مرسوم رقم 2.21.406 صادر في 4 ذي الحجة 1442 (15 يوليو 2021) بتطبيق القانون رقم 05.20 المتعلق بالأمن السيبراني

رئيس الحكومة،

بناء على الظهير الشريف رقم 1.17.08 الصادر في 21 من رجب 1438 (19 أبريل 2017) بتفويض السلطة فيما يتعلق بإدارة الدفاع الوطني ؛

وعلى القانون رقم 05.20 المتعلق بالأمن السيبراني الصادر بتنفيذه الظهير الشريف رقم 1.20.69 بتاريخ 4 ذي الحجة 1441 (25 يوليو 2020)؛

وعلى المرسوم رقم 2.82.673 الصادر في 28 من ربيع الأول 1403 (13 يناير1983) المتعلق بتنظيم إدارة الدفاع الوطني كما وقع تغييره وتتميمه، ولا سيما بالمرسوم رقم 2.11.509 الصادر في 22 من شوال 1432 (21 سبتمبر 2011) ؛

وبعد المداولة في مجلس الحكومة المنعقد بتاريخ 16 من ذي القعدة 1442 (27 يونيو 2021)؛

وبعد المداولة في المجلس الوزاري المنعقد بتاريخ 17 من ذي القعدة 1442 (28 يونيو 2021)،

رسم ما يلي :

الفصل الأول

هيئات حكامة الأمن السيبراني

الفرع الأول

السلطة الوطنية للأمن السيبراني

المادة الأولى

يراد بالسلطة الوطنية للأمن السيبراني المنصوص عليها في القانون المشار إليه أعلاه رقم 05.20، المديرية العامة لأمن نظم المعلومات التابعة لإدارة الدفاع الوطني، ويشار إليها بعده بالسلطة الوطنية.

الفرع الثاني

اللجنة الاستراتيجية للأمن السيبراني

المادة 2

يترأس اللجنة الاستراتيجية للأمن السيبراني المنصوص عليها في المادة 35 من القانون السالف الذكر رقم 05.20، الوزير المنتدب لدى رئيس الحكومة المكلف بإدارة الدفاع الوطني، وتتألف من الأعضاء التالي بيانهم :

- الوزير المكلف بالداخلية ؛
- الوزير المكلف بالشؤون الخارجية ؛
- الوزير المكلف بالاقتصاد والمالية ؛
- الوزير المكلف بالصناعة والاقتصاد الرقمي ؛
- المفتش العام للقوات المسلحة الملكية ؛
- قائد الدرك الملكي ؛
- المدير العام للدراسات والمستندات ؛
- المدير العام للأمن الوطني ؛
- رئيس المكتب الخامس لأركان الحرب العامة للقوات المسلحة الملكية ؛
- مفتش سلاح الإشارة لأركان الحرب العامة للقوات المسلحة الملكية؛
- المدير العام لمراقبة التراب الوطني ؛
- المدير العام لأمن نظم المعلومات ؛
- المدير العام للوكالة الوطنية لتقنين المواصلات ؛
- المدير العام لوكالة التنمية الرقمية.

في حالة الغياب أو المانع من الحضور، يمكن للوزراء المذكورين أعلاه أن يمثلوا من طرف الكتاب العامين لقطاعهم، في حين يمثل الأعضاء الآخرون من طرف نوابهم المباشرين.

يمكن لرئيس اللجنة الاستراتيجية للأمن السيبراني أن يدعو لحضور أشغالها كل شخص أو هيئة يرى فائدة في مشاركتها.

المادة 3

تجتمع اللجنة الاستراتيجية للأمن السيبراني بدعوة من رئيسها على الأقل مرة واحدة في السنة، وفق جدول أعمال يحدده.

يمكن عقد اجتماعات استثنائية للجنة في حالة الاستعجال، أو بمبادرة من رئيسها، أو بطلب من أحد أعضائها.

المادة 4

تتولى المديرية العامة لأمن نظم المعلومات مهام كتابة اللجنة الاستراتيجية للأمن السيبراني.

ولهذه الغاية، تقوم، تحت إشراف رئيس اللجنة الاستراتيجية للأمن السيبراني، بتنظيم اجتماعاتها، وتحضير جدول أعمالها، وإعداد تقاريرها، وكذا تتبع تنفيذ قراراتها.

المادة 5

تحدد كيفيات سير اللجنة الاستراتيجية للأمن السيبراني في نظام داخلي تصادق عليه في أول اجتماع لها.

يمكن للجنة الاستراتيجية للأمن السيبراني أن تحدث لديها لجنة أو لجانا تساعدها في إنجاز مهامها.

الفرع الثالث

لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة

المادة 6

تطبيقا لأحكام الفقرة الثالثة من المادة 36 من القانون السالف الذكر رقم 05.20، تتألف لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة، التي تترأسها المديرية العامة لأمن نظم المعلومات، من ممثلين عن السلطات والهيئات التالية :

- السلطة الحكومية المكلفة بالداخلية ؛
- المفتشية العامة للقوات المسلحة الملكية ؛
- الدرك الملكي ؛
- المديرية العامة للدراسات والمستندات ؛
- المديرية العامة للأمن الوطني ؛
- المديرية العامة لمراقبة التراب الوطني ؛
- المكتب الخامس لأركان الحرب العامة للقوات المسلحة الملكية ؛
- مفتشية سلاح الإشارة لأركان الحرب العامة للقوات المسلحة الملكية.

تعين السلطات والهيئات المذكورة ممثليها الدائمين في اللجنة ونوابا عنهم.

يمكن لرئيس لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة أن يدعو لحضور اجتماعاتها كل شخص أو هيئة يرى فائدة في مشاركتها.

المادة 7

تعد لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة تقارير عن أشغالها، وتحيلها إلى اللجنة الاستراتيجية للأمن السيبراني.

المادة 8

تطبيقا لأحكام الفقرة الثالثة من المادة 36 من القانون السالف الذكر رقم 05.20، تعد لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة إطارا لإدارة الأزمات والأحداث السيبرانية الجسيمة، وتعرضه للمصادقة على اللجنة الاستراتيجية للأمن السيبراني.

يحدد الإطار السالف الذكر، على الخصوص، مجال تدخل كل عضو من أعضاء لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة، وكذا الإجراءات المتعلقة بإدارة الأزمات، وكيفيات التواصل وتبادل المعلومات.

تناط بكل عضو من أعضاء لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة، في حدود الصلاحيات المسندة إلى السلطة أو الهيئة التابع لها، مهمة تفعيل الأعمال المحددة من طرف اللجنة وتتبعها.

الفصل الثاني

إجراءات حماية أمن نظم المعلومات

الفرع الأول

أحكام خاصة بالهيئات والبنيات التحتية ذات الأهمية الحيوية المتوفرة على نظم معلومات حساسة

القسم الفرعي الأول

التوجيهات الوطنية لأمن نظم المعلومات

المادة 9

في إطار التوجيهات الصادرة عن السلطة الوطنية المنصوص عليها في الفقرة الأولى من المادة 4 من القانون السالف الذكر رقم 05.20، تحدد السلطة الوطنية بمقرر توجيهات وطنية لأمن نظم المعلومات تتضمن، على الخصوص، القواعد التنظيمية والتقنية لأمن نظم المعلومات، وتنشرها في موقعها على الإنترنت.

القسم الفرعي الثاني

الدليل المرجعي لتصنيف أصول المعلومات ونظم المعلومات

المادة 10

تطبيقا لأحكام المادتين 5 و 14 من القانون السالف الذكر رقم 05.20، تقوم الهيئات والبنيات التحتية ذات الأهمية الحيوية بتصنيف نظم معلوماتها بناء على تحليل لتأثيرات الحوادث التي من المحتمل أن تمس بسرية أو بتوافر أو بتمامية أصول المعلومات، التي تشمل جميع الموارد كالمعدات والبرمجيات والمعطيات والإجراءات، المكونة لنظم المعلومات المذكورة.

المادة 11

لأجل القيام بالتصنيف المنصوص عليه في المادة 10 أعلاه، تقوم كل هيئة وكل بنية تحتية ذات أهمية حيوية بإجراء تحليل لتأثيرات حوادث الأمن السيبراني الماسة بسرية أو بتوافر أو بتمامية أصول معلوماتها.

يجب أن يعكس مستوى تأثيرات الحوادث المذكورة أهمية العواقب التي يمكن أن تؤدي إلى عدم قدرة الهيئة أو البنية التحتية ذات الأهمية الحيوية على :

- القيام بمهامها ؛
- الحفاظ على حياة الأشخاص أو صحتهم أو راحتهم ؛
- الامتثال للقوانين والأنظمة والالتزامات التعاقدية ؛
- الحفاظ على سمعتها وسمعة الدولة ؛
- الحفاظ على ثقة المواطنين والشركاء في الخدمات المقدمة وتعزيزها،

أو أن تؤدي إلى قدرة الهيئة أو البنية التحتية ذات الأهمية الحيوية على التأثير على سير عمل الأغيار من الهيئات التي تعتمد على خدماتها.

يتم تحليل التأثيرات وفق السلم التالي :

1 - **تأثير خطير جدا** : إذا أمكن لحادث أمن سيبراني يمس بسرية أو بتوافر أو بتمامية أصل المعلومات، أن :

- يؤثر سلبا على الحفاظ على القدرات الأمنية والدفاعية للدولة ؛
- يضر بالمصالح الاستراتيجية للدولة ؛
- يضر بصحة السكان وسلامتهم ؛
- يربك أو يضر بسير الاقتصاد الوطني ؛
- يتسبب في عجز كلي أو جزئي للعديد من البنيات التحتية ذات الأهمية الحيوية من شأنه أن يعرقل أداء وظائفها الأساسية.

2 - **تأثير خطير** : إذا أمكن لحادث أمن سيبراني يمس بسرية أو بتوافر أو بتمامية أصل المعلومات، أن يتسبب في :

- عجز كلي أو جزئي لبنية تحتية ذات أهمية حيوية من شأنه أن يعرقل أداء وظائفها الأساسية ؛
- عجز كلي لهيئة أو أكثر، لا تعتبر بنية تحتية ذات أهمية حيوية، من شأنه أن يعرقل أداء وظائفها الأساسية ؛
- خسائر مالية مهمة لهيئة واحدة أو أكثر، أو لبنية تحتية ذات أهمية حيوية واحدة أو أكثر.

3 - **تأثير معتدل** : إذا أمكن لحادث أمن سيبراني يمس بسرية أو بتوافر أو بتمامية أصل المعلومات، أن يتسبب في :

- إرباك أو اضطراب طفيف لوظائف بنية تحتية ذات أهمية حيوية ؛
- عجز جزئي لهيئة واحدة أو أكثر، لا تعتبر بنية تحتية ذات أهمية حيوية أو أكثر، من شأنه أن يعرقل أداء وظائفها ؛
- خسائر مالية غير مهمة ؛
- أو أي عواقب أخرى ذات طبيعة مماثلة.

4 - **تأثير محدود**: إذا أمكن لحادث أمن سيبراني يمس بسرية أو بتوافر أو بتمامية أصل المعلومات، أن يتسبب في :

- إرباك أو اضطراب لوظائف هيئة ما لا تعتبر بنية تحتية ذات أهمية حيوية ؛
- خسائر مالية محدودة ؛
- أو أي عواقب أخرى ذات طبيعة مماثلة.

المادة 12

يتم تصنيف نظام المعلومات استنادا إلى السلم المعتمد في تحليل التأثيرات المنصوص عليه في المادة 11 أعلاه، وذلك وفق المستويات التالية :

- «الفئة أ»، إذا كان لحادث أمن سيبراني واحد على الأقل يمس بسرية أو بتوافر أو بتمامية أحد أصول المعلومات المكون لنظام المعلومات تأثير خطير جدا؛
- «الفئة ب»، إذا كان لجميع حوادث الأمن السيبراني التي تمس بسرية أو بتوافر أو بتمامية أصول المعلومات المكونة لنظام المعلومات تأثير خطير على الأكثر ؛
- «الفئة ج»، إذا كان لجميع حوادث الأمن السيبراني التي تمس بسرية أو بتوافر أو بتمامية أصول المعلومات المكونة لنظام المعلومات تأثير معتدل على الأكثر.
- «الفئة د»، إذا كان لجميع حوادث الأمن السيبراني التي تمس بسرية أو بتوافر أو بتمامية أصول المعلومات المكونة لنظام المعلومات تأثير محدود على الأكثر.

تعتبر نظم المعلومات التي تنتمي إلى «الفئة أ» أو «الفئة ب» نظم معلومات حساسة.

يجب على كل هيئة حسب مدلول القانون السالف الذكر رقم 05.20 إبلاغ السلطة الوطنية بنظم معلوماتها الحساسة.

المادة 13

يتم ترتيب فئات أصول المعلومات من نوع «معطيات» المصنفة استنادا إلى السلم المعتمد في تحليل التأثيرات المنصوص عليه في المادة 11 أعلاه، حسب مستوى حساسيتها من حيث السرية، وفقا للمستويات التالية :

- «سري جدا» إذا كان لحادث أمن سيبراني يمس بالسرية، تأثير خطير جدا ؛
- «سري» إذا كان لحادث أمن سيبراني يمس بالسرية، تأثير خطير ؛
- «مكتوم» إذا كان لحادث أمن سيبراني يمس بالسرية، تأثير معتدل ؛
- «نشر محدود» إذا كان لحادث أمن سيبراني يمس بالسرية، تأثير محدود.

لأجل تطبيق أحكام المادة 11 من القانون السالف الذكر رقم 05.20، تعتبر المعطيات المصنفة في أحد المستويين «سري جدا» و«سري» معطيات حساسة.

المادة 14

تطبق كل هيئة أو بنية تحتية ذات أهمية حيوية تدابير الحماية المتعلقة بأمن نظم المعلومات المناسبة للتصنيف المخصص لها. وتشمل هذه التدابير، على الخصوص، ما يلي :

- وضع العلامات ومعالجة المعلومات والدعامات وتخزينها ونقلها وإتلافها ؛
- تعليمات الأمن التي يجب مراعاتها من قبل الأشخاص ؛
- الأمن المادي.

تصدر السلطة الوطنية التوجيهات والمراجع المتعلقة بهذه التدابير، مع الأخذ بعين الاعتبار مختلف مستويات تصنيف نظم المعلومات والمعطيات.

المادة 15

تراجع كل هيئة أو بنية تحتية ذات أهمية حيوية تصنيف أصولها المعلوماتية ونظم معلوماتها مرة واحدة على الأقل كل ثلاث (3) سنوات، وكلما دعت الضرورة إلى ذلك.

المادة 16

تقوم كل هيئة أو بنية تحتية ذات أهمية حيوية بإبلاغ المستخدمين لديها وتحسيسهم بإجراءات استعمال أصول المعلومات ونظم المعلومات وفقا للتصنيف وتدابير الحماية المخصصة لها.

القسم الفرعي الثالث

مهام المسؤول عن أمن نظم المعلومات

المادة 17

لأجل تطبيق الفقرة الأولى من المادة 6 من القانون السالف الذكر رقم 05.20، تقوم كل هيئة أو بنية تحتية ذات أهمية حيوية بإخبار السلطة الوطنية بالمسؤول عن أمن نظم معلوماتها الذي يتولى، على الخصوص، القيام بما يلي :

- تحديد تحديات ومخاطر الأمن السيبراني وتحليلها، مع مراعاة التطورات التنظيمية والتقنية ؛
- تحديد أهداف الأمن السيبراني للهيئة بالتعاون مع الأطراف المعنية ووضع تدابير الأمن المناسبة ؛
- المساهمة في وضع سياسة أمن نظم المعلومات وتتبعها بتعاون مع الأطراف المعنية ؛
- تحديد خطة عمل سنوية أو متعددة السنوات لتنفيذ سياسة أمن نظم المعلومات ؛
- تتبع إدارة حوادث الأمن السيبراني ؛
- تقديم تقارير منتظمة إلى رؤسائه حول مخاطر أمن نظم المعلومات ؛
- تنشيط دورات تحسيسية لفائدة المستخدمين.

الفرع الثاني

لائحة قطاعات الأنشطة ذات الأهمية الحيوية

المادة 18

تحدد في الملحق رقم 1 المرفق بهذا المرسوم لائحة قطاعات الأنشطة ذات الأهمية الحيوية وكذا السلطات الحكومية أو المؤسسات العمومية أو باقي الأشخاص الاعتباريين الخاضعين للقانون العام المشرفين على تنسيق هذه القطاعات.

يمكن تغيير أو تتميم اللائحة السالفة الذكر بقرار لرئيس الحكومة باقتراح من إدارة الدفاع الوطني.

الفرع الثالث

مقتضيات خاصة بالمتعهدين

المادة 19

لتطبيق أحكام الفقرة الثانية من المادة 28 من القانون السالف الذكر رقم 05.20، يقوم المتعهد بما يلي :

- تعيين شخص مكلف بتسهيل الولوج إلى مرافق المتعهد وتقديم المساعدة اللازمة لوضع الأجهزة التقنية بشبكاته ؛

- توفير عناصر هندسة شبكاته من أجل تحديد مكان تفعيل هذه الأجهزة ومواصفاتها التقنية ؛

- توفير المتطلبات التقنية المسبقة لربط الأجهزة المذكورة بنقاط شبكة المتعهد التي تحددها السلطة الوطنية ؛

- السماح بوضع الأجهزة التقنية في وسط مؤمن ؛

- مساعدة السلطة الوطنية على وضع الأجهزة التقنية التي تمكن من جمع وتحليل المعطيات التقنية طبقا لأحكام المادة 28 من القانون السالف الذكر رقم 05.20 ؛

- الاقتصار في الولوج إلى هذه الأجهزة على الأشخاص المعينين من لدن السلطة الوطنية لهذا الغرض ؛

- السماح للسلطة الوطنية بإدارة واستغلال الأجهزة التقنية عن بعد، وكذا اختبارها بكيفية دورية لضمان فعاليتها عند وقوع حادث أمن سيبراني.

يجب ألا تؤثر هذه الأجهزة على توافر وأمن وتمامية الشبكات والخدمات المقدمة من طرف المتعهد.

الفصل الثالث

معايير تأهيل متعهدي افتحاص أمن نظم المعلومات وكيفيات إجراء الافتحاص ومعايير تأهيل مقدمي خدمات الأمن السيبراني

الفرع الأول

معايير تأهيل متعهدي الافتحاص

المادة 20

يخضع تأهيل متعهد افتحاص أمن نظم المعلومات للمعايير التالية :

- أن يؤسس في شكل شركة خاضعة للقانون المغربي ؛

- أن يتوفر على خبرة في ميدان افتحاص أمن نظم المعلومات ؛

- أن يتوفر على بنية تنظيمية مخصصة حصريا لافتحاص أمن نظم المعلومات ؛

- أن يستوفي الشروط الواردة في مرجع متطلبات متعهدي افتحاص أمن نظم المعلومات المنصوص عليه في المادة 22 بعده ؛

- أن يؤهل على الأقل في ثلاثة (3) مجالات افتحاص من بين المجالات المحددة في الملحق رقم 2 المرفق بهذا المرسوم، وأن يتوفر على مفتحص واحد على الأقل في كل مجال من مجالات التأهيل المطلوبة.

علاوة على ذلك، يتعين على متعهد الافتحاص لأجل تقديم خدمات افتحاص أمن نظم المعلومات المصنفة ضمن «الفئة أ» المنصوص عليها في المادة 12 من هذا المرسوم، أن يستوفي الشروط التالية :

- أن يكون أغلبية رأس ماله مملوكا من لدن مغاربة ؛

- أن يكون كل المفتحصين المقترحين من جنسية مغربية.

المادة 21

يودع طلب التأهيل من لدن متعهد افتحاص أمن نظم المعلومات لدى السلطة الوطنية، مشفوعا بملف يتضمن الوثائق التالية :

- نسخة من النظام الأساسي للشركة ؛

- شهادة تقييد الشركة بالسجل التجاري ؛

- لائحة بأسماء الشركاء وجنسيتهم ؛

- نسخ من الوثائق المثبتة لهوية مسيري الشركة وأعضاء أجهزة إدارتها وكذا المفتحصين المقترحين ؛

- مذكرة توضح الموارد البشرية والتقنية المتوفرة لدى الشركة ؛

- نسخة من السجل العدلي للمفتحصين المقترحين ؛

- السير الذاتية للمفتحصين، وعند الاقتضاء نسخ من دبلوماتهم وشواهدهم ؛

- نسخ لعقود الشغل المبرمة مع المفتحصين المقترحين ؛

- نسخ من الشواهد المسلمة من أصحاب المشاريع الذين تم القيام لحسابهم بخدمات افتحاص أمن نظم المعلومات، والتي تشير على الخصوص إلى طبيعة الخدمة المقدمة وتاريخ إنجازها ؛

- وثيقة تبين المنهجية المتبعة للقيام بخدمات الافتحاص موضوع طلب التأهيل.

يتعين على متعهد افتحاص أمن نظم المعلومات أن يخبر السلطة الوطنية بكل تغيير يطرأ على أحد العناصر الواردة في ملف طلب التأهيل.

المادة 22

بعد التأكد من استيفاء ملف الطلب لكافة الوثائق والمعلومات المطلوبة، تقوم السلطة الوطنية بإخضاع متعهد افتحاص أمن نظم المعلومات، على نفقته، لتقييم خدمات الافتحاص موضوع الطلب من لدن إحدى الهيئات التي تحددها السلطة الوطنية لهذا الغرض.

يتم إجراء هذا التقييم وفق الشروط الواردة في مرجع متطلبات متعهدي افتحاص أمن نظم المعلومات الذي تعده السلطة الوطنية وتنشره في موقعها على الإنترنت. يحدد هذا المرجع على الخصوص كيفيات تقييم المفتحصين وكذا مستويات التأهيل.

المادة 23

بناء على نتائج التقييم المنصوص عليه في المادة 22 أعلاه، يمكن للسلطة الوطنية أن تتخذ قرارا للتأهيل يتضمن على الخصوص :

- تسمية متعهد افتحاص أمن نظم المعلومات وعنوان مقره الرئيسي ؛
- مجالات الافتحاص موضوع التأهيل مع الإشارة إلى أن المتعهد يمكنه افتحاص نظم المعلومات الحساسة من «الفئة أ» أو «الفئة ب» ؛
- مدة صلاحيته على ألا تتجاوز ثلاث (3) سنوات ؛
- قائمة المفتحصين حسب مجالات الافتحاص، مع الإشارة إلى مستويات تأهيلهم.

في حالة الرفض، تبلغ السلطة الوطنية قرارها إلى طالب التأهيل.

المادة 24

يتم تجديد تأهيل متعهد افتحاص أمن نظم المعلومات وفق نفس الشروط المقررة للحصول عليه، على أن يتم تقديم طلب التجديد ستين (60) يوما على الأقل قبل انتهاء مدة صلاحية قرار التأهيل.

المادة 25

يقوم متعهد افتحاص أمن نظم المعلومات بإخبار السلطة الوطنية، فورا، بكل تغيير يطرأ على أحد العناصر التي تم على أساسها منح التأهيل.

المادة 26

إذا لم يعد متعهد الافتحاص المؤهل مستوفيا لأحد المعايير التي تم على أساسها منحه التأهيل، تقوم السلطة الوطنية بإعذاره لتنفيذ الأوامر ذات الصلة الصادرة عنها داخل أجل تحدده حسب أهمية هذه الأوامر.

وفي حالة عدم الامتثال للإعذار، تقوم السلطة الوطنية بتوقيف التأهيل إلى حين تنفيذ الأوامر المذكورة، وإذا تعذر ذلك يتم سحب التأهيل.

المادة 27

تنشر لائحة متعهدي افتحاص أمن نظم المعلومات المؤهلين بالجريدة الرسمية، وفي موقع الإنترنت الخاص بالسلطة الوطنية.

الفرع الثاني

كيفيات إجراء افتحاص أمن نظم المعلومات الحساسة المنجز من لدن متعهدي الافتحاص المؤهلين

المادة 28

تقوم الهيئات والبنيات التحتية ذات الأهمية الحيوية بإجراء افتحاص لأمن نظم معلوماتها الحساسة وفق المجالات المحددة في الملحق رقم 2 المرفق بهذا المرسوم، كلما كانت هذه النظم متناسبة مع المجالات المذكورة، على ألا تفصل بين كل عملية افتحاص في نفس المجال مدة ثلاث (3) سنوات.

المادة 29

يتم إجراء الافتحاص بناء على عقد يبرم بين طالب الافتحاص ومتعهد الافتحاص المؤهل.

لا يتم الشروع في هذا الافتحاص إلا بعد انعقاد اجتماع بين ممثلي متعهد الافتحاص والهيئة المفتحصة، ويتم خلاله الاتفاق على كافة الجوانب المتعلقة بالافتحاص، وجميع بنود العقد السالف الذكر الذي يجب أن يتضمن، على الخصوص، ما يلي :

- موضوع الافتحاص ونطاقه وأماكن إجرائه وكيفياته ؛
- أسماء ومهام المفتحصين المعينين من لدن المتعهد ؛
- المعايير المعتمدة من أجل القيام بالافتحاص ؛
- آجال تنفيذ الافتحاص ؛
- قنوات آمنة للتواصل بين المتعهد والهيئة المفتحصة وعند الاقتضاء بين المتعهد وطالب الافتحاص ؛
- الوسائل الضرورية لإنجاز الافتحاص ؛
- بنود السرية المتعلقة بالافتحاص.

المادة 30

يجب على الهيئة أن تمد متعهد الافتحاص، قبل الشروع في عملية الافتحاص، بالوثائق اللازمة للقيام بمهامه.

ويتعين على متعهد الافتحاص التقيد، أثناء القيام بمهامه، بالمتطلبات التقنية لكل مجال افتحاص المحددة في مرجع متطلبات متعهدي الافتحاص المنصوص عليه في المادة 22 أعلاه.

المادة 31

يجب على متعهد الافتحاص إبلاغ الهيئة المفتحصة، على الفور، بكل اختلال ملاحظ تبين أنه يمثل خطرا وشيكا وهاما، وأن يقترح كلما أمكن ذلك، الإجراءات التي تمكن من إزالة هذا الخطر.

يقوم متعهد الافتحاص بتوثيق كل ما تمت معاينته بمناسبة قيامه بمهمته، وتتبعه وحفظه طوال مدة الافتحاص.

المادة 32

يجب على متعهد الافتحاص المؤهل عند الانتهاء من مهامه أن يسلم لطالب الافتحاص التقرير النهائي للافتحاص مرفقا بجميع الوثائق والدعامات ذات الصلة.

يعقد اجتماع ختامي يقدم خلاله المتعهد إلى طالب الافتحاص والهيئة المفتحصة ملخصا عن تقرير الافتحاص والتوصيات ذات الصلة.

كما يجب عليه عند الانتهاء من مهمة الافتحاص، ألا يحتفظ بأي نسخة من التقارير والوثائق والدعامات المقدمة.

المادة 33

تعمل الهيئة أو المسؤول عن البنية التحتية ذات الأهمية الحيوية، التي تم افتحاصها، على حفظ تقرير الافتحاص، وجميع الوثائق المرتبطة به، لمدة لا تقل عن ثلاث (3) سنوات.

الفرع الثالث

معايير تأهيل مقدمي خدمات الأمن السيبراني

المادة 34

لتطبيق أحكام المادة 25 من القانون السالف الذكر رقم 05.20، يتم تأهيل مقدم خدمات الأمن السيبراني في مجال رصد حوادث الأمن السيبراني أو مجال التحليل والتحقيق والمعالجة لحوادث الأمن السيبراني أو هما معا، حسب المعايير التالية :

- أن يؤسس في شكل شركة خاضعة للقانون المغربي ؛

- أن يتوفر على خبرة في ميدان تقديم خدمات الأمن السيبراني ؛

- أن يتوفر على بنية تنظيمية ووسائل تقنية مخصصة حصريا لتقديم خدمات الأمن السيبراني ؛

- أن يتوفر ضمن مستخدميه، على الأقل، على ثلاثة (3) متخصصين في إحدى مجالي التأهيل المذكورين، تتوفر فيهم الخبرة والمؤهلات اللازمة المحددة في مرجع متطلبات مقدمي خدمات الأمن السيبراني الذي تعده السلطة الوطنية وتنشره في موقعها على الإنترنت ؛

- أن يضمن إيواء المعطيات الحساسة المتعلقة بخدمتي رصد وتحليل حوادث الأمن السيبراني ومعالجتها، حصريا داخل التراب الوطني ؛

- أن يضمن استغلال خدمتي رصد وتحليل حوادث الأمن السيبراني وتدبيرها، حصريا داخل التراب الوطني.

علاوة على ذلك، يتعين على مقدم الخدمات لأجل تقديم خدمات الأمن السيبراني لنظم المعلومات المصنفة ضمن «الفئة أ» المنصوص عليها في المادة 12 من هذا المرسوم، أن يستوفي الشروط التالية :

- أن يكون أغلبية رأس ماله مملوكا من لدن مغاربة ؛

- أن يكون كل المتخصصين المقترحين من جنسية مغربية.

المادة 35

يودع طلب التأهيل من لدن مقدم خدمات الأمن السيبراني لدى السلطة الوطنية، مشفوعا بملف يتضمن الوثائق التالية:

- نسخة من النظام الأساسي للشركة ؛

- شهادة تقييد الشركة بالسجل التجاري ؛

- لائحة بأسماء الشركاء وجنسيتهم ؛

- نسخ من الوثائق المثبتة لهوية مسيري الشركة وأعضاء أجهزة إدارتها وكذا المتخصصين المقترحين ؛

- مذكرة توضح الموارد البشرية والتقنية المتوفرة لدى الشركة ؛

- نسخة من السجل العدلي للمتخصصين المقترحين ؛

- السير الذاتية للمتخصصين، وعند الاقتضاء نسخ من دبلوماتهم وشواهدهم ؛

- نسخ لعقود الشغل المبرمة مع المتخصصين المقترحين ؛

- نسخ من الشواهد المسلمة من أصحاب المشاريع الذين تم القيام لحسابهم بخدمات الأمن السيبراني، والتي تشير على الخصوص إلى طبيعة الخدمة المقدمة وتاريخ إنجازها؛

- وثيقة تبين المنهجية المتبعة للقيام بخدمات الأمن السيبراني موضوع طلب التأهيل.

يتعين على مقدم خدمات الأمن السيبراني أن يخبر السلطة الوطنية بكل تغيير يطرأ على أحد العناصر الواردة في ملف طلب التأهيل.

المادة 36

بعد التأكد من استيفاء ملف الطلب لكافة الوثائق والمعلومات المطلوبة، تقوم السلطة الوطنية بإخضاع مقدم خدمات الأمن السيبراني، على نفقته، لتقييم الخدمات موضوع الطلب من لدن إحدى الهيئات التي تحددها السلطة الوطنية لهذا الغرض.

يتم إجراء هذا التقييم وفق الشروط الواردة في مرجع متطلبات مقدمي خدمات الأمن السيبراني الذي تعده السلطة الوطنية وتنشره في موقعها على الإنترنت.

المادة 37

بناء على نتائج التقييم المنصوص عليه في المادة 36 أعلاه، يمكن للسلطة الوطنية أن تتخذ قرارا للتأهيل يتضمن على الخصوص :

- تسمية مقدم خدمات الأمن السيبراني وعنوان مقره الرئيسي ؛

- مجالات التأهيل مع الإشارة إلى أن مقدم الخدمات يمكنه تقديم خدمات الأمن السيبراني لنظم المعلومات الحساسة من «الفئة أ» أو «الفئة ب» ؛

- مدة صلاحيته على ألا تتجاوز ثلاث (3) سنوات ؛

- قائمة المتخصصين حسب مجالات تقديم خدمات الأمن السيبراني.

في حالة الرفض، تبلغ السلطة الوطنية قرارها إلى طالب التأهيل.

المادة 38

يتم تجديد تأهيل مقدم خدمات الأمن السيبراني وفق نفس الشروط المقررة للحصول عليه، على أن يتم تقديم طلب التجديد ستين (60) يوما على الأقل قبل انتهاء مدة صلاحية قرار التأهيل.

المادة 39

يقوم مقدم خدمات الأمن السيبراني بإخبار السلطة الوطنية، فورا، بكل تغيير يطرأ على أحد العناصر التي تم على أساسها منح التأهيل.

المادة 40

إذا لم يعد مقدم خدمات الأمن السيبراني مستوفيا لأحد المعايير التي تم على أساسها منحه التأهيل، تقوم السلطة الوطنية بإعذاره لتنفيذ الأوامر ذات الصلة الصادرة عنها داخل أجل تحدده حسب أهمية هذه الأوامر.

وفي حالة عدم الامتثال للإعذار، تقوم السلطة الوطنية بتوقيف التأهيل إلى حين تنفيذ الأوامر المذكورة، وإذا تعذر ذلك يتم سحب التأهيل.

المادة 41

تنشر لائحة مقدمي خدمات الأمن السيبراني المؤهلين في الجريدة الرسمية، وفي موقع الإنترنت الخاص بالسلطة الوطنية.

الفصل الرابع

مقتضيات مختلفة و انتقالية وختامية

المادة 42

تضع السلطة الوطنية دليلا مرجعيا لإدارة حوادث الأمن السيبراني وتنشره في موقعها على الإنترنت. يحدد الدليل المذكور، على الخصوص، كيفيات الإبلاغ عن حوادث الأمن السيبراني ومعالجتها.

المادة 43

تتوفر الهيئات والبنيات التحتية ذات الأهمية الحيوية على أجل أقصاه اثنا عشر (12) شهرا، ابتداء من تاريخ نشر هذا المرسوم بالجريدة الرسمية، من أجل تصنيف نظم معلوماتها وإبلاغ السلطة الوطنية بالنظم التي لها طابع حساس، وذلك طبقا لأحكام القانون السالف الذكر رقم 05.20 والنصوص المتخذة لتطبيقه.

المادة 44

تظل قرارات اعتماد متعهدي خدمات الافتحاص، المتخذة وفق مقتضيات قرار رئيس الحكومة رقم 3.44.18 الصادر في 21 من صفر 1440 (31 أكتوبر 2018) بتحديد شروط اعتماد المتعهدين الخواص لافتحاص نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية وكيفيات إجراء الافتحاص، سارية المفعول إلى حين انتهاء مدة صلاحيتها.

المادة 45

تنسخ مقتضيات :

- المرسوم رقم 2.11.508 الصادر في 22 من شوال 1432 (21 سبتمبر 2011) بإحداث اللجنة الاستراتيجية لأمن نظم المعلومات ؛

- المرسوم رقم 2.15.712 الصادر في 12 من جمادى الآخرة 1437 (22 مارس 2016) بتحديد إجراءات حماية نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية ؛

- قرار رئيس الحكومة رقم 3.44.18 الصادر في 21 من صفر 1440 (31 أكتوبر 2018) بتحديد شروط اعتماد المتعهدين الخواص لافتحاص نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية وكيفيات إجراء الافتحاص.

المادة 46

يسند تنفيذ هذا المرسوم الذي ينشر بالجريدة الرسمية إلى الوزير المنتدب لدى رئيس الحكومة المكلف بإدارة الدفاع الوطني.

وحرر بالرباط في 4 ذي الحجة 1442 (15 يوليو 2021).

الإمضاء : سعد الدين العثماني.

*

* *

الملحق رقم 1

لائحة قطاعات الأنشطة ذات الأهمية الحيوية وكذا السلطات الحكومية والمؤسسات العمومية وباقي الأشخاص الاعتباريين الخاضعين للقانون العام المشرفين على تنسيق هذه القطاعات

قطاعات الأنشطة ذات الأهمية الحيوية	السلطات الحكومية و المؤسسات العمومية و باقي الأشخاص الاعتباريين الخاضعين للقانون العام المشرفين على تنسيق هذه القطاعات
قطاع الأمن العمومي	السلطة الحكومية المكلفة بالداخلية
قطاع الشؤون الخارجية	السلطة الحكومية المكلفة بالشؤون الخارجية
قطاع المالية	السلطة الحكومية المكلفة بالمالية
قطاع التشريع	الأمانة العامة للحكومة
قطاع الفلاحة	السلطة الحكومية المكلفة بالفلاحة
قطاع الصحة	السلطة الحكومية المكلفة بالصحة
قطاعات الصناعة والتجارة والاقتصاد الرقمي	السلطة الحكومية المكلفة بالصناعة والتجارة والاقتصاد الرقمي
قطاع الاتصال السمعي البصري	السلطة الحكومية المكلفة بالاتصال
قطاع إنتاج وتوزيع الطاقة	السلطة الحكومية المكلفة بالداخلية
	السلطة الحكومية المكلفة بالطاقة
قطاع المعادن	السلطة الحكومية المكلفة بالمعادن
قطاع النقل	السلطات الحكومية المكلفة بالنقل
قطاع إنتاج وتوزيع الماء	السلطات الحكومية المكلفة بالماء
القطاع البنكي	بنك المغرب
قطاع المواصلات	الوكالة الوطنية لتقنين المواصلات
قطاع التأمينات والاحتياط الاجتماعي	هيئة مراقبة التأمينات والاحتياط الاجتماعي

* * *

الملحق رقم 2

مجالات الافتحاص التي يتم تأهيل مقدمي خدمات افتحاص أمن نظم المعلومات فيها

- **افتحاص تنظيمي ومادي:** يهدف إلى التأكد من تطابق السياسات وتدابير الأمن، التي تم تحديدها وتطبيقها من لدن الهيئة المفتحصة، مع توجيهات السلطة الوطنية ؛

- **افتحاص هندسي:** يهدف إلى التحقق من مطابقة ممارسات الأمن المتعلقة باختيار وتموضع وتفعيل المعدات والبرمجيات المستعملة في نظام المعلومات للممارسات الجاري بها العمل ولمتطلبات الأمن والقواعد الداخلية للهيئة المفتحصة ؛

- **افتحاص الإعدادات:** يهدف إلى التحقق من مطابقة تفعيل ممارسات الأمن للمتطلبات والقواعد الداخلية للهيئة المفتحصة عند إعداد المعدات والبرمجيات المستعملة في نظام المعلومات ؛

- **افتحاص شفرة المصدر:** يهدف إلى تحليل جزئي أو شامل لشفرة المصدر أو للظروف التي تم وفقها تحويل هذه الشفرة إلى برمجية حتى يتم التأكد من احترام القواعد المحددة للبرمجة أو تحليل الثغرات المرتبطة بالبرمجة ؛

- **اختبارات الاختراق:** تمكن من تقييم أمن نظام معلومات أو شبكة بواسطة محاكاة هجمة حقيقية على نظام المعلومات. وتمكن هذه الوسيلة من اكتشاف ثغرات نظام معلومات الهيئة المفتحصة والتأكد من قابلية استغلالها وأثرها على هذه الهيئة ؛

- **افتحاص الأنظمة الصناعية:** يهدف إلى تقييم مستوى أمن النظام الصناعي وآليات التحكم المرتبطة به.