تحديث الأنظمة، ورفع تقارير دورية للإدارة حول المخاطر المحتملة.
2. **الالتزام بالوقاية:** نلتزم بتطبيق تدابير الحماية الأساسية، بما في ذلك تحديث البرمجيات دورياً، واستخدام أنظمة مكافحة الفيروسات، وتفعيل جدران الحماية، واعتماد سياسة "التحقق الثنائي" ( (2FA لجميع حسابات الموظفين الحساسة.
3. **سياسة النسخ الاحتياطي:** تقرر الشركة الالتزام بإجراء نسخ احتياطي دوري (أسبوعي على الأقل) لجميع البيانات الحيوية، وحفظ نسخة مشفرة خارج مقر المؤسسة أو عبر حلول سحابية آمنة لضمان استعادة البيانات في حالات الطوارئ.
4. **الاستجابة للحوادث:** نقر بالالتزام ببروتوكول الاستجابة للحوادث المذكور في الإطار التوجيهي، والذي يتضمن عزل الأجهزة المصابة فوراً، وإبلاغ الجهات المختصة في حال وقوع اختراق كبير يهدد بيانات العملاء أو الأمن الرقمي الوطني.
5. **نطاق التطبيق:** يسري هذا الاعتماد على جميع فروع الشركة، وموظفيها، والمقاولين المتعاملين مع أنظمتها الرقمية، ويُعتبر جزءاً لا يتجزأ من ثقافة العمل والالتزام المهني داخل المؤسسة.

**اعتماد الإدارة:**

- **اسم المدير العام** .....
- **التوقيع** .....
- **ختم الشركة:**
- **تاريخ الاعتماد**.... / .... / .....