قرار مجلس الوزراء رقم 1699 لسنة 2020 بتاريخ 27/08/2020 يُعمل بأحكام اللائحة التنفيذية المرافقة فى شأن قانون مكافحة جرائم تقنية المعلومات المشار إليه .

المادة 1 إصدار

يُعمل بأحكام اللائحة التنفيذية المرافقة فى شأن قانون مكافحة جرائم تقنية المعلومات المشار إليه .

المادة 1

فى تطبيق أحكام هذه اللائحة يقصد بالكلمات والعبارات التالية المعنى المبين قرين كل منها :

الجهاز : الجهاز القومى لتنظيم الاتصالات .

التشفير Encryption : منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيًا بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة .

مفتاح التشفير Encryption Key : أرقام أو رموز أو حروف ذات طول محدد تستخدم فى عمليات التشفير وفك التشفير .

ويستخدم نفس المفتاح فى التشفير وفك التشفير ويسمى التشفير المتماثل ، ويجب الحفاظ على سرية المفتاح .

ويستخدم زوج من المفاتيح مترابطين بعلاقة رياضية بحيث يستخدم أحدهما فى التشفير والآخر فى فك التشفير ويسمى التشفير غير المتماثل ، ويجب الحفاظ على سرية أحد المفاتيح بينما يعلن عن الآخر بشروط ومعايير محددة .

البنية التحتية المعلوماتية الحرجة Critical Information Infrastructure : مجموعة أنظمة أو شبكات أو أصول معلوماتية أساسية يؤدى الكشف عن تفصيلاتها تعطيلها أو تغيير طريقة عملها بطريقة غير مشروعة ، أو الدخول غير المصرح به عليها ، أو الدخول أو الوصول بشكل غير قانونى للبيانات والمعلومات التى تحفظها أو تعالجها ، أو يؤدى القيام بأى فعل غير مشروع آخر بها إلى التأثير على توافر خدمات الدولة ومرافقها الأساسية أو خسائر اقتصادية أو اجتماعية كبيرة على المستوى الوطنى .

ويعد من البنية التحتية المعلوماتية الحرجة على الأخص ما يستخدم فى الطاقة الكهربائية ، الغاز الطبيعى والبترول ، الاتصالات ، والجهات المالية والبنوك ، والصناعات المختلفة ، والنقل والمواصلات والطيران المدنى ، والتعليم والبحث العلمى ، والبث الإذاعى والتليفزيونى ، ومحطات مياه الشرب والصرف الصحى والموارد المائية ، والصحة ، الخدمات الحكومية وخدمات الإغاثة وخدمات الطوارئ ، وغيرها من مرافق المعلومات والاتصالات التى قد تؤثر على الأمن القومى أو الاقتصاد القومى والمصلحة العامة وما فى حكمها .

نظام التحكم الصناعى : حاسب أو مجموعة حواسب متصلة ببعضها البعض ، وبالمعدات المتحكم بها وأدوات الاتصال المتبادل بينهم رقمية Digital أو تناظرية Analog ، أو غيرها بما فى ذلك الحساسات والمنفذات Actuator لتشغيل هذه المعدات والتحكم بها منطقيًا طبقًا للصناعة المعنية ، أو الأعمال المطلوبة فى مكان واحد أو موزعة فى أماكن متقاربة أو موزعة جغرافيًا مع اتصال النظام بالإنترنت أو بغيره من الأنظمة المماثلة أو غير المماثلة أو استقلاله وعدم اتصاله بما عداه مع تراكم مستوى التحكم أو عدم تراكمه .

نقاط الضعف Vulnerabilities : خلل أو ثغرة فى نظام تشغيل أو تطبيقات أو شبكات المعلومات أو العمليات أو السياسات الخاصة بتأمين المعلومات أو فى بيئة تقنية المعلومات أو الاتصالات والتى يمكن استغلالها فى عمليات الاختراق أو الهجوم أو الاتلاف أو التجسس أو أى عمل غير مشروع .

المادة 2 إصدار

يُنشر هذا القرار فى الجريدة الرسمية ، ويُعمل به من اليوم التالى لتاريخ نشره .

صدر برئاسة مجلس الوزراء فى 8 المحرم سنة 1442 هـ

(الموافق 27 أغسطس سنة 2020 م) .

رئيس مجلس الوزراء

دكتور/ مصطفى كمال مدبولى

المادة 2

يلتزم مقدمو خدمات تقنيات المعلومات باتخاذ الإجراءات التقنية والتنظيمية التالية تنفيذًا للبندين (2 و3) من الفقرة أولاً من المادة رقم (2) من القانون :

1 - تشفير البيانات والمعلومات بما يحافظ على سريتها ، وعدم اختراقها باستخدام نظام تشفير قياسى متماثل أو غير متماثل لا يقل فى تأمينه عن (Advanced Encryption Standard (ASE-128 بمفتاح شفرة لا يقل عن (128 بت) ، مع مسئوليته بالحفاظ على سرية وأمان مفتاح التشفير .

2 - تنصيب واستخدام نظم وبرامج ومعدات مكافحة البرمجيات والهجمات الخبيثة والتأكد من صلاحيتها وتحديثها .

3 - استخدام بروتوكولات آمنة ، مثل بروتوكول نقل النص التشعبى المؤمن HTTPS .

4 - وضع صلاحيات بالشبكات والملفات وقواعد البيانات وتحديد المسئولين ، لضمان حماية الوصول المنطقى Logical Access إلى الأصول المعلوماتية والتقنية لمنع الوصول غير المصرح به .

5 - إعداد قائمة بالأجهزة والمعدات وأرقامها المميزة والمسلسلة وطرازاتها وكذا بيان بالنظم والبرامج والتطبيقات وقواعد البيانات المستخدمة ومواصفاتها .

6 - تطبيق أفضل الممارسات والضوابط عند اختيار مواصفات كلمات السر أو المرور وفقًا للملحق رقم (1) المرفق باللائحة التنفيذية .
7 - توثيق إجراءات التنصيب والتشغيل الخاصة بالأنظمة .
8 - ضمان تنفيذ وتشغيل وصيانة الأنظمة وإلزام الأطراف المتعاقد معها بإبرام اتفاقيات تحدد مستوى تقديم الخدمة مع الجهة وحدود مسئولية كل جهة .
9 - إجراء التحديثات الخاصة بالنظم والبرامج والتطبيقات بشكل دورى وإتمام الاختبارات اللازمة قبل إجراء التحديثات .
10 - إجراء اختبار سنوى للكشف عن الاختراقات أو المخاطر الأمنية .
11 - استخدام معدات وأجهزة ونظم وبرمجيات الجدران النارية (NGFW-UTM-Firewalls) لحماية الشبكات والنظم .

المادة 3

يلتزم مقدمو خدمات تقنية المعلومات والاتصالات التى تمتلك أو تدير أو تشغل البنية التحتية المعلوماتية الحرجة المخاطبين بأحكام هذا القانون ، باتخاذ الإجراءات التقنية والتنظيمية التالية تنفيذًا للبندين (2 و3) من الفقرة أولاً من المـادة رقم (2) من القانون :
1 - إعداد سياسة أمن معلومات واعتمادها من الإدارة العليا للبنية التحتية المعلوماتية الحرجة وضمان مراجعتها كل عام لضمان استمرار ملائمة وكفاية وفاعلية تلك السياسة .
على أن تتضمن تلك السياسة متطلبات الأجهزة والجهات الرقابية والتنظيمية المختصة بالبنية التحتية المعلوماتية الحرجة ، والمتطلبات القانونية ، والمتطلبات الخاصة بالموارد البشرية .
2 - ضمان التأكد من الامتثال لمـا ورد بهذا القانون ولائحته والقرارات التنفيذية ذات الصلة من التزامات تقنية أو تنظيمية .
3 - تشفير البيانات والمعلومات بما يحافظ على سريتها ، وعدم اختراقها باستخدام نظام تشفير قياسى متماثل أو غير متماثل لا يقل تأمينه عن (AES-256) Advanced Encryption Standard بمفتاح شفرة لا يقل عن (256 بت) يتم توليده باستخدام نظام عشوائى آمن . واستخدام نظام إدارة مفاتيح تشفير قياسى للحفاظ على سريتها ودورة حياتها ومستويات استخدامها فى التطبيقات المختلفة .
4 - استخدام شهادات تصديق إلكترونى صادرة من جهة من جهات إصدار شهادات التوقيع الإلكترونى المعترف بها فى جمهورية مصر العربية وبضوابط قانون تنظيم التوقيع الإلكترونى ولائحته التنفيذية ، وذلك لكافة المستخدمين لأنظمة المعلومات الخاصة بالبنية المعلوماتية التحتية الحرجة .
5 - منع الوصول المـادى لغير المخول أو المصرح لهم الدخول أو الوصول لمقار وأجهزة ومعدات أنظمة البنية التحتية المعلوماتية الحرجة .
6 - استخدام ضوابط نفاذ قوية Strong Authentication وفعالة من خلال فئتين أو أكثر من فئـات التوثـق Multi-factor Authentication وبحسب مستوى المخاطـر ، بما يضمن تحديد المسئولية وعدم الإنكار .
7 - توثيق إجراءات التنصيب والتشغيل الخاصة بنظم البنية التحتية المعلوماتية الحرجة وإتاحتها للمستخدمين المخول لهم ذلك عند حاجتهم إليها ، وإلزام الموردين بتزويد الجهة بكامل الوثائق الخاصة بالإجراءات التشغيلية .
8 - ضمان تنفيذ وتشغيل وصيانة أنظمة البنية التحتية المعلوماتية الحرجة وإلزام الأطراف المتعاقد معها بإبرام اتفاقيات تحدد مستوى تقديم الخدمة مع الجهة .
9 - تنصيب واستخدام نظم وبرامج ومعدات المكافحة والحماية من البرمجيات والهجمات الخبيثة ، والكشف عنها والتأكد من صلاحيتها وتحديثها .
10 - إجراء التحديثات الخاصة بالنظم والبرامج والتطبيقات بشكل دورى . مع الأخذ فى الاعتبار ضوابط التعامل مع إجراء التحديثات على أنظمة التحكم الصناعى مع عدم اتصالها المباشر بشبكة الإنترنت ، وإتمام الاختبارات اللازمة قبل إجراء التحديثات .
11 - إجراء مسح سنوى لأنظمة التحكم الصناعى للكشف عن الثغرات ونقاط الضعف واتخاذ الإجراءات اللازمة للتعامل معها .
12 - إجراء اختبار سنوى للكشف عن الاختراقات أو المخاطر الأمنية وتثبيت أجهزة المنع والكشف عن الاختراقات .
13 - اتخاذ الإجراءات الملائمة للتعامل مع الثغرات الفنية للأجهزة وللنظم والبرامج والتطبيقات عند العلم بها .
14 - إجراء عمليات أخذ نسخ احتياطية شهرية للبيانات والمعلومات ، والاحتفاظ بها وتخزينها مشفرة فى موقع آخر .
15 - استخدام معدات وأجهزة ونظم وبرمجيات الجدران النارية (NGFW-UTM-Firewalls) لحماية الشبكات والنظم .
16 - استخدام بروتوكولات آمنة ، مثل بروتوكول نقل النص التشعبى المؤمن HTTPS .
17 - إعداد قائمة بالأجهزة والمعدات وأرقامها المميزة والمسلسلة وطرازاتها وكذا بيان بالنظم والبرامج والتطبيقات وقواعد البيانات المستخدمة ومواصفاتها .
18 - تحديد مسئوليات الإدارة العليا ومسئولى تكنولوجيا المعلومات وأمن المعلومات بشكل واضح وصلاحيات وسلطات وواجبات والتزامات كل منهم ، مع ضرورة اتساق ذلك مع ما تقوم به إدارات الموارد البشرية وشئون العاملين من إعـداد للهياكل ، والتوصيف الوظيفى ، والأنشطة التدريبية وغيرها من أنشطة وعمليات تلك الإدارات .
19 - إبلاغ المركز الوطنى للاستعداد لطوارئ الحاسب والشبكات بالجهاز عن أى حوادث أو اختراقات فور العلم بحدوثها .
20 - وضع خطة استمرارية العمل والبدائل المقترحة فى حال حدوث أى مخاطر أو أزمات تتعلق بتقديم الخدمة أو انقطاعها ، والقدرة على استعادة الخدمة والعمل فى حال الكوارث ، واختبـار الخطـة دوريًا .

المادة 4

يُنشأ بالجهاز سجلان لقيد الخبراء ، يقيد بأولهما الفنيون والتقنيون العاملون بالجهاز ، ويقيد بالآخر الخبراء من الفنيين والتقنيين من غير العاملين به .
ويتم القيد فى السجل الأول الخاص بالعاملين بالجهاز بناءً على القواعد والشروط والإجراءات الآتية :

1 - أن يكون حاصلاً على مؤهل علمى أو فنى أو تقنى يتناسب ومجال الخبرة .
2 - أن يكون قد أمضى عام على الأقل فى عمله بالجهاز .
3 - أن يجتاز الاختبارات الفنية التى يجريها الجهاز للمتقدم .

المادة 5

يُقيد الخبراء من الفنيين والتقنيين من غير العاملين بالجهاز بالسجل الثانى للخبراء طبقًا للقواعد والشروط الآتية :
1 - أن يكون مصريًا متمتعًا بالأهلية المدنية الكاملة .
ويجوز قيد الأجنبى على أن يتعهد كتابة بخضوعه للقوانين المصرية .
2 - أن يكون محمود السيرة حسن السمعة .
3 - ألا يكون قد سبق الحكم عليه بحكم نهائى بالإدانة فى جريمة مخلة بالشرف .
4 - أن يكون لديه سيرة ذاتية تتضمن خبرة عملية مناسبة .
5 - موافقة الجهات المعنية من جهات الأمن القومى على القيد بالسجل .
ويترتب على تخلف أى شرط من الشروط السابقة الشطب من السجل بقرار من الجهاز .

المادة 6

يقوم الخبراء وفقًا للمادتين رقمى (1) ، (10) من القانون بتنفيذ المهام الفنية والتقنية التى يتم تكليفهم بها من جهات التحقيق أو الجهات القضائية المختصة أو من الجهات المعنية بمكافحة جرائم تقنية المعلومات بشأن الجرائم موضوع هذا القانون .

المادة 7

يُراعى الجهاز الحفاظ على سرية البيانات الواردة بسجلات قيد الخبراء وعدم الإفصاح عنها إلا بموجب أمر قضائى .

المادة 8

يتعين على من يرغب فى قيد اسمه فى السجل الثانى للخبراء أن يتقدم للرئيس التنفيذى للجهاز بطلب كتابى بذلك موضحًا فيه التخصص الذى يرغب العمل فيه كخبير ، وأن يرفق بالطلب صور الشهادات والمستندات المؤيدة لطلبه .
ويمكن للجهاز أن يطلب منه خلال ثلاثون يومًا من تاريخ تقديم الطلب معلومات إضافية قبل الفصل فى الطلب ، ويعتبر عدم الرد على الطلب لمدة ستين يومًا من تاريخ تقديمه رفضًا له .
وفى حال رفض الجهاز الطلب ، يحق للمتقدم التظلم بالإجراءات المقررة قانونًا .

المادة 9

تحوز الأدلة الرقمية ذات القيمة والحجية للأدلة الجنائية المادية فى الإثبات الجنائى إذا توافرت فيها الشروط والضوابط الآتية :
1 - أن تتم عملية جمع أو الحصول أو استخراج أو استنباط الأدلة الرقمية محل الواقعة باستخدام التقنيات التى تضمن عدم تغيير أو تحديث أو محو أو تحريف للكتابة أو البيانات والمعلومات ، أو أى تغيير أو تحديث أو إتلاف للأجهزة أو المعدات أو البيانات والمعلومات ، أو أنظمة المعلومات أو البرامج أو الدعامات الالكترونية وغيرها .
ومنها على الأخص تقنية Write Blocker، Digital Images Hash، وغيرها من التقنيات المماثلة .
2 - أن تكون الأدلة الرقمية ذات صلة بالواقعة وفى إطار الموضوع المطلوب إثباته أو نفيه ، وفقًا لنطاق قرار جهة التحقيق أو المحكمة المختصة .
3 - أن يتم جمع الدليل الرقمى واستخراجه وحفظه وتحريزه بمعرفة مأمورى الضبط القضائى المخول لهم التعامل فى هذه النوعية من الأدلة ، أو الخبراء أو المتخصصين المنتدبين من جهات التحقيق أو المحاكمة ، على أن يبين فى محاضر الضبط ، أو التقارير الفنية على نوع ومواصفات البرامج والأدوات والأجهزة والمعدات التى تم استخدامها ، مع توثيق كود وخوارزم Hash الناتج عن استخراج نسخ مماثلة ومطابقة للأصل من الدليل الرقمى بمحضر الضبط أو تقرير الفحص الفنى ، مع ضمان استمرار الحفاظ على الأصل دون عبث به .
4 - فى حالة تعذر فحص نسخة الدليل الرقمى وعدم إمكانية التحفظ على الأجهزة محل الفحص لأى سبب يتم فحص الأصل ويثبت ذلك كله فى محضر الضبط أو تقرير الفحص والتحليل .
5 - أن يتم توثيق الأدلة الرقمية بمحضر إجراءات من قبل المختص قبل عمليات الفحص والتحليل له وكذا توثيق مكان ضبطه ومكان حفظه ومكان التعامل معه ومواصفاته .

المادة 10

يتم توصيف وتوثيق الدليل الرقمى من خلال طباعة نسخ من الملفات المخزن عليها أو تصويرها بأى وسيلة مرئية أو رقمية ، واعتمادها من الأشخاص القائمين على جمع أو استخراج أو الحصول أو التحليل للأدلة الرقمية ، مع تدوين البيانات التالية على كل منها :
1 - تاريخ ووقت الطباعة والتصوير .
2 - اسم وتوقيع الشخص الذى قام بالطباعة والتصوير .
3 - اسم أو نوع نظام التشغيل ورقم الإصدار الخاص به .
4 - اسم البرنامج ونوع الإصدار أو الأوامر المستعملة لإعداد النسخ .
5 - البيانات والمعلومات الخاصة بمحتوى الدليل المضبوط .
6 - بيانات الأجهزة والمعدات والبرامج والأدوات المستخدمة .

المادة 11

يلتزم كل مسئول عن إدارة موقع أو حساب خاص أو بريد إلكترونى أو نظام معلوماتى سواء كان شخصا طبيعيًا أو اعتباريًا وفقا للمادة رقم (29) من القانون ، باتخاذ التدابير والاحتياطات التأمينية الفنية اللازمة وفقا للالتزامات الواردة فى المـادة رقم (2) من هذه اللائحة بالنسبة لمديرى مواقع مقدمى خدمات تقنية المعلومات .

كما يلتزم مديرو مواقع مقدمى خدمات تقنية المعلومات والاتصالات التى تمتلك أو تدير أو تشغل البنية التحتية المعلوماتية الحرجة بالالتزامات الواردة فى المادة رقم (3) من هذه اللائحة .

ويلتزم الممثل القانونى ومسئول الإدارة الفعلية لمقدمى الخدمة بإثبات توفيره الامكانيات التى تمكن مديرو المواقع من اتخاذ التدابير والاحتياطات التأمينية اللازمة لقيامه بعمله .

وفى جميع الأحوال يلتزم الممثل القانونى ومسئول الإدارة الفعلية ومدير الموقع لدى أى مقدم خدمة بإتاحة مفاتيح التشفير الخاصة به للمحكمة المختصة أو لجهات التحقيق المختصة فى حال وجود تحقيق فى إحدى الشكاوى أو المحاضر أو الدعاوى عند طلبها رسميًا من تلك الجهات .

المادة 12

يشترط لاعتماد الجهاز إقرار المجنى عليه بالصلح طبقا للمادة رقم 42 من القانون ، فى الجرائم المنصوص عليها فى المواد (14، 17، 18، 23) استيفاء وتقديم ما يلى :

1 - شهادة صادرة من النيابة أو المحكمة المختصة بحسب الأحوال بالقيد والوصف للجريمة محل الصلح .

2 - صورة طبق الأصل من المحضر أو الوثيقة التى أثبت فيها الصلح بين المتهم والمجنى أو وكيله الخاص أو خلفه العام أمام النيابة أو المحكمة المختصة والمتضمنة إقرار المجنى عليه بهذا الصلح .

3 - شهادة صادرة من النيابة المختصة تفيد عدم صدور حكم نهائى فى الدعوى الجنائية .

4 - طلب باسم الرئيس التنفيذى للجهاز لاعتماد المحضر أو الوثيقة المتضمنة إقرار المجنى عليه بالصلح يقدم من المتهم أو من وكيله أو من خلفه العام .

المادة 13

يكون تصالح المتهم طبقًا للمادة رقم (42) من القانون ، فى الجرائم المنصوص عليها بالمـادتين (29، 35) من القانون من خلال الجهاز باستيفاء وتقديم ما يلى :

شهادة صادرة من النيابة أو المحكمة المختصة بحسب الأحوال بالقيد والوصف للجريمة موضـوع التصـالح .

شهادة صادرة من النيابة المختصة تفيد عدم صدور حكم نهائى فى موضوع الجريمة محل طلب التصالح .

أن يقدم المتهم الراغب فى التصالح أو وكيله قبل رفع الدعوى الجنائية الإيصال الدال على سداده مبلغًا يعادل ضعف الحد الأقصى للغرامة المقررة للجريمة .

أن يقدم المتهم الراغب فى التصالح أو وكيله بعد رفع الدعوى الجنائية الإيصال الدال على سداده ثلثى الحد الأقصى للغرامة المقررة للجريمة أو قيمة الحد الأدنى للغرامة أيهما أكثر قبل صدور حكم نهائى فى الموضوع .