الإطار التوجيهي للأمن السيبراني

للمؤسسات الخاصة والمشروعات المتناهية الصغر والصغرى والمتوسطة

(MSMEs)

المقدمة

يشهد العالم، وليبيا بصفة خاصة، توسعًا سريعًا في استخدام التقنيات الرقمية والخدمات الإلكترونية، مما يجعل الأمن السيبراني ركيزة أساسية لحماية السيادة الرقمية، والاقتصاد الوطني، والمؤسسات العامة والخاصة، وحقوق الأفراد. ومع تزايد التهديدات الرقمية، يهدف هذا الإطار إلى دعم المؤسسات والشركات في ليبيا لتعزيز مستوى أمنها السيبراني، ووضع أسس تنظيمية وتدابير وقائية تساعد على حماية الأنظمة الرقمية وتقليل المخاطر التشغيلية.

إن هذا الإطار لا يسعى فقط لحماية البيانات، بل يهدف إلى بناء إطار تشريعي وتنظيمي فعال يحكم الفضاء السيبراني، وتعزيز الثقة والتعاون بين القطاعين العام والخاص. ويمثل هذا العمل خطوة أولى نحو تطوير منظومة وطنية متكاملة للأمن السيبراني في الدولة الليبية، بما يضمن استمرارية الأعمال وحماية البنى التحتية الحيوية من أي أنشطة ضارة أو تخريبية

الأهداف الاستراتيجية للمؤسسة:

- بناء إطار تشريعي وتنظيمي داخلي فعال يحكم الفضاء السيبراني للمؤسسة.
- حماية البيانات والبنى التحتية الرقمية من مخاطر التدمير أو التجسس أو التخريب.
- تعزيز جاهزية المؤسسة لرصد ومنع والتجاوب مع التهديدات السيبرانية فور وقوعها.
- نشر ثقافة المسؤولية الجماعية بين كافة المستويات الإدارية والوظيفية.

الركائز الأساسية للامتثال (المستوى الإداري(

- **الحوكمة والمسؤولية:** تلتزم الإدارة بتعيين مسؤول عن أمن المعلومات (CISO) أو من ينوب عنه، ليكون المرجع الأول في تقييم المخاطر والإشراف على تنفيذ السياسات الأمنية.
- **إدارة الوصول والهوية:** يجب تطبيق مبدأ "الحد الأدنى من الصلاحيات"، بحيث لا يُمنح أي موظف حق الوصول إلا للبيانات والأنظمة الضرورية لأداء مهامه الوظيفية فقط، مع مراجعة هذه الصلاحيات بشكل دوري.

- **أمن الشبكات والأنظمة:** الالتزام بتثبيت جدران الحماية (Firewalls) وبرامج مكافحة الفيروسات الأصلية، مع ضمان تحديثها وتحديث أنظمة التشغيل فور صدور التنبيهات الأمنية لسد الثغرات.

- **سياسة النسخ الاحتياطي (Backup):** الالتزام بإجراء نسخ احتياطي دوري (أسبوعي كحد أدنى) للبيانات الحساسة، مع حفظ نسخة مشفرة في مكان منفصل جغرافياً أو سحابياً لضمان الاستعادة في حالات الكوارث.

- **التدريب المستمر:** تخصيص موارد لتدريب الموظفين ورفع وعيهم الأمني، باعتبار العنصر البشري هو الحلقة الأهم في منظومة الدفاع..

الامتثال والمسؤولية القانونية: تلتزم المؤسسة باللوائح الوطنية للأمن السيبراني. ويُعد الإهمال في تطبيق هذه التدابير مخالفة قد تعرض المؤسسة لغرامات مالية أو إيقاف مؤقت للترخيص من قبل الجهات المختصة، خاصة في حالات الإهمال التي تؤدي لتسريب بيانات المواطنين.