

هيئة تنظيم الاتصالات

قرار

رقم ٢٠١٨/٩٣

بإصدار لائحة أمن شبكة الاتصالات

استنادا إلى قانون تنظيم الاتصالات الصادر بالمرسوم السلطاني رقم ٢٠٠٢/٣٠ ،
وإلى اللائحة التنفيذية لقانون تنظيم الاتصالات الصادرة بالقرار رقم ٢٠٠٨/١٤٤ ،
وإلى موافقة مجلس إدارة الهيئة ،
وبناء على ما تقتضيه المصلحة العامة ،

تقرر

المادة الأولى

يعمل في شأن أمن شبكة الاتصالات ، بأحكام اللائحة المرفقة .

المادة الثانية

ينشر هذا القرار في الجريدة الرسمية ، ويعمل به من اليوم التالي لتاريخ نشره .

صدر في : ٣ من ربيع الثاني ١٤٤٠ هـ

الموافق : ١١ من ديسمبر ٢٠١٨ م

محمد بن حمد الرمحي

رئيس مجلس إدارة

هيئة تنظيم الاتصالات

لائحة أمن شبكة الاتصالات

المادة (١)

في تطبيق أحكام هذه اللائحة يكون للكلمات والعبارات الواردة فيها المعنى ذاته المنصوص عليه في قانون تنظيم الاتصالات ، ولائحته التنفيذية ، ويكون للكلمات والعبارات الآتية المعنى المبين قرين كل منها ، ما لم يقتض سياق النص معنى آخر :

١ - الشبكة :

شبكة اتصالات المرخص له .

٢ - الحوادث الأمني :

أي خرق أمني ، أو فقدان سلامة الشبكة أو أمنها .

٣ - الاختراق :

الوصول غير الشرعي إلى بيانات حساسة عن طريق التحايل على نظام الحماية .

٤ - اتفاقية الخدمة المدارة :

التعاقد مع الغير لتشغيل أو صيانة أو إدارة شبكة الاتصالات التي يمتلكها المرخص له .

٥ - مقدم الخدمة المدارة :

الجهة المتعاقد معها لتشغيل أو صيانة أو إدارة شبكة الاتصالات الخاصة بالمرخص له .

٦ - الدعم الفني من المستوى الثالث :

الدعم الذي يتطلب تدخل المتخصصين من موفري المعدات ، أو الأنظمة .

المادة (٢)

تسري أحكام هذه اللائحة على جميع مكونات الشبكة ، بما في ذلك الشبكة الأساسية ، وشبكة الوصول ، وسياسة إدارة كلمات المرور ، والمقاسم ، والتحديثات ، ونظام أسماء النطاقات (DNS) ، والمباني .

كما تسري على جميع الأجهزة والمرافق الموصلة بالشبكة ، بما في ذلك شبكات تطوير المحتوى (CDN) ، وأنظمة التخزين (الدائم والمؤقت) ، وأنظمة توزيع المحتوى .

المادة (٣)

يلتزم المرخص له بالآتي :

- ١ - تطبيق التدابير الفنية والتنظيمية اللازمة لإدارة المخاطر الأمنية المرتبطة بشبكات وخدمات الاتصالات الواردة في المعيار القياسي (ISO 22301) لاستمرارية الأعمال ، والمعايير القياسية الصادرة من الاتحاد الدولي للاتصالات عبر مجموعة سلسلة المعايير X (ITU-T X series standards) .
- ٢ - إجراء تدريب منتظم للعاملين لديه بإدارة أمن الشبكات ، وعقد جلسات توعوية عامة لباقي العاملين مرة واحدة في السنة على الأقل .
- ٣ - تطبيق التدابير الفنية اللازمة لحماية الشبكة من أي مخاطر محتملة عن طريق الشبكات الداخلية للمشاركين .
- ٤ - تطبيق التدابير الفنية اللازمة لمنع محاولات الكشف عن نقاط الضعف الموجودة في الشبكة .
- ٥ - إجراء عمليات تدقيق أمني داخلية بصفة دورية لتحديد التهديدات ، ونقاط الضعف على مستوى الشبكة ونظام التشغيل ، ومستوى التطبيقات وإجراءات وعمليات المشغلين ، وذلك للتأكد من مستوى أمن الشبكة ، وضمان عدم حدوث أي اختراق ، أو ولوج شخص غير مصرح له إليها ، وإجراء عملية تدقيق أمني خارجية بإشراك طرف ثالث مستقل من ذوي الخبرة مرة واحدة في السنة على الأقل ، وذلك بعد موافقة الهيئة ، على أن يقوم المرخص له بتزويد الهيئة بمواعيد هذه العمليات ، ونتائجها خلال المدة التي تحددها الهيئة .
- ٦ - إجراء تقييم دوري لبيان مستوى أمن المباني وعناصر الشبكة الخارجية والمحطات والأبراج ومستوى التطبيقات ، والخوادم ، وبرمجيات الأنظمة ، وذلك لتحديد التهديدات ونقاط الضعف المحتملة ، واتخاذ ما يلزم من إجراءات إذا تبين وجود أي خلل ، أو تهديد محتمل في مستوى الأمن .
- ٧ - التأكد من قيام موفر المعدات أو الأنظمة بضمان توفير وتثبيت الإصلاحات المتعلقة بأمن وسلامة الشبكة في وقت مناسب ، وبطريقة فعالة .

- ٨ - إعداد سجل يقيد فيه المخاطر التي تتعرض لها الشبكة والخدمات المقدمة ، والأحداث التي تقع داخل مباني ومواقع المرخص له ، على أن يتم موافاة الهيئة بتقرير مفصل عما تم قيده في هذا السجل مرة واحدة في السنة على الأقل ، أو عند طلبها .
- ٩ - الاحتفاظ بتسجيلات الدوائر التلفزيونية المغلقة (CCTV) ، وسجل الدخول والخروج من المباني ، وسجل نظام كشف التسلل (IDS) ، على أن يلتزم المرخص له بحفظ التسجيلات وهذه السجلات طبقا لوسائل أمانة ومناسبة لمدة سنة واحدة على الأقل .
- ١٠ - إخطار الهيئة بأي حادث أمني يؤثر على سلامة الشبكة خلال (٢٤) أربع وعشرين ساعة من تاريخ العلم بحدوثة ، وإعداد تقرير تفصيلي عنه ، ورفعها إلى الهيئة خلال (١٥) الخمسة عشر يوما الآتية لتاريخ العلم ، على أن يشتمل هذا التقرير على الإجراءات التي تم اتباعها لإدارته ، والإجراءات التصحيحية والوقائية التي تم اتخاذها بشأنه ، ويكون للهيئة - متى رأت ضرورة لذلك - إعلام الجمهور عن الحادث الأمني الذي وقع .
- ١١ - إخطار الهيئة فور وقوع أي اختراق ذي تأثير كبير على تشغيل شبكات وخدمات المرخص له أو محاولة اختراق يمكن أن يكون لها التأثير نفسه إذا نجحت ، ويكون للهيئة في هذه الحالة الحق في إعلام الجمهور بحدوث الاختراق ، أو طلب ذلك من المرخص له بما يحقق المصلحة العامة . وفي جميع الأحوال يلتزم المرخص له بإخطار الهيئة بأي حوادث قد ينتج عنها تعطيل ، أو انقطاع الخدمات .
- ١٢ - إبقاء أنظمة إدارة وتشغيل الشبكة داخل السلطنة .
- ١٣ - حظر الوصول عن بعد إلى الشبكة إلا من قبل العاملين بالدعم الفني من المستوى الثالث ، وذلك في حالة الضرورة ، ولفترة محدودة ، وبعد الحصول على موافقة المرخص له .
- ١٤ - ضمان عدم قيام مقدم الخدمة المدارة والمتعاقدين معه من الباطن بتشغيل أو إدارة أو صيانة أو الوصول إلى نظم وأجهزة تحقيق متطلبات الأمن الوطني ، أو الاضطلاع بأي أنشطة من خلالها .
- ١٥ - تطبيق التدابير الفنية اللازمة لحماية شبكات وخدمات الاتصالات ضد الحوادث الأمنية .

- ١٦ - تطبيق التدابير الفنية اللازمة لحماية أجهزة وخوادم الشبكة .
- ١٧ - تطبيق التدابير الفنية اللازمة لحماية المواقع والمباني التابعة له ، وحصر الدخول إليها للمصرح لهم فقط .
- ١٨ - تطبيق التدابير الفنية اللازمة لحماية بيانات المشترك ضد السرقة ، أو الفقدان .
- ١٩ - تطبيق التدابير الفنية اللازمة لحماية كابينة الكوابل الخارجية ، وكابينة توزيع الألياف البصرية (FDH) ، ونقطة التوزيع (DP) .
- ٢٠ - تطبيق التدابير الفنية اللازمة لحماية مواقع الأبراج ، والمحطات .
- ٢١ - تزويد الهيئة بالبيانات ، والمعلومات متى طلبت ذلك .

المادة (٤)

يجب على المرخص له عند إبرام اتفاقية الخدمة المدارة مراعاة الآتي :

- ١ - ضمان بقاء أمن الشبكة والخدمات والمباني ضمن المسؤولية الكاملة للمرخص له .
- ٢ - تقييم المخاطر والامتثال لتدابير التخفيف من المخاطر بشكل واضح من قبل المرخص له .
- ٣ - تقييم قدرة مقدم الخدمة المدارة من قبل المرخص له عبر عملية ممنهجة .
- ٤ - إدارة متطلبات أمن الشبكة والخدمات والمباني بشكل مستمر ، وعلى المرخص له الحصول على ضمانات من مقدم الخدمة المدارة بأن هذه المتطلبات قد استوفيت .
- ٥ - إدارة أمن الشبكة والخدمات والمباني بعناية في أثناء تغيير مقدم الخدمة المدارة ، أو إنهاء العقد معه .
- ٦ - تضمين اتفاقية الخدمة المدارة الآتي :
 - أ - متطلبات أمن الشبكة والخدمات والمباني .
 - ب - المتطلبات الأمنية المتعلقة بموظفي مقدم الخدمة المدارة .
 - ج - متطلبات إدارة عملية الوصول إلى أنظمة الاتصالات وتقنية المعلومات والصلاحيات الممنوحة لمستخدمي هذه الأنظمة .
 - د - المتطلبات الأمنية المتعلقة بالخدمات والمنتفعين والبيانات والنظم .

المادة (٥)

تتمتع التقارير والبيانات والمعلومات المقدمة من المرخص له تطبيقاً لأحكام هذه اللائحة بالسرية التامة ، ولا يجوز الاطلاع عليها من قبل الغير إلا إذا ارتأت الهيئة إتاحتها لطرف ثالث بما يخدم المصلحة العامة .

المادة (٦)

يجوز للهيئة ، في أي وقت ، سواء بنفسها أو عن طريق الشركات المتخصصة في هذا الشأن ، إجراء عمليات تدقيق أمنية دورية ، بالإضافة إلى عمليات التدقيق الأمني في حالة حدوث أي حادث أمني ، وذلك كله على نفقة المرخص له .
وفي جميع الأحوال يلتزم المرخص له بتنفيذ التوجيهات التي تصدرها الهيئة في هذا الشأن .

المادة (٧)

مع عدم الإخلال بالعقوبات المقررة قانوناً ، تفرض غرامة إدارية على كل من يخالف أحكام هذه اللائحة حسب الجدول الآتي ، وتضاعف الغرامة في حالة التكرار :

م	المخالفة	الغرامة بالريال العماني
١	مخالفة البندين (١ أو ١٥) من المادة (٣)	(٢٠٠٠٠٠) مائتا ألف
٢	مخالفة البنود (٣ أو ٤ أو ٥ أو ٦ أو ٧ أو ٨ أو ٩ أو ١١ أو ١٤) من المادة (٣)	(٣٠٠٠٠٠) ثلاثون ألفاً
٣	مخالفة البنود (٢ أو ١٠ أو ١٢ أو ١٩) من المادة (٣) ، أو مخالفة المادة (٤) أو المادة (٥)	(١٠٠٠٠٠) عشرة آلاف
٤	مخالفة البندين (١٦ أو ٢٠) من المادة (٣)	(٢٠٠٠٠٠) عشرون ألفاً
٥	مخالفة البند (١٧) من المادة (٣)	(١٠٠٠٠٠) عشرة آلاف + ضعف التكاليف اللازمة لإصلاح الضرر
٦	مخالفة البند (١٨) أو البند (١٣) أو البند (٢١) من المادة (٣)	(١٠٠٠٠٠٠) مائة ألف
٧	مخالفة المادة (٦)	(١٥٠٠٠٠٠) مائة وخمسون ألفاً