الصباح AL-SABAH
www.alsabahpress.com Alsabah Media
No. 4652 | الأحد | 4 صفر 1445 هـ | 20 أغسطس 2023 م | السنة السادسة عشرة

اللائحة ملزمة لجميع الجهات المعنية والعاملين ..وتعديلها وفق المصلحة العامة

الإطار الوطني لحوكمة «الأمن السيبراني»: آليات لمواجهة المخاطر وتقييمها دوريا

تصميم قاعدة بيانات بالتهديدات الإلكترونية بمشاركة الجهات المختصة

لا بد من استحداث إدارة تتبع الجهات العسكرية للتنسيق المباشر مع المركز

أصدر رئيس المركز الوطني للأمن السيبراني محمد بوعركي قرارا بشأن الإطار الوطني لحوكمة الأمن السيبراني، وذلك لإحكام سير العمليات والإجراءات الإدارية وفق أطر تنظيمية فاعلة لتحقيق الأهداف الاستراتيجية للمركز.

وجاء في القرار: عملا 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 والإجراءات الادارية وفق أطر تنظيمية فاعلة في سبيل تحقيق الأهداف الاستراتيجية للمركز.

وتنطبق هذه اللائحة على الجهات المعنية ذات الصلة باختصاصات المركز، والجهات الأخرى التي يحددها رئيس المركز وفقا 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 2019/3/18.

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 وفقا لأحكام المرسوم رقم 37 لسنة 2022، والتي تنقسم طبقا لهذا الإطار لما يلي:

1 – المرخِّص: هي الجهة التي تملك طِبقا للقانون حق الترخيص للأفراد أو الشركات وغيرهم بتقديم خدمة أو أكثر للمستفيد/ للمستفيدين.

2 – المرخص له أو مقدم الخدمة: الأفراد أو الشركات الذين يرخص لهم بتقديم خدمة أو أكثر للمستفيد/ للمستفيدين.

3 – الجهات العسكرية والأمنية: الجيش الكويتي، وزارة الداخلية، الحرس الوطني، وقوة الاطفاء.

4 – الجهات الحيوية: هي الجهات المعنية التي تمتلك بيانات حساسة، أو أنظمة، أو شبكات، أو منشآت تضمن الحفاظ على استمرار وظائف الدولة الاساسية أو المجتمع أو الاقتصاد، والتي يترتب في حال تعطلها أو تدميرها أو إتلافها الاضرار الجسيم بالأمن الوطني أو الأمن العام أو اقتصاد الدولة.

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

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

7 – الترخيص: الإذن الممنوح من المركز أو (المرخص) الى الافراد/ الشركات للسماح لهم بتقديم خدمات وحلول أمنية في مجال الأمن السيبراني ومزاولة الأنشطة والعمليات ذات الصلة ووفقا لما يحدده المركز أو (المرخص).

مادة 2:

قواعد الحوكمة:

* اللجنة العليا:

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

2 – اعتماد الخطة العامة لمواجهة المخاطر والتهديدات السيبرانية الوطنية.

3 – رفع التقارير الدورية الى مجلس الوزراء بتطورات الاستراتيجية.

* 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 الى مجلس الوزراء واللجنة العليا.

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

11 – إنشاء قاعدة بيانات بالتهديدات الالكترونية بمشاركة الجهات المختصة.

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

13 – تقييم النواحي الامنية لخدمات الحكومية الالكترونية، والإشراف على تطويرها.

14 – إصدار الدليل الوطني الخاص بإجراءات عمليات الامن السيبراني.

15 – إصدار الدليل الوطني الخاص بإجراءات الاستجابة لحوادث الامن السيبراني.

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

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

18 – إصدار دليل هياكل الوحدات التنظيمية الخاصة بعمليات الامن 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 الامني السيبراني العام للدولة الى مجلس الوزراء واللجنة العليا.

24 – تنظيم عمل مقدمي خدمات الامن السيبراني.

25 – وضع الشروط والمواصفات الفنية لأي جهات أو أنظمة في مجال الامن 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.

* الجهات العسكرية والأمنية:

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

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

3 – تنفيذ ضوابط ومعايير الأمن السيبراني الوطنية الاساسية الصادرة من منظم قطاع مشغلي الخدمات الالكترونية، ورفع التقارير الدورية والتوصيات بشأنها الى المركز.

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

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

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

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

8 – إصدار وتحديث الإجراءات الخاصة بعمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة بمنظم القطاع ومشغلي الخدمات الالكترونية.

9 – المشاركة بخطة التدريب والتمارين والمسابقات الصادرة من المركز.

10 – وضع وتنفيذ خطة التدريب والتمارين والمسابقات الخاصة بمنظم القطاع ومشغلي الخدمات الالكترونية.

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 الالكترونية.

13 – المحافظة على أمن منظم القطاع السيبراني ومشغلي الخدمات الالكترونية بما لا يتعارض مع اختصاصات المركز، مع تمكين المركز من مباشرة اختصاصاته، والالتزام بتنفيذ واتباع كل ما يصدر منه.

14 – إخطار المركز بشكل فوري بأي خطر، أو تهديد، أو اختراق واقع، أو محتمل.

15 – تبادل المعلومات والتقارير الامنية بين منظم القطاع والمركز.

16 – المساهمة في إنشاء قاعدة بيانات بالتهديدات الالكترونية الخاصة بالمركز وإدامتها.

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

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

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

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

21 – رفع المقترحات والتوصيات المتعلقة بالأمن السيبراني لمنظم القطاع ومشغلي الخدمات الالكترونية الى المركز.

22 – رفع المقترحات والتوصيات المتعلقة بالأمن السيبراني لمنظم القطاع ومشغلي الخدمات الالكترونية الى المركز.

23 – القيام بأي واجب يكلف به من المركز.

مهام 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 الالكترونية.

2 – إعداد الخطة التشغيلية الخاصة به بناء على الاستراتيجية الوطنية واستراتيجية منظم قطاع مشغلي الخدمات الالكترونية، والعمل على تنفيذها تحت إشراف المركز.

3 – تنفيذ ضوابط ومعايير الأمن السيبراني الوطنية الاساسية الصادرة من المركز، ورفع التقارير الدورية والتوصيات بشأنها الى المركز.

4 – إصدار وتحديث اللوائح، والسياسات الخاصة بمنظم القطاع ومشغلي الخدمات الالكترونية، والعمل على تنفيذها بعد اعتمادها من المركز.

5 – التقييم الدوري للمخاطر السيبرانية وقياس مستوى الجاهزية الخاصة بمنظم القطاع ومشغلي الخدمات الالكترونية، ورفع التقارير الدورية والتوصيات بشأنها الى المركز.

6 – إعداد وتنفيذ خطة بناء القدرات الخاصة بمنظم القطاع ومشغلي الخدمات الالكترونية.

7 – تطوير عمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة بمنظم القطاع ومشغلي الخدمات الالكترونية.

8 – إصدار وتحديث الإجراءات الخاصة بعمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة بمنظم القطاع ومشغلي الخدمات الالكترونية.

9 – المشاركة بخطة التدريب والتمارين والمسابقات الصادرة من المركز.

10 – وضع وتنفيذ خطة التدريب والتمارين والمسابقات الخاصة بمنظم القطاع ومشغلي الخدمات الالكترونية.

11 – إعداد وتنفيذ خطته الخاصة ببناء القدرات بإشراف المركز.

12 – المحافظة على أمنه السيبراني بما لا يتعارض مع اختصاصاته، والالتزام بتنفيذ واتباع كل ما يصدر منه.

13 – إخطار المركز بشكل فوري بأي خطر، أو تهديد، أو اختراق واقع، أو محتمل.

14 – تبادل المعلومات والتقارير الامنية مع منظم قطاع مشغلي الخدمات الالكترونية.

15 – إعداد وتنفيذ خطط التوعية ونشر الثقافة السيبرانية.

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

17 – أخذ موافقة المركز قبل حفظ أي بيانات حساسة أو معالجتها خارج دولة الكويت، وفقا للوائح والضوابط والإجراءات المنظمة والصادرة من قبل المركز.

18 – رفع التقارير الدورية بشأن الوضع الامني السيبراني الى المركز.

19 – رفع المقترحات والتوصيات المتعلقة بالأمن السيبراني الى المركز.

20 – القيام بأي واجب يكلف به من المركز.

* المرخص:

1 – تعيين/ إنشاء جهة ادارية متخصصة في مجال حوكمة الأمن السيبراني باعتبارها جهة تنسيق مباشرة للعمل مع المركز.

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

3 – تنفيذ المرخِّص والجهات الخاضعة لَه ضوابط ومعايير الأمن السيبراني الوطنية الاساسية الصادرة من المركز، ورفع التقارير الدورية والتوصيات بشأنها الى المركز.

4 – إصدار وتحديث اللوائح، والسياسات الخاصة بالمرخص والجهات الخاضعة له، والعمل على تنفيذها بعد اعتمادها من المركز.

5 – التقييم الدوري للمخاطر السيبرانية وقياس مستوى الجاهزية الخاصة بالمرخص والجهات الخاضعة له، ورفع التقارير الدورية والتوصيات بشأنها الى المركز.

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

7 – تطوير عمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة بالمرخص والجهات الخاضعة له.

8 – إصدار وتحديث الإجراءات الخاصة بعمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة بالمرخص والجهات الخاضعة له.

9 – المشاركة بخطة التدريب والتمارين والمسابقات الصادرة من المركز.

10 – وضع وتنفيذ خطة التدريب والتمارين والمسابقات الخاصة بالمرخص والجهات الخاضعة له.

11 – إعداد وتنفيذ خطة بناء القدرات الخاصة بالمرخِّص، والإشراف على تنفيذ خطة الجهات الخاضعة له.

12 – المحافظة على أمن المرخص السيبراني والجهات الخاضعة لها بما لا يتعارض مع اختصاصات المركز، مع تمكين المركز من مباشرة اختصاصاته، والالتزام بتنفيذ واتباع كل ما يصدر منه.

13 – إخطار المركز بشكل فوري بأي خطر، أو تهديد، أو اختراق واقع، أو محتمل.

14 – تبادل المعلومات والتقارير الامنية بين المرخِّص والمركز.

15 – المساهمة في إنشاء قاعدة بيانات بالتهديدات الالكترونية الخاصة بالمركز وإدامتها.

16 – إعداد وتنفيذ الخطط الخاصة بالمرخص بشأن التوعية ونشر الثقافة السيبرانية.

17 – الإشراف على تنفيذ الخطط الخاصة بالجهات الخاضعة له بشأن التوعية ونشر الثقافة السيبرانية.

18 – التزام الجهات الخاضعة بتزويد المرخص 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، وفقا للوائح والضوابط والإجراءات المنظمة والصادرة من قبل المرخِّص.

20 – رفع التقارير الدورية بشأن الوضع الأمني السيبراني للمرخِّص والجهات الخاضعة له الى المركز.

21 – رفع المقترحات والتوصيات المتعلقة بالأمن السيبراني للمرخص والجهات الخاضعة له الى المركز.

22 – القيام بأي واجب يكلف به من المركز.

* المرخص له أو مقدم الخدمة:

1 – تعيين/ إنشاء جهة ادارية متخصصة في مجال حوكمة الأمن السيبراني باعتبارها جهة تنسيق مباشرة للعمل مع المرخِّص.

2 – إعداد الخطة التشغيلية الخاصة بها بناء على الاستراتيجية الوطنية واستراتيجية المرخص، والعمل على تنفيذها تحت إشراف المرخص.

3 – تنفيذ ضوابط ومعايير الأمن السيبراني الوطنية الاساسية الصادرة من المرخص، ورفع التقارير الدورية والتوصيات بشأنها الى المرخص.

4 – تنفيذ اللوائح، والسياسات الصادرة من المرخص.

5 – التقييم الدوري للمخاطر السيبرانية وقياس مستوى الجاهزية الخاصة به ورفع التقارير الدورية والإجراءات التي تمت بشأنها الى المرخص.

6 – إعداد وتنفيذ الضوابط والخطط الخاصة بمواجهة المخاطر والتهديدات السيبرانية تحت إشراف المرخِّص.

7 – تطوير عمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة به تحت إشراف المرخِّص.

8 – إصدار وتحديث الإجراءات الخاصة بعمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة به تحت إشراف المرخِّص.

9 – المشاركة بخطة التدريب والتمارين والمسابقات الصادرة من المرخص.

10 – وضع وتنفيذ خطة التدريب والتمارين والمسابقات الخاصة به تحت إشراف المرخِّص.

11 – إعداد وتنفيذ خطته الخاصة ببناء القدرات بإشراف المرخص.

12 – المحافظة على أمنه السيبراني بما لا يتعارض مع اختصاصات المرخص، مع تمكين المرخِّص والمركز من مباشرة اختصاصاتها، والالتزام بتنفيذ واتباع كل ما يصدر منهما.

13 – إخطار المرخص بشكل فوري بأي خطر، أو تهديد، أو اختراق واقع، أو محتمل.

14 – تبادل المعلومات والتقارير الأمنية مع المرخِّص.

15 – إعداد وتنفيذ خطط التوعية ونشر الثقافة السيبرانية.

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

17 – أخذ موافقة المركز قبل حفظ أي بيانات حساسة أو معالجتها خارج دولة الكويت، وفقا للوائح والضوابط والإجراءات المنظمة والصادرة من قبل المرخص.

18 – رفع التقارير الدورية بشأن الوضع الأمني السيبراني بها الى المرخِّص.

19 – رفع المقترحات والتوصيات المتعلقة بالأمن السيبراني بها الى المرخِّص.

20 – القيام بأي واجب يكلف به من المرخِّص.

* 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 بناء على الاستراتيجية الوطنية، والعمل على تنفيذها تحت إشراف المركز، ورفع التقارير الدورية والتوصيات بشأنها الى المركز.

3 – تنفيذ منظم القطاع ومشغلي الخدمات الالكترونية ضوابط ومعايير الأمن السيبراني الوطنية الاساسية الصادرة من المركز، ورفع التقارير الدورية والتوصيات بشزنها الى المركز.

4 – إصدار وتحديث اللوائح، والسياسات الخاصة بمنظم القطاع ومشغلي الخدمات الالكترونية، والعمل على تنفيذها بعد اعتمادها من المركز.

5 – التقييم الدوري للمخاطر السيبرانية وقياس مستوى الجاهزية الخاصة بمنظم القطاع ومشغلي الخدمات الالكترونية، ورفع التقارير الدورية والتوصيات بشأنها الى المركز.

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

7 – تطوير عمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة بالمرخص والجهات الخاضعة له.

8 – إصدار وتحديث الإجراءات الخاصة بعمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة بالمرخص والجهات الخاضعة له.

9 – المشاركة بخطة التدريب والتمارين والمسابقات الصادرة من المركز.

10 – وضع وتنفيذ خطة التدريب والتمارين والمسابقات الخاصة بالمرخص والجهات الخاضعة له.

11 – إعداد وتنفيذ خطة بناء القدرات الخاصة بالمرخِّص، والإشراف على تنفيذ خطة الجهات الخاضعة له.

12 – المحافظة على أمن المرخص السيبراني والجهات الخاضعة لها بما لا يتعارض مع اختصاصات المركز، مع تمكين المركز من مباشرة اختصاصاته، والالتزام بتنفيذ واتباع كل ما يصدر منه.

13 – إخطار المركز بشكل فوري بأي خطر، أو تهديد، أو اختراق واقع، أو محتمل.

14 – تبادل المعلومات والتقارير الامنية بين المركز والمرخِّص.

15 – المساهمة في إنشاء قاعدة بيانات بالتهديدات الالكترونية الخاصة بالمركز وإدامتها.

16 – إعداد وتنفيذ الخطط الخاصة بالمرخص بشأن التوعية ونشر الثقافة السيبرانية.

17 – الإشراف على تنفيذ الخطط الخاصة بالجهات الخاضعة له بشأن التوعية ونشر الثقافة السيبرانية.

18 – التزام الجهات الخاضعة بتزويد المرخص 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، وفقا للوائح والضوابط والإجراءات المنظمة والصادرة من قبل المرخِّص.

20 – رفع التقارير الدورية بشأن الوضع الأمني السيبراني للمرخِّص والجهات الخاضعة لهَ الى المركز.

21 – رفع المقترحات والتوصيات المتعلقة بالأمن السيبراني للمرخص والجهات الخاضعة له الى المركز.

22 – القيام بأي واجب يكلف به من المركز.

* المرخِّص له أو مقدم الخدمة:

1 – تعيين/ إنشاء جهة ادارية متخصصة في مجال حوكمة الأمن السيبراني باعتبارها جهة تنسيق مباشرة للعمل مع المرخِّص.

2 – إعداد الخطة التشغيلية الخاصة بها بناء على الاستراتيجية الوطنية واستراتيجية المرخص، والعمل على تنفيذها تحت إشراف المرخص.

3 – تنفيذ ضوابط ومعايير الأمن السيبراني الوطنية الاساسية الصادرة من المرخص، ورفع التقارير الدورية والتوصيات بشأنها الى المرخص.

4 – تنفيذ اللوائح، والسياسات الصادرة من المرخص.

5 – التقييم الدوري للمخاطر السيبرانية وقياس مستوى الجاهزية الخاصة به ورفع التقارير الدورية والإجراءات التي تمت بشأنها الى المرخص.

6 – إعداد وتنفيذ الضوابط والخطط الخاصة بمواجهة المخاطر والتهديدات السيبرانية تحت إشراف المرخِّص.

7 – تطوير عمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة به تحت إشراف المرخِّص.

8 – إصدار وتحديث الإجراءات الخاصة بعمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة بمنظم القطاع ومشغلي الخدمات الالكترونية، ورفع التقارير الدورية والتوصيات بشأنها الى المركز.

6 – إعداد وتنفيذ خطته الخاصة ببناء القدرات بإشراف المرخص.

12 – المحافظة على أمنه السيبراني بما لا يتعارض مع اختصاصاته، والالتزام بتنفيذ واتباع كل ما يصدر منه.

13 – إخطار المركز بشكل فوري بأي خطر، أو تهديد، أو اختراق واقع، أو محتمل.

14 – تبادل المعلومات والتقارير الامنية بين منظم القطاع والمركز.

15 – المساهمة في إنشاء قاعدة بيانات بالتهديدات الالكترونية الخاصة بالمركز وإدامتها.

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

17 – الإشراف على تنفيذ الخطط الخاصة بمشغلي الخدمات الالكترونية بشأن التوعية ونشر الثقافة السيبرانية.

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

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

20 – رفع المقترحات والتوصيات المتعلقة بالأمن السيبراني لمنظم القطاع ومشغلي الخدمات الالكترونية الى المركز.

21 – القيام بأي واجب يكلف به من المركز.

مهام 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 الالكترونية.

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

3 – تنفيذ ضوابط ومعايير الأمن السيبراني الوطنية الاساسية الصادرة من منظم قطاع مشغلي الخدمات الالكترونية، ورفع التقارير الدورية والتوصيات بشأنها الى منظم قطاع مشغلي الخدمات الالكترونية.

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

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

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

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

8 – إصدار وتحديث الإجراءات الخاصة بعمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة بمنظم قطاع مشغلي الخدمات الالكترونية.

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

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

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

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

13 – إخطار منظم قطاع مشغلي الخدمات الالكترونية بشكل فوري بأي خطر، أو تهديد، أو اختراق واقع، أو محتمل.

14 – تبادل المعلومات والتقارير الامنية مع منظم قطاع مشغلي الخدمات الالكترونية.

15 – إعداد وتنفيذ خطط التوعية ونشر الثقافة السيبرانية.

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

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

18 – رفع التقارير الدورية بشأن الوضع الأمني السيبراني به الى منظم قطاع مشغلي الخدمات الالكترونية.

19 – رفع المقترحات والتوصيات المتعلقة بالأمن السيبراني به الى منظم قطاع مشغلي الخدمات الالكترونية.

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

رئيس المركز الوطني للأمن السيبراني اللواء محمد بوعركي

تطوير عمليات الأمن السيبراني وفرق الاستجابة للحوادث الخاصة بالجهات الخاضعة

تبادل المعلومات والتقارير الأمنية على المستوى الوطني والدولي وتنفيذها

تقييم النواحي الأمنية لخدمات الحكومة الإلكترونية تنظيم آليات وسبل عملها