

## سياسة قطر للطاقة بشأن الإفصاح المسؤول

### ١. حول هذه السياسة

تدرك قطر للطاقة مدى أهمية المحافظة على أمن أنظمتها لتكنولوجيا المعلومات وبنيتها التحتية. وفي إطار التزامنا بالأمن، فقد وضعنا هذه السياسة بشأن الإفصاح المسؤول لتعلمكم بتوقعاتنا فيما يتعلق بالإبلاغ عن الثغرات الأمنية المُكتشفة في أنظمتنا على نحو يتسم بالسلامة والأمن والمسؤولية.

وتهدف هذه السياسة إلى توفير إطار بما يتيح إمكانية الإبلاغ عن الثغرات الأمنية على نحو يتسم بالمسؤولية ومعالجتها أو تصحيحها، وذلك للمحافظة على سلامة خدماتنا واستمراريتها وأمنها. وإذا كنت باحثاً أمنياً وواجهت ثغرة أمنية، فإننا نود أن نتعاون معك لإصلاحها قبل أن يطلع عليها الآخرون مع احتمالية أن يُساء استغلالها. ويُعرف ذلك باسم "الإفصاح المسؤول".

### ٢. النطاق

يتعين عليك الإبلاغ عن أية اكتشافات تتعلق بالثغرات الأمنية في أنظمتنا بأسرع وقت ممكن وفي حدود المعقول على النحو المبين أدناه. ونحن مهتمون بالفئات التالية من الثغرات الأمنية: تنفيذ التعليمات البرمجية عن بُعد، الثغرات الأمنية في لغة الاستعلام الهيكلية (SQL)، وعيوب المصادقة أو التفويض، وتنفيذ التعليمات البرمجية من جانب الخادم، والأخطاء، والثغرات الأمنية في التشفير.

فيما يلي الفئات التي تقع خارج النطاق:

- الإبلاغ عن شكاوى الخدمات (يُرجى الاتصال بالمسؤول المحلي في قطر للطاقة)
- الإبلاغ عن أشكال الاحتيال المحتملة أو المسائل ذات الصلة بالامتثال (يُرجى الاتصال بخط المساعدة العام في قطر للطاقة)
- الإبلاغ عن حملات التصيد الاحتيالي، أو رسائل البريد الإلكتروني، أو الفيروسات، أو البرامج الضارة (يُرجى الإبلاغ إلى [CyberIncidentReport@qatarenergy.qa](mailto:CyberIncidentReport@qatarenergy.qa))

### ٣. الإبلاغ عن ثغرة أمنية بطريقة مسؤولة

إذا اكتشفت وجود ثغرة أمنية، عندئذ يُرجى وصفها بشكل مفصل مع تقديم الدليل المؤيد إن أمكن ذلك، وذلك حتى ينتهي لخبرائنا المختصين في مخاطر المعلومات تحليل هذا الاكتشافات. وبأقصى حد ممكن، يُرجى إدراج التالي في بلاغك:

- نوع الثغرة الأمنية أو المشكلة
- الخدمة، أو المنتج، أو محدد مواقع المعلومات (URL) المتأثر
- تكوين خاص أو متطلبات لإعادة إنتاج المشكلة



- المعلومات اللازمة لإعادة إنتاج المشكلة
  - أثر الثغرة الأمنية، بالإضافة إلى شرح الكيفية التي يمكن من خلالها للمهاجم اكتشافها وأن يقوم باستغلالها
- نحن نفضل أن تكون الرسالة باللغة الإنجليزية أو العربية. ويمكنك إرسال البلاغ إلى [CyberIncidentReport@qatarenergy.qa](mailto:CyberIncidentReport@qatarenergy.qa). وتتوافر إمكانية استقبال البلاغات المجهولة الهوية، إلا ويُرجى ملاحظة أنه في حالة عدم ذكر اسمك، فلن نتمكن من تقاسم المستجدات حول متابعة البلاغ معك.
- ولا ينبغي أن يتجاوز حجم الرسالة بالبريد الإلكتروني ١٠ ميغا بايت. ويُرجى الاتصال بنا مبكراً عبر عنوان البريد الإلكتروني المبين أعلاه إن كنت بحاجة إلى إرسال مرفق يزيد حجمه على هذا الحجم.
- سيقوم محللو مخاطر المعلومات لدينا الاكتشافات وسيقومون بالرد في أسرع ممكن في حدود المعقول. وسيتم تحليل كل حالة على حدة. ونرجو منك أن تمنحنا الفرصة ووقت معقول لإجراء التحليل، والمحافظة على سرية المعلومات، وعدم الكشف عن الثغرة الأمنية إلى الغير دون استشارة محللينا.

وسوف نعالج كل التفاصيل الخاصة التي تلقيناها من جانبك وفقاً لإشعار الخصوصية العالمي لقطر للطاقة، وذلك لعملائنا في مجال أنشطة الأعمال والشركاء والأطراف المقابلة. وستتم معالجة بياناتك لأغراض الرد على بلاغك ومعالجة الثغرات الأمنية التي تم الإبلاغ عنها. وسنحافظ على بياناتك بعد التحقيق في بلاغك لفترة تصل إلى عام.

#### ٤. قواعد المشاركة الأخلاقية

نحن نأخذ أمن أنظمتنا وبنيتنا التحتية على محمل جاد، ونقدر الجهود التي يبذلها باحثونا الأمنيون الذين يكشفون على نحو مسؤول عن أية ثغرات أمنية يجدونها. ولضمان أمن أنظمتنا وعدم تعرض موظفينا وعمالنا وأصحاب المصلحة لأية أضرار، فإننا نرجو منك اتباع قواعد المشاركة الأخلاقية هذه عند الإبلاغ عن ثغرة أمنية:

- أبلغنا بالثغرة الأمنية على [CyberIncidentReport@qatarenergy.qa](mailto:CyberIncidentReport@qatarenergy.qa).
- أبلغ عن الثغرة الأمنية بأسرع ما يمكن لتفادي وقوع أي ضرر محتمل.
- حافظ على سرية المعلومات (وأية بيانات تم الحصول عليها نتيجة المشكلة)، وتجنب تخزين البيانات السرية، ولا تكشف عنها إلى الآخرين.
- ابدل قصارى جهدك لتجنب المساس بسرية بيانات الغير أو البيانات الشخصية؛
- لا تستغل الثغرة الأمنية لمصلحتك الخاصة أو بما يضر بقطر للطاقة، أو بموظفينا، أو عملائنا، أو أصحاب المصلحة.
- لا تستخدم الهندسة الاجتماعية للوصول إلى أنظمتنا أو بنيتنا التحتية.
- لا تتركب أية أبواب خلفية ولا تدخل تعديلات على أية بيانات في أنظمتنا.
- لا تنتسخ، أو تدخل تعديلات، أو تزيل أية بيانات من أنظمتنا.

- لا تؤثر سلباً على سرية خدماتنا أو نزاهتها أو توافرها.
- لا تقم بأية هجمات لحجب الخدمة ولا تستخدم تكنولوجيا الوصول بالقوة.
- لا تستخدم أية عمليات مسح آلية.

#### ٥. الإبلاغ عن ثغرة أمنية

إذا كنت تعتقد أنك اكتشفت ثغرة أمنية في أي نظام من أنظمتنا أو بنيتنا التحتية، فيرجى إبلاغنا بها من خلال إرسال رسالة بالبريد الإلكتروني إلى [CyberIncidentReport@qatarenergy.qa](mailto:CyberIncidentReport@qatarenergy.qa). ونرجو منك تزويدنا بأكبر قدر ممكن من التفاصيل، بما في ذلك:

- نوع الثغرة الأمنية أو المشكلة التي اكتشفتها.
- الخدمة، أو عنوان بروتوكول الإنترنت (IP)، أو محدد مواقع المعلومات (URL) المتأثر.
- أي تكوين خاص أو متطلبات لازمة لإعادة إنتاج المشكلة.
- المعلومات اللازمة لإعادة إنتاج المشكلة.
- أثر الثغرة الأمنية وشرح الكيفية التي يمكن من خلالها للمهاجم أن يقوم باستغلالها.

وسوف يراجع فريقنا الأمني بلاغك في أقرب وقت ممكن وسيعمل على معالجة الثغرة الأمنية في حينه. وسنحيطك علماً بمستوى التقدم المحرز لدينا في هذا الأمر، وسنقدر لك تعاونك في مساعدتنا على الحفاظ على أمن أنظمتنا وبنيتنا التحتية.

#### ٦. أسئلة

إذا كانت لديك أية أسئلة حول سياستنا بشأن الإفصاح المسؤول أو عملية الإبلاغ، فيرجى إرسال رسالة بالبريد الإلكتروني إلى [CyberIncidentReport@qatarenergy.qa](mailto:CyberIncidentReport@qatarenergy.qa). كما نقدر لكم التزامكم بالإفصاح المسؤول ونتطلع إلى العمل معكم للحفاظ على أمن أنظمتنا وبنيتنا التحتية.