المركز الوطني للأمن السيبراني

قرار رقم (35/ 2023)

بشأن الإطار الوطني لحوكمة الأمن السيبراني

رئيس المركز الوطني للأمن السيبراني

– بعد الاطلاع على المرسوم رقم (37) لسنة 2022 الصادر بتاريخ 02/02/2022، بإنشاء المركز الوطني للأمن السيبراني،

– وعلى قرار مجلس الوزراء الموقر رقم (117) لسنة 2022، بتحديد الوزير المشرف على المركز الوطني للأمن السيبراني،

– وعلى قرار مجلس الوزراء الموقر رقم (1377) لسنة 2022، بتعيين رئيس المركز الوطني للأمن السيبراني،

– وبناء على ما تقتضيه مصلحة العمل.

المقدمة

عملاً بالمرسوم رقم 37 لسنة 2022 بشأن إنشاء المركز الوطني للأمن السيبراني يصدر المركز لائحة تختص بوضع الإطار الوطني العام لعمليات الأمن السيبراني والحوكمة وذلك لإحكام سير العمليات والاجراءات الإدارية وفق أطر تنظيمية فاعلة في سبيل تحقيق الأهداف الإستراتيجية للمركز.

النطاق

تنطبق هذه اللائحة على الجهات المعنية ذات الصلة باختصاصات المركز، والجهات الأخرى التي يحددها رئيس المركز وفقاً لأحكام المرسوم رقم 37 لسنة 2022.

مادة (1)

التعريفات والمصطلحات

(أ) اللجنة العليا: اللجنة الوطنية العليا المنشأة بموجب قرار مجلس الوزراء رقم 355 في اجتماعه (2019/11) بتاريخ 18/03/2019.

(ب) المركز: المركز الوطني للأمن السيبراني.

(ت) الجهات المعنية: الجهات الحكومية المدنية والعسكرية والأمنية ومؤسسات القطاع العام والخاص داخل دولة الكويت ذات الصلة باختصاصات المركز، والجهات الأخرى التي يحددها رئيس المركز وفقاً لأحكام المرسوم رقم 37 لسنة 2022، والتي تنقسم طبقاً لهذا الإطار لما يلي:

1. المرخِّص: هي الجهة التي تمتلك طبقاً للقانون حق الترخيص للأفراد أو الشركات وغيرهم بتقديم خدمة أو أكثر للمستفيد / للمستفيدين.
2. المرخَّص له أو مقدم الخدمة: الأفراد أو الشركات الذين يرخَّص لهم بتقديم خدمة أو أكثر للمستفيد / للمستفيدين.
3. الجهات العسكرية والأمنية: الجيش الكويتي، وزارة الداخلية، الحرس الوطني، وقوة الإطفاء.
4. الجهات الحيوية: هي الجهات المعنية التي تمتلك بيانات حساسة،

أو أنظمة، أو شبكات، أو منشآت تضمن الحفاظ على استمرار وظائف الدولة الأساسية أو المجتمع أو الاقتصاد، والتي يترتب في حال تعطلها أو تدميرها أو إتلافها الإضرار الجسيم بالأمن الوطني أو الأمن العام أو اقتصاد الدولة.

5. منظم قطاع مشغلي الخدمات الإلكترونية: هي الجهة التي تمتلك طبقاً للقوانين والنظم واللوائح حق التنظيم والإشراف على خطط وعمليات تنفيذ المشاريع الإلكترونية وحوكمتها.

6. مقدم الخدمة الإلكترونية العام: هي الجهات التابعة لمؤسسات الدولة وشركاتها، والتي لها حق تشغيل وتقديم الخدمات الإلكترونية.

7. الترخيص: الإذن الممنوح من المركز أو (المرخِّص) إلى الأفراد / الشركات للسماح لهم بتقديم خدمات وحلول امنيه في مجال الأمن السيبراني ومزاولة الأنشطة و العمليات ذات الصلة و وفقا لما يحدده المركز أو (المرخص).

مادة (2)

قواعد الحوكمة

(أ) اللجنة العليا:

1. اعتماد الاستراتيجيات الوطنية، والسياسات والمعايير المتعلقة بالأمن السيبراني.

2. اعتماد الخطة العامة لمواجهة المخاطر والتهديدات السيبرانية الوطنية.

3. رفع التقارير الدورية إلى مجلس الوزراء بتطورات الاستراتيجية.

(ب) المركز:

1. إصدار الاستراتيجيات الوطنية للأمن السيبراني، ومتابعة تنفيذها مع الجهات المعنية بعد اعتمادها من اللجنة الوطنية العليا.

2. الإشراف على إعداد وتنفيذ الخطط التشغيلية للجهات المعنية.

3. إصدار وتنفيذ الخطط التشغيلية للمركز.

4. إصدار وثيقة الإجراءات التي تنظم العلاقة بين الجهات المعنية لتحقيق الأهداف الوطنية.

5. إصدار وثيقة تصنيفات حوادث الأمن السيبراني الوطنية.

6. تصنيف مؤسسات الدولة حسب أثرها على الأمن الوطني وتحديد الجهات الحيوية.

7. إصدار اللوائح، والسياسات الوطنية العامة التي تعنى بالأمن السيبراني.

8. إصدار ضوابط ومعايير الأمن السيبراني الوطنية الأساسية، والإشراف على تنفيذها.

9. التقييم الدوري للمخاطر السيبرانية وقياس مستوى الجاهزية على المستوى الوطني ورفع التقارير الدورية بشأنها إلى مجلس الوزراء واللجنة العليا.

10. إصدار تعليمات وتوجيهات وارشادات مواجهة المخاطر والتهديدات السيبرانية الوطنية، والإشراف على تنفيذها.

11. إنشاء قاعدة بيانات بالتهديدات الإلكترونية بمشاركة الجهات المختصة.

12. إصدار التعليمات والتوجيهات والإرشادات الوطنية لتطوير عمليات الأمن السيبراني وفرق الاستجابة للحوادث، والإشراف على تنفيذها من قبل الجهات المعنية.

13. تقييم النواحي الأمنية لخدمات الحكومة الإلكترونية، والإشراف على تطويرها.

14. إصدار الدليل الوطني الخاص بإجراءات عمليات الأمن السيبراني.

15. إصدار الدليل الوطني الخاص بإجراءات الاستجابة لحوادث الأمن السيبراني.

16. إصدار وتنفيذ خطط وبرامج التدريب والتمارين والمسابقات السيبرانية السنوية على المستوى الوطني.

17. تنظيم سبل وآليات تبادل المعلومات والتقارير الأمنية على المستوى الوطني والدولي، والإشراف على تنفيذها.

18. إصدار دليل هياكل الوحدات التنظيمية الخاصة بعمليات الأمن السيبراني، والوظائف الخاصة بها.

19. إصدار دليل وظائف الأمن السيبراني وشروط ومعايير شغلها، ومسارات التأهيل والترقي الوظيفي.

20. إصدار دليل بناء القدرات الوطنية، والإشراف على تنفيذها.

21. إصدار الخطط الوطنية بشأن التوعية ونشر الثقافة السيبرانية، والإشراف على تنفيذها.

22. مراجعة واعتماد مقترحات اللوائح والسياسات الخاصة بالجهات المعنية والفرق التخصصية.

23. رفع التقارير الدورية بشأن الوضع الأمني السيبراني العام للدولة إلى مجلس الوزراء واللجنة العليا.

24. تنظيم عمل مقدمي خدمات الأمن السيبراني.

25. وضع الشروط والمواصفات الفنية لأي أجهزة أو أنظمة في مجال الأمن السيبراني، والموافقة على استعمالها أو استيرادها أو تداولها في الدولة، وإصدار التعليمات المنظمة لها.

26. القيام بأي واجب يكلف به المركز من مجلس الوزراء أو من اللجنة العليا.

(ت) الجهات العسكرية والأمنية:

1. تعيين/إنشاء جهة إدارية متخصصة في مجال حوكمة الأمن السيبراني ضمن الهيكل التنظيمي للجهة باعتبارها جهة تنسيق مباشرة مع المركز ومنظم لأعمالها داخلياً.

2. إعداد الخطة التشغيلية الخاصة بها بناءً على الاستراتيجية الوطنية الخاصة بالأمن السيبراني، والعمل على تنفيذها تحت إشراف المركز، ورفع التقارير الدورية والتوصيات بشأنها إلى المركز.

3. تنفيذ ضوابط ومعايير الأمن السيبراني الوطنية الأساسية الصادرة من المركز، ورفع التقارير الدورية والتوصيات بشأنها إلى المركز.
4. إصدار وتحديث اللوائح، والسياسات الخاصة بها، والعمل على تنفيذها بعد اعتمادها من المركز.
5. التقييم الدوري للمخاطر السيبرانية وقياس مستوى الجاهزية الخاصة بها، ورفع التقارير الدورية والتوصيات بشأنها إلى المركز.
6. إعداد وتنفيذ الضوابط والخطط الخاصة بمواجهة المخاطر والتهديدات السيبرانية.
7. تطوير عمليات الأمن السيبراني وفرق الاستجابة لحوادث الأمن السيبراني الخاصة بها.
8. إصدار وتحديث الإجراءات الخاصة بعمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة بها.
9. المشاركة بخطة التدريب والتمارين والمسابقات الصادرة من المركز.
10. وضع وتنفيذ خطة التدريب والتمارين والمسابقات الخاصة بها.
11. إعداد وتنفيذ خطته الخاصة ببناء القدرات.
12. المحافظة على أمنها السيبراني بما لا يتعارض مع اختصاصات المركز، مع تمكين المركز من مباشرة اختصاصاته، والالتزام بتنفيذ واتباع كل ما يصدر منه.
13. اخطار المركز بشكل فوري بأي خطر، أو تهديد، أو اختراق واقع ،أو محتمل.
14. تبادل المعلومات والتقارير الأمنية مع المركز.
15. المساهمة في إنشاء قاعدة بيانات بالتهديدات الإلكترونية الخاصة بالمركز وإدامتها.
16. إعداد وتنفيذ الخطط الخاصة بها بشأن التوعية ونشر الثقافة السيبرانية.
17. الالتزام بتزويد الجهة الإدارية المتخصصة في مجال حوكمة الأمن السيبراني بما تحتاجه من الوثائق والمعلومات والبيانات والتقارير اللازمة للقيام باختصاصاتها، وتمكينها من فحص (أو ربط إن تطلب الأمر) الأجهزة والشبكات والنظم والبرمجيات الخاصة بالجهات التابعة لها، مع التزام الجهة الإدارية المتخصصة في مجال حوكمة الأمن السيبراني بتزويد وتمكين المركز بذلك.
18. أخذ موافقة المركز قبل حفظ أي بيانات حساسة أو معالجتها خارج دولة الكويت، وفقاً للوائح والضوابط والإجراءات المنظمة والصادرة من قبل الجهة الإدارية المتخصصة في مجال حوكمة الأمن السيبراني.
19. رفع التقارير الدورية بشأن الوضع الأمني السيبراني إلى المركز.
20. رفع المقترحات والتوصيات المتعلقة بالأمن السيبراني إلى المركز.
21. القيام بأي واجب يكلف به من المركز.

(ث) المرخِّص

1. تعيين / إنشاء جهة إدارية متخصصة في مجال حوكمة الأمن السيبراني باعتبارها جهة تنسيق مباشرة للعمل مع المركز.
2. إعداد الخطة التشغيلية الخاصة بها بناءً على الاستراتيجية الوطنية، والعمل على تنفيذها تحت إشراف المركز، ورفع التقارير الدورية والتوصيات بشأنها إلى المركز.
3. تنفيذ المرخِّص والجهات الخاضعة له ضوابط ومعايير الأمن السيبراني الوطنية الأساسية الصادرة من المركز، ورفع التقارير الدورية والتوصيات بشأنها إلى المركز.
4. إصدار وتحديث اللوائح، والسياسات الخاصة بالمرخِّص والجهات الخاضعة له، والعمل على تنفيذها بعد اعتمادها من المركز.
5. التقييم الدوري للمخاطر السيبرانية وقياس مستوى الجاهزية الخاصة بالمرخِّص والجهات الخاضعة له، ورفع التقارير الدورية والتوصيات بشأنها إلى المركز.
6. إعداد وتنفيذ الضوابط والخطط الخاصة بمواجهة المخاطر والتهديدات السيبرانية.
7. تطوير عمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة بالمرخِّص والجهات الخاضعة له.
8. إصدار وتحديث الإجراءات الخاصة بعمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة بالمرخِّص والجهات الخاضعة له.
9. المشاركة بخطة التدريب والتمارين والمسابقات الصادرة من المركز.
10. وضع وتنفيذ خطة التدريب والتمارين والمسابقات الخاصة بالمرخِّص والجهات الخاضعة له.
11. إعداد وتنفيذ خطة بناء القدرات الخاصة بالمرخِّص، والإشراف على تنفيذ خطة الجهات الخاضعة له.
12. المحافظة على أمن المرخِّص السيبراني والجهات الخاضعة لها بما لا يتعارض مع اختصاصات المركز، مع تمكين المركز من مباشرة اختصاصاته، والالتزام بتنفيذ واتباع كل ما يصدر منه.
13. اخطار المركز بشكل فوري بأي خطر، أو تهديد، أو اختراق واقع ،أو محتمل.
14. تبادل المعلومات والتقارير الأمنية بين المرخِّص والمركز.
15. المساهمة في إنشاء قاعدة بيانات بالتهديدات الإلكترونية الخاصة بالمركز وإدامتها.
16. إعداد وتنفيذ الخطط الخاصة بالمرخِّص بشأن التوعية ونشر الثقافة السيبرانية.
17. الإشراف على تنفيذ الخطط الخاصة بالجهات الخاضعة له بشأن التوعية ونشر الثقافة السيبرانية.
18. التزام الجهات الخاضعة بتزويد المرخِّص بالوثائق والمعلومات والبيانات والتقارير اللازمة للقيام باختصاصاته، وتمكينه من فحص (أو ربط إن تطلب الأمر) الأجهزة والشبكات والنظم والبرمجيات الخاصة بالجهات الخاضعة له، مع التزام المرخِّص بتزويد وتمكين المركز بذلك.

19. أخذ موافقة المركز قبل حفظ أي بيانات حساسة أو معالجتها خارج دولة الكويت، وفقاً للوائح والضوابط والإجراءات المنظمة والصادرة من قبل المرخّص.
20. رفع التقارير الدورية بشأن الوضع الأمني السيبراني للمرخّص والجهات الخاضعة له إلى المركز.
21. رفع المقترحات والتوصيات المتعلقة بالأمن السيبراني للمرخّص والجهات الخاضعة له إلى المركز.
22. القيام بأي واجب يكلف به من المركز.

(ج) المرخَّص له أو مقدم الخدمة:

1. تعيين / إنشاء جهة إدارية متخصصة في مجال حوكمة الأمن السيبراني باعتبارها جهة تنسيق مباشرة للعمل مع المرخّص.
2. إعداد الخطة التشغيلية الخاصة بها بناءً على الاستراتيجية الوطنية واستراتيجية المرخّص، والعمل على تنفيذها تحت إشراف المرخّص.
3. تنفيذ ضوابط ومعايير الأمن السيبراني الوطنية الأساسية الصادرة من المرخّص، ورفع التقارير الدورية والتوصيات بشأنها إلى المرخّص.
4. تنفيذ اللوائح، والسياسات الصادرة من المرخّص.
5. التقييم الدوري للمخاطر السيبرانية وقياس مستوى الجاهزية الخاصة به ورفع التقارير الدورية والاجراءات التي تمت بشأنها إلى المرخّص.
6. إعداد وتنفيذ الضوابط والخطط الخاصة بمواجهة المخاطر والتهديدات السيبرانية تحت إشراف المرخّص.
7. تطوير عمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة به تحت إشراف المرخّص.
8. إصدار وتحديث الإجراءات الخاصة بعمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة به تحت إشراف المرخّص.
9. المشاركة بخطة التدريب والتمارين والمسابقات الصادرة من المرخّص.
10. وضع وتنفيذ خطة التدريب والتمارين والمسابقات الخاصة به تحت إشراف المرخّص.
11. إعداد وتنفيذ خطته الخاصة ببناء القدرات بإشراف المرخّص.
12. المحافظة على أمنه السيبراني بما لا يتعارض مع اختصاصات المرخّص، مع تمكين المرخّص والمركز من مباشرة اختصاصاتها، والالتزام بتنفيذ واتباع كل ما يصدر منهما.
13. اخطار المرخّص بشكل فوري بأي خطر، أو تهديد، أو اختراق واقع ،أو محتمل.
14. تبادل المعلومات والتقارير الأمنية مع المرخّص.
15. إعداد وتنفيذ خطط التوعية ونشر الثقافة السيبرانية.
16. الالتزام بتزويد المرخّص بالوثائق والمعلومات والبيانات والتقارير اللازمة للقيام باختصاصاته، وتمكينه من فحص (أو ربط إن تطلب الأمر) الأجهزة والشبكات والنظم والبرمجيات الخاصة به، مع التزام المرخّص بتزويد وتمكين المركز بذلك.
17. أخذ موافقة المركز قبل حفظ أي بيانات حساسة أو معالجتها خارج دولة الكويت، وفقاً للوائح والضوابط والإجراءات المنظمة والصادرة من قبل المرخّص.
18. رفع التقارير الدورية بشأن الوضع الأمني السيبراني بها إلى المرخّص.
19. رفع المقترحات والتوصيات المتعلقة بالأمن السيبراني بها إلى المرخّص.
20. القيام بأي واجب يكلف به من المرخّص.

(ح) منظم قطاع مشغلي الخدمات الإلكترونية:

1. تعيين / إنشاء جهة إدارية متخصصة في مجال حوكمة الأمن السيبراني باعتبارها جهة تنسيق مباشرة للعمل مع المركز.
2. إعداد الخطة التشغيلية الخاصة بها بناءً على الاستراتيجية الوطنية، والعمل على تنفيذها تحت إشراف المركز، ورفع التقارير الدورية والتوصيات بشأنها إلى المركز.
3. تنفيذ منظم القطاع ومشغلي الخدمات الإلكترونية ضوابط ومعايير الأمن السيبراني الوطنية الأساسية الصادرة من المركز، ورفع التقارير الدورية والتوصيات بشأنها إلى المركز.
4. إصدار وتحديث اللوائح، والسياسات الخاصة بمنظم القطاع ومشغلي الخدمات الإلكترونية، والعمل على تنفيذها بعد اعتمادها من المركز.
5. التقييم الدوري للمخاطر السيبرانية وقياس مستوى الجاهزية الخاصة بمنظم القطاع ومشغلي الخدمات الإلكترونية، ورفع التقارير الدورية والتوصيات بشأنها إلى المركز.
6. إعداد وتنفيذ الضوابط والخطط الخاصة بمواجهة المخاطر والتهديدات السيبرانية.
7. تطوير عمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة بمنظم القطاع ومشغلي الخدمات الإلكترونية.
8. إصدار وتحديث الإجراءات الخاصة بعمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة بمنظم القطاع ومشغلي الخدمات الإلكترونية.
9. المشاركة بخطة التدريب والتمارين والمسابقات الصادرة من المركز.
10. وضع وتنفيذ خطة التدريب والتمارين والمسابقات الخاصة بمنظم القطاع ومشغلي الخدمات الإلكترونية.
11. إعداد وتنفيذ خطة منظم القطاع ببناء القدرات الخاصة بها.
12. إعداد وتنفيذ خطة بناء القدرات الخاصة بمنظم القطاع، والإشراف على تنفيذ خطة مشغلي الخدمات الإلكترونية.
13. المحافظة على أمن منظم القطاع السيبراني ومشغلي الخدمات الإلكترونية بما لا يتعارض مع اختصاصات المركز، مع تمكين المركز من

مباشرة اختصاصاته، والالتزام بتنفيذ واتباع كل ما يصدر منه.

14. اخطار المركز بشكل فوري بأي خطر، أو تهديد، أو اختراق واقع ،او محتمل.

15. تبادل المعلومات والتقارير الأمنية بين منظم القطاع والمركز.

16. المساهمة في إنشاء قاعدة بيانات بالتهديدات الإلكترونية الخاصة بالمركز وإدامتها.

17. إعداد وتنفيذ الخطط الخاصة بمنظم القطاع بشأن التوعية ونشر الثقافة السيبرانية.

18. الإشراف على تنفيذ الخطط الخاصة بمشغلي الخدمات الإلكترونية بشأن التوعية ونشر الثقافة السيبرانية.

19. التزام مشغلي الخدمات الإلكترونية بتزويد منظم القطاع بالوثائق والمعلومات والبيانات والتقارير اللازمة للقيام باختصاصاته، وتمكينه من فحص (أو ربط إن تطلب الأمر) الأجهزة والشبكات والنظم والبرمجيات الخاصة بمشغلي الخدمات الإلكترونية، مع التزام منظم القطاع بتزويد وتمكين المركز بذلك.

20. أخذ موافقة المركز قبل حفظ أي بيانات حساسة أو معالجتها خارج دولة الكويت، وفقاً للوائح والضوابط والإجراءات المنظمة والصادرة من قبل منظم القطاع.

21. رفع التقارير الدورية بشأن الوضع الأمني السيبراني لمنظم القطاع ومشغلي الخدمات الإلكترونية إلى المركز.

22. رفع المقترحات والتوصيات المتعلقة بالأمن السيبراني لمنظم القطاع ومشغلي الخدمات الإلكترونية إلى المركز.

23. القيام بأي واجب يكلف به من المركز.

(خ) مقدم الخدمة الإلكترونية العام:

1. تعيين / إنشاء جهة إدارية متخصصة في مجال حوكمة الأمن السيبراني باعتبارها جهة تنسيق مباشرة للعمل مع منظم قطاع مشغلي الخدمات الإلكترونية.

2. إعداد الخطة التشغيلية الخاصة به بناءً على الاستراتيجية الوطنية واستراتيجية منظم قطاع مشغلي الخدمات الإلكترونية، والعمل على تنفيذها تحت إشراف منظم قطاع مشغلي الخدمات الإلكترونية.

3. تنفيذ ضوابط ومعايير الأمن السيبراني الوطنية الأساسية الصادرة من منظم قطاع مشغلي الخدمات الإلكترونية، ورفع التقارير الدورية والتوصيات بشأنها إلى منظم قطاع مشغلي الخدمات الإلكترونية.

4. تنفيذ اللوائح، والسياسات الصادرة من منظم قطاع مشغلي الخدمات الإلكترونية.

5. التقييم الدوري للمخاطر السيبرانية وقياس مستوى الجاهزية الخاصة به ورفع التقارير الدورية والاجراءات التي تمت بشأنها الى منظم قطاع مشغلي الخدمات الإلكترونية.

6. إعداد وتنفيذ الضوابط والخطط الخاصة بمواجهة المخاطر والتهديدات السيبرانية تحت إشراف منظم قطاع مشغلي الخدمات الإلكترونية.

7. تطوير عمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة به تحت إشراف منظم قطاع مشغلي الخدمات الإلكترونية.

8. إصدار وتحديث الإجراءات الخاصة بعمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة به تحت إشراف منظم قطاع مشغلي الخدمات الإلكترونية.

9. المشاركة بخطة التدريب والتمارين والمسابقات الصادرة من منظم قطاع مشغلي الخدمات الإلكترونية.

10. وضع وتنفيذ خطة التدريب والتمارين والمسابقات الخاصة به تحت إشراف منظم قطاع مشغلي الخدمات الإلكترونية.

11. إعداد وتنفيذ خطته الخاصة ببناء القدرات بإشراف منظم قطاع مشغلي الخدمات الإلكترونية.

12. المحافظة على أمنه السيبراني بما لا يتعارض مع اختصاصات منظم قطاع مشغلي الخدمات الإلكترونية، مع تمكين منظم قطاع مشغلي الخدمات الإلكترونية والمركز من مباشرة اختصاصاتهما، والالتزام بتنفيذ واتباع كل ما يصدر منهما.

13. اخطار منظم قطاع مشغلي الخدمات الإلكترونية بشكل فوري بأي خطر، أو تهديد، أو اختراق واقع، أو محتمل.

14. تبادل المعلومات والتقارير الأمنية مع منظم قطاع مشغلي الخدمات الإلكترونية.

15. إعداد وتنفيذ خطط التوعية ونشر الثقافة السيبرانية.

16. الالتزام بتزويد منظم قطاع مشغلي الخدمات الإلكترونية بالوثائق والمعلومات والبيانات والتقارير اللازمة للقيام باختصاصاته، وتمكينه من فحص (أو ربط إن تطلب الأمر) الأجهزة والشبكات والنظم والبرمجيات الخاصة به، مع التزام منظم قطاع مشغلي الخدمات الإلكترونية بتزويد وتمكين المركز بذلك.

17. أخذ موافقة المركز قبل حفظ أي بيانات حساسة أو معالجتها خارج دولة الكويت، وفقاً للوائح والضوابط والإجراءات المنظمة والصادرة من قبل منظم قطاع مشغلي الخدمات الإلكترونية.

18. رفع التقارير الدورية بشأن الوضع الأمني السيبراني به إلى منظم قطاع مشغلي الخدمات الإلكترونية.

19. رفع المقترحات والتوصيات المتعلقة بالأمن السيبراني به إلى منظم قطاع مشغلي الخدمات الإلكترونية.

20. القيام بأي واجب يكلف به من منظم قطاع مشغلي الخدمات الإلكترونية.

(د) الجهات الحيوية:

1. تعيين / إنشاء جهة إدارية متخصصة في مجال حوكمة الأمن السيبراني ضمن الهيكل التنظيمي للجهة باعتبارها جهة تنسيق مباشرة

مع المركز ومنظم لأعمالها داخلياً.

2. إعداد الخطة التشغيلية الخاصة بها بناءً على الاستراتيجية الوطنية، والعمل على تنفيذها تحت إشراف المركز، ورفع التقارير الدورية والتوصيات بشأنها إلى المركز.

3. تنفيذ ضوابط ومعايير الأمن السيبراني الوطنية الأساسية الصادرة من المركز، ورفع التقارير الدورية والتوصيات بشأنها إلى المركز.

4. إصدار وتحديث اللوائح، والسياسات الخاصة بها، والعمل على تنفيذها بعد اعتمادها من المركز.

5. التقييم الدوري للمخاطر السيبرانية وقياس مستوى الجاهزية الخاصة بها، ورفع التقارير الدورية والتوصيات بشأنها إلى المركز.

6. إعداد وتنفيذ الضوابط والخطط الخاصة بمواجهة المخاطر والتهديدات السيبرانية.

7. تطوير عمليات الأمن السيبراني وفرق الاستجابة لحوادث الأمن السيبراني الخاصة بها.

8. إصدار وتحديث الإجراءات الخاصة بعمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة بها.

9. المشاركة بخطة التدريب والتمارين والمسابقات الصادرة من المركز.

10. وضع وتنفيذ خطة التدريب والتمارين والمسابقات الخاصة بها.

11. اعداد وتنفيذ خطته الخاصة ببناء القدرات.

12. المحافظة على أمنها السيبراني بما لا يتعارض مع اختصاصات المركز، مع تمكين المركز من مباشرة اختصاصاته، والالتزام بتنفيذ واتباع كل ما يصدر منه.

13. اخطار المركز بشكل فوري بأي خطر أو تهديد أو اختراق واقع او محتمل.

14. تبادل المعلومات والتقارير الأمنية مع المركز.

15. المساهمة في إنشاء قاعدة بيانات بالتهديدات الإلكترونية الخاصة بالمركز وإدامتها.

16. إعداد وتنفيذ الخطط الخاصة بها بشأن التوعية ونشر الثقافة السيبرانية.

17. الالتزام بتزويد الجهة الإدارية المتخصصة في مجال حوكمة الأمن السيبراني بما تحتاجه من الوثائق والمعلومات والبيانات والتقارير اللازمة للقيام باختصاصاتها، وتمكينها من فحص (أو ربط إن تطلب الأمر) الأجهزة والشبكات والنظم والبرمجيات الخاصة بالجهات التابعة لها، مع التزام الجهة الإدارية المتخصصة في مجال حوكمة الأمن السيبراني بتزويد وتمكين المركز بذلك.

18. أخذ موافقة المركز قبل حفظ أي بيانات حساسة أو معالجتها خارج دولة الكويت، وفقاً للوائح والضوابط والإجراءات المنظمة والصادرة من قبل الجهة الإدارية المتخصصة في مجال حوكمة الأمن السيبراني.

19. رفع التقارير الدورية بشأن الوضع الأمني السيبراني إلى المركز.

20. رفع المقترحات والتوصيات المتعلقة بالأمن السيبراني إلى المركز.

21. القيام بأي واجب يكلف به من المركز.

(ذ) مقدم خدمة أمن سيبراني:

1. الالتزام بالتسجيل لدى المركز بالسجل الخاص باستيفاء المعايير الأمنية الصادرة من المركز.

2. الالتزام باستيفاء كافة الاشتراطات والضوابط الأساسية والمكملة والمعدلة لها بشأن منح التراخيص الصادرة من الجهات المعنية في الدولة كل حسب الاختصاصات المقررة لكل منها وفقاً للقوانين والنظم واللوائح، وفي حدود الإطار العام للاشتراطات والضوابط الصادرة من المركز.

3. الالتزام بالمحافظة على استيفاء كافة الاشتراطات والضوابط الأساسية والمكملة والمعدلة لها المقررة لمنح الترخيص طوال فترة تقديم الخدمة، مع الالتزام بالإخطار الفوري للجهة المعنية المانحة للترخيص في حال فقد أحد الاشتراطات أو الضوابط.

مادة (3)

فرق العمل التخصصية

يشكل المركز عدد من فرق العمل التخصصية حسب ما تقتضيه الحاجة لتمكينه من القيام باختصاصاته، وفيما لا يتعارض مع المسئوليات الواردة في هذه اللائحة المناطة بالجهات المعنية.

مادة (4)

الإنفاذ

تعتبر لائحة الإطار الوطني لعمليات الأمن السيبراني والحوكمة ملزمة على كافة الجهات المعنية والعاملين فيها، وتلتزم الجهات المعنية بفرض ما يلزم حسب مسئولياتها الخاصة بها وبما لا يتعارض مع أحكامها.

مادة (5)

التعديلات

يجوز للمركز تعديل هذه اللائحة متى كان لذلك مقتضى بناءً على ما تقضيه المصلحة العامة.

مادة (6)

تاريخ النفاذ

على الجهات المختصة تنفيذ هذا القرار كل فيما يخصه ويعمل به اعتباراً من تاريخ صدوره ونشره في الجريدة الرسمية.

رئيس المركز الوطني للأمن السيبراني

محمد عبدالعزيز بوعركي

صدر في: 16 أغسطس 2023 م