هيئة تنظيم الاتصالات
Telecommunications Regulatory Authority

قرار رقم (5) لسنة 2017
بإصدار اللائحة التنظيمية لإدارة مخاطر البنية التحتية الأساسية للاتصالات

مجلس إدارة هيئة تنظيم الاتصالات:

بعد الاطلاع على قانون الاتصالات الصادر بالمرسوم بقانون رقم (48) لسنة 2002، وعلى الأخص المادة (3) الفقرتين (ب) و(هـ)،

وعلى المرسوم رقم (47) لسنة 2008 بإعادة تشكيل مجلس إدارة هيئة تنظيم الاتصالات، وتعديلاته،

وعلى القرار رقم (29) لسنة 2016 بشأن اعتماد الخطة الوطنية الرابعة للاتصالات،

وبناءً على عرض المدير العام لهيئة تنظيم الاتصالات،

وبعد موافقة مجلس إدارة هيئة تنظيم الاتصالات،

قرر الآتي:

المادة الأولى

يعمل بأحكام اللائحة التنظيمية لإدارة مخاطر البنية التحتية الأساسية للاتصالات المرافقة لهذا القرار.

المادة الثانية

يُنشر هذا القرار واللائحة التنظيمية المرافقة في الجريدة الرسمية، ويُعمل بها من اليوم التالي لتاريخ النشر.

رئيس مجلس إدارة هيئة تنظيم الاتصالات
د. محمد أحمد العامر

صدر بتاريخ: 4 رمضان 1438هـ
الموافق: 30 مايو 2017م

اللائحة التنظيمية لإدارة مخاطر البنية التحتية الأساسية للاتصـــالات

مادة (1)

التعريفات

أ- في تطبيق أحكام هذه اللائحة، يكون للكلمات و المصـــطلحات التالية المعاني المبينة قرين كل منها، ما لم يقتضِ سياق النص خلاف ذلك، كما يكون للكلمات و المصطلحات المستخدمة في هذه اللائحة ذات المعاني الواردة في المادة (1) من قانون الاتصالات الصادر بالمرسوم بقانون رقم (48) لسنة 2002:

قانون الاتصالات:	قانون الاتصالات الصادر بالمرسوم بقانون رقم (48) لسنة 2002.
المرخص له المعني:	أي مرخص لـه يصـــدر بشـــأنـه قرار إدارة المخـاطر المنصوص عليه في المادة (4) من هذه اللائحة.
المقيِّم:	كل شـــخص طبيعي أو اعتباري معتمد كمدقق أول لنظم إدارة أمن المعلومات (ISMS) على أســـاس معيار الأيزو 27001 وذلك لتقييم وتدقيق نظم إدارة أمن المعلومات.
حصر الأصول:	قائمة موثقة لجميع الأصـــول التي تم حصـــرها في البنية التحتية الاساسية للاتصالات.
خطة استمرارية العمل:	إطار عمل لأفضـل الممارسـات للحد من الانقطاعات أثناء وقوع الحوادث غير المتوقعة والتي قد توقف تنفيذ الأعمال بشـكل تام. ويتمثل الغرض من هذه الممارسـة هو تحسـين مرونة الاعمال واستمراريتها.
تدقيق الاعتماد:	تدقيق يُنفذ من قبل مقيم مؤهل مستقل لصـالح المرخص له المعني لاعتماد البنية التحتية الاســـاســـية للاتصـــالات

	للمرخص له المعني، ويطلق على نتائج هذا التدقيق اسم "تقرير تدقيق الاعتماد".
البنية التحتية الأساسية للاتصالات:	تشمل: أ) أي بنية تحتية للاتصالات تعتبر أساسية لاستمرارية الوظائف الاجتماعية الحيوية والمتعلقة بالصحة، والسلامة، والأمن الوطني، والاقتصاد أو الرفاهية الاجتماعية للأشخاص، والتي قد يسبب انقطاعها أو تدميرها أثراً بالغاً. ب) أي نظام مركزي يخزن ويعالج البيانات الشخصية.
حادث أمني:	أية حدث غير مرغوب فيه أو غير متوقع ينتج عنه فقدان الخدمة أو اختراق غير مصرح به بشكل متعمد أو خلال أنشطة كيدية.
مؤشر المخاطر المحتملة:	أدوات رقمية أو بيانات قانونية تدل على خرق أمني محتمل، وتتضمن "عنوان بروتوكول الإنترنت" لمصدر الاختراق الأمني والأساليب الأخرى المستخدمة من قبل المصدر لتنفيذ الاختراق الأمني.
البنية التحتية:	الأنظمة والمرافق المادية الأساسية والتنظيمية مثل (المباني، وأجهزة الشبكات، ومزودات الطاقة، والأشخاص والعمليات) المطلوبة لتشغيل شبكة الاتصالات العامة.
شهادة الأيزو:	المنظمة الدولية للمعايير.
اختبار الاختراق:	عملية منهجية تُستخدم للتحقق من ضوابط الحماية للمرخص له المعني لتحديد أية نقاط ضعف يمكن استغلالها من قبل المهاجمين في الفضاء السيبراني.

البيانات الشخصية:	أي معلومات متعلقة بشخص طبيعي معرف أو ممكن التعرف عليه، أو شخص طبيعي يمكن تحديده بطريقة مباشرة أو غير مباشرة بوسائل يمكن استخدامها بطريقة معقولة على الأرجح من قبل المرخص له، وعلى وجه الخصوص عن طريق الرجوع إلى معلومات المستخدم أو المشترك، ورقم الهوية، وبيانات الموقع، ومعرف الهوية عبر الإنترنت أو بعامل أو أكثر يخص الهوية المادية والفيسيولوجية والوراثية والعقلية والاقتصادية والثقافية أو الاجتماعية لهذا الشخص.
تقييم المخاطر:	عملية منهجية لتقييم المخاطر المحتملة على البنية التحتية الأساسية للاتصالات.
قرار إدارة المخاطر:	قرار يصدر من قبل الهيئة طبقاً لأحكام المادة 4 من هذه اللائحة.
عملية إدارة المخاطر:	مجموعة أنشطة ومناهج متسقة تُستخدم في الحد من المخاطر التي تشكل تهديد على البنية التحتية الاساسية للاتصالات.
المخاطر:	التهديد بوقوع أو احتمالية وقوع ضرر أو خسارة أو أي حادثة سلبية أخرى بسبب نقاط ضعف خارجية أو داخلية، ويمكن تفاديها من خلال اتخاذ اجراءات وقائية.
الإجراء الوقائي:	إجراء أو أداة ضبط توفر الحماية من وقوع ضرر لضمان أمن وتوفر البنية التحتية الاساسية للاتصالات.

اختراق أمني:	أي نفاذ غير مصـرح به للبيانات والتطبيقات والشـبكات و المرافق، ينتج عنه إفصاح عن اية معلومات حساسة أو اية تأثيرات محتملة على تشغيل البنية التحتية.
تدقيق المراقبة:	تدقيق دوري يُنفذ من قبل مقيِّم مستقل لصـالح المرخص له المعني لضمان استيفاء بنيته التحتية الاساسية للاتصالات لمتطلبات معيار الأيزو 27001، ويطلق على نتيجة هذا التدقيق اسم "تقرير تدقيق المراقبة".

ب-تكون الإشـــارات إلى الوقت هي إشـــارات إلى الوقت في مملكة البحرين مقاســـاً باستخدام نظام توقيت 24 ساعة.

مادة (2)

أهداف اللائحة

تهدف هذه اللائحة إلى تحقيق ما يلي:

أ. وضع عملية إدارة المخاطر لحصر وتحديد البنية التحتية الاساسية للاتصالات.

ب. وضع أسلوب موحد ومتسق لتقييم وحماية أمن وتوفر البنية التحتية الاساسية للاتصالات.

ج. تحديد مسـئوليات والتزامات المرخص له فيما يتعلق بالكشـف والاسـتجابة في الوقت المناسب للحوادث الامنية والاختراقات الامنية.

د. تحديد المسئوليات والالتزامات للمرخص له فيما يتعلق بإدارة المخاطر.

هـ. تحديد المســـئوليات والالتزامات للمرخص له المعني فيما يتعلق بعملية إدارة المخاطر لبنيته التحتية الأساسية للاتصالات.

مادة (3)

التزامات المرخص لهم

أ- يلتزم المرخص لهم بالقيام بما يلي:

1- اتخاذ الإجراءات المناسبة لإدارة المخاطر على أمن وتوفر بنيتهم التحتية، والخطوات المناسبة لحماية أمن وتوفر بنيتهم التحتية، قدر المستطاع.

2- إبلاغ الهيئة خلال أربعة وعشرين (24) ساعة من علمه بأي اختراق أمني أو وقوع حادث أمني.

3- تقديم تقرير تفصيلي للهيئة خلال خمسة (5) أيام عمل من علمه بأي اختراق أمني أو وقوع حادث أمني على أن يتضمن هذا التقرير البيانات والمعلومات الآتية:

أ. تاريخ ووقت ابتداء الاختراق الامني أو وقوع الحادث الأمني.

ب. تاريخ ووقت معالجة الاختراق الامني أو الحادث الأمني بشكل كامل وفي حال ما إذا كان الحادث مازال مستمراً وقت البلاغ، يجب ابلاغ الهيئة بوقت معالجته حال توفر ذلك.

ج. معلومات بشأن الموقع ومنها العنوان كحد أدنى.

د. شرح موجز عن الاختراق الامني أو الحادث الأمني، بما في ذلك السبب والضرر الناتج عنه والخسارة المالية المقدرة وإجراءات التخفيف من آثاره الذي تم اتخاذها من قبل المرخص له حتى إعداد التقرير.

هـ. أي مؤشرات للمخاطر المحتملة التي تم تحديدها أثناء التحقيق.

ب- يجوز للهيئة عند استلامها تقريراً طبقاً لأحكام هذه المادة اتخاذ الإجراءين التاليين أو أحداهما، متى رأت ذلك مناسباً:

أ) إبلاغ الجمهور بوقوع الاختراق الامني أو الحادث الأمني، أو تطلب من المرخص له إبلاغ الجمهور.

ب) إبلاغ الأجهزة الأمنية أو الجهات الحكومية المعنية بهذا التقرير.

مادة (4)
قرار إدارة المخاطر

أ- تصدر الهيئة قرار إدارة المخاطر للفئات الآتية من المرخص لهم ممن:

1- يحملون الترخيص الممتاز لخدمات الاتصالات المتنقلة.

2- يحملون الترخيص الممتاز لمرافق الاتصالات الدولية.

3- يقومون بتركيب وتشغيل و/أو إدارة البنية التحتية الاساسية للاتصالات حسبما يتم تحديده من الهيئة.

ب- تأخذ الهيئة في الاعتبار، لتحديد المرخص له المعني طبقاً للبند (3) من الفقرة (أ) من هذه المادة المعايير الآتية:

1- مدى أهمية البنية التحتية للمرخص له المعني لدعم القطاعات الرئيسية للمجتمع والاقتصاد.

2- أثر عدم توفر البنية التحتية للمرخص له المعني على القطاعات الرئيسية للمجتمع والاقتصاد.

3- الخسائر المادية للقطاعات الرئيسية للمجتمع والاقتصاد الناتجة عن عطل البنية التحتية للمرخص له المعني.

ج- يجب أن يتضمن قرار إدارة المخاطر، على الأقل، ما يلي:

1- مبررات اعتبار المرخص له على أنه مرخص له معني.

2- المستندات المطلوبة من قبل المرخص له المعني طبقاً لأحكام المادة (5) من هذه اللائحة.

3- المواصفات العامة لعناصر البنية التحتية.

4- قائمة أولية بأنواع التهديدات.

مادة (5)

التزامات المرخص لهم المعنيون

يجب على المرخص لهم المعنيين تنفيذ عملية إدارة المخاطر –عند اســـتلام قرار إدارة المخاطر–وذلك وفقاً لأحكام القرار والأحكام الآتية:

أ- يجب على المرخص له المعني خلال فترة ثلاثة (3) أشهر من تاريخ استلام قرار إدارة المخاطر:

1- تحديد بنيته التحتية الاساسية للاتصالات في مستند حصر الأصول.

2- تزويد الهيئة بمستند حصر الأصول وفقاً لقرار إدارة المخاطر.

ب- إعداد وتنفيذ والحصـــول على وحفظ وتقديم المســـتندات التالية إلى الهيئة خلال ثمانية عشرة (18) شهراً من تاريخ استلام قرار إدارة المخاطر من قبل الهيئة:

1- خطة استمرارية العمل.

2- شهادة الأيزو 27001.

3- تقرير تدقيق الاعتماد لشهادة الأيزو 27001.

4- تقرير تقييم المخاطر المطبق لتدقيق الاعتماد.

ج– تزويد الهيئة بعد حصوله على شهادة الأيزو 27001 وبصفة سنوية بالمستندات الآتية:

1- تقرير تدقيق المراقبة لشهادة الأيزو 27001.

2- تقرير تقييم المخاطر المطبق لتدقيق المراقبة.

3- خطة استمرارية العمل المحدثة؛ إن وجدت.
4- نسخة من خطة الاستجابة للحوادث وفقاً لمتطلبات شهادة الأيزو 27001.

د- الحصـول على إعادة اعتماد شـهادة الأيزو 27001 كل ثلاث (3) سـنوات من تاريخ الحصول على شهادة الأيزو 27001 وإبلاغ الهيئة بذلك.

مادة (6)
عمليات تقييم المخاطر الإضافية

أ- للهيئة أن تطلب من المرخص له المعني تنفيذ عملية تقييم مخاطر إضـــافية في حال ارتأت بأن البنية التحتية الاساسية للاتصالات للمرخص له المعني غير آمنة بدرجة كافية، وقد تتضـــمن هذه العملية تنفيذ اختبار الاختراق من قبل مقيِّم مســـتقل مؤهل ومناســـب، على أن يتحمل المرخص له المعني تكاليف المقيِّم المستقل.

ب- في حال طلب الهيئة إجراء عملية تقييم مخاطر إضـافية طبقاً للفقرة (أ) من هذه المادة، يجب على المرخص له المعني اسـتكمال وتقديم تقرير تقييم المخاطر الإضـافية إلى الهيئة خلال ثلاثة (3) أشـهر من تاريخ طلب الهيئة، ما لم تصـدر أية تعليمات كتابية بخلاف ذلك من قبل الهيئة.

مادة (7)
الإجراءات الوقائية الإضافية

أ- للهيئة أن تطلب من المرخص له المعني -بعد مراجعة المســتندات المقدمة من قبله طبقاَ لأحكـام المواد (5) و(6) و(8) من هذه اللائحـة- تنفيـذ الإجراءات الوقـائيـة

الإضـافية بهدف زيادة الحد من المخاطر على بنيته التحتية الأسـاسـية للاتصـالات وذلك خلال ثلاثة (3) أشهر من تاريخ الطلب.

ب-يجب على المرخص له المعني أن يؤكد إلى الهيئة كتابياً بشـكل فوري عند اسـتكمال تنفيذ الإجراءات الوقائية الإضافية المنصوص عليها في الفقرة (أ) من هذه المادة.

مادة (8)
عملية إدارة المخاطر غير الكافية

في حال ارتأت الهيئة بأن المسـتندات المقدمة بموجب أحكام المواد (5) و(6) و(7) من هذه اللائحة من قبل المرخص له المعني غير كافية، للهيئة الحق في تعيين مقيِّم مستقل لتحديد أية قصور. على أن يتحمل المرخص له المعني تكاليف المقيِّم المستقل.

مادة (9)
تحقيق الالتزام بأحكام اللائحة

مع عدم الإخلال بصـــلاحية الهيئة المنصـــوص عليها في المادة (8) من هذه اللائحة، يعتبر إخلال المرخص له بأحكام هذه اللائحة إخلالاً جسيماً لأحكام قانون الاتصـالات. وللهيئة اتخاذ التدابير والجزاءات المنصـــوص عليها في قانون الاتصـــالات على كل مرخص له يخالف أحكام هذه اللائحة.

مادة (10)
التكاليف

يجب على كل مرخص له معني تحمل كافة التكاليف الخاصـــة للوفاء بالتزاماته بموجب هذه اللائحة، بما في ذلك تكاليف تنفيذ عملية تقييم المخاطر الإضافية المنصوص عليها

في المادة (6) من هذه اللائحة وتنفيذ الإجراءات الوقائية الإضـــافية المنصـــوص عليها المادة (7) من هذه اللائحة.

مادة (11)
السرية

أ- يجب ان تتعامل الهيئة مع كافة المعلومات المقدمة لها بموجب هذه اللائحة وفقا لأحكام قانون الاتصالات ذات العلاقة والإرشادات الصادرة من قبل الهيئة.
ب- يجب على المرخص لهم اتخاذ كافة الإجراءات اللازمة لضمان خصوصية وســرية المعلومات التي حصــلوا عليها في إطار تطبيق هذه اللائحة، ويُســمح بالإفصاح عن هذه المعلومات فقط وفقا لأحكام قوانين مملكة البحرين.