# إحضار سياسة الكشف عن نقاط الضعف الخاصة بشركة ذات مسؤولية محدودة

## مقدمة

ترحب شركة Bring Your, LLC بتعليقات الباحثين الأمنيين وعامة الناس للمساعدة في تحسين أماننا. إذا كنت تعتقد أنك اكتشفت ثغرة أمنية أو مشكلة خصوصية أو بيانات مكشوفة أو مشكلات أمنية أخرى في أي من أصولنا، فنحن نريد أن نسمع منك. تحدد هذه السياسة خطوات إبلاغنا بنقاط الضعف، وما نتوقعه، وما يمكن أن تتوقعه منا.

## الأنظمة في النطاق

تنطبق هذه السياسة على أي أصول رقمية تملكها أو تديرها أو تحتفظ بها شركة Bring Your, LLC.

## خارج النطاق

- الأصول أو المعدات الأخرى غير المملوكة للأطراف المشاركة في هذه السياسة.

يجب الإبلاغ عن الثغرات الأمنية المكتشفة أو المشتبه بها في الأنظمة خارج النطاق إلى البائع المناسب أو السلطة المختصة.

## التزاماتنا

عند العمل معنا، وفقًا لهذه السياسة، يمكنك أن تتوقع منا ما يلي:

- الرد على بلاغك على الفور، والعمل معك لفهم بلاغك والتحقق من صحته ؛

- نسعى جاهدين لإطلاعك على التقدم المحرز في الثغرة الأمنية أثناء معالجتها ؛

- العمل على معالجة نقاط الضعف المكتشفة في الوقت المناسب، ضمن القيود التشغيلية لدينا؛ و

- قم بتوسيع Safe Harbor لأبحاث الثغرات الأمنية المتعلقة بهذه السياسة.

## توقعاتنا

من خلال المشاركة في برنامج الكشف عن الثغرات الأمنية بحسن نية، نطلب منك ما يلي:

- العب وفقًا للقواعد، بما في ذلك اتباع هذه السياسة وأي اتفاقيات أخرى ذات صلة. إذا كان هناك أي تعارض بين هذه السياسة وأي شروط أخرى معمول بها، فستسود شروط هذه السياسة ؛

- الإبلاغ عن أي ثغرة أمنية اكتشفتها على الفور؛

- تجنب انتهاك خصوصية الآخرين، وتعطيل أنظمتنا، وتدمير البيانات، و/أو الإضرار بتجربة المستخدم؛

- استخدم القنوات الرسمية فقط لمناقشة معلومات الثغرات الأمنية معنا ؛

- منحنا فترة زمنية معقولة (90 يومًا على الأقل من التقرير الأولي) لحل المشكلة قبل الكشف عنها علنًا؛

- إجراء الاختبار فقط على الأنظمة الموجودة داخل النطاق، واحترام الأنظمة والأنشطة التي تقع خارج النطاق؛

- إذا كانت هناك ثغرة أمنية توفر وصولاً غير مقصود إلى البيانات: حدد كمية البيانات التي تصل إليها بالحد الأدنى المطلوب لإثبات إثبات المفهوم بشكل فعال؛ والتوقف عن الاختبار وإرسال تقرير على الفور إذا واجهت أي بيانات مستخدم أثناء الاختبار، مثل معلومات التعريف الشخصية (PII)، أو معلومات الرعاية الصحية الشخصية (PHI)، أو بيانات بطاقة الائتمان، أو معلومات الملكية؛

- يجب ألا تتفاعل إلا مع الحسابات التجريبية التي تمتلكها أو بإذن صريح من صاحب الحساب؛ و

- لا تشارك في الابتزاز.

## القنوات الرسمية

يرجى الإبلاغ عن المشكلات الأمنية عبر <security@bringyour.com>، مع توفير جميع المعلومات ذات الصلة. كلما قدمت تفاصيل أكثر، أصبح من الأسهل بالنسبة لنا فرز المشكلة وإصلاحها.

##الملاذ الآمن

عند إجراء أبحاث الثغرات الأمنية، وفقًا لهذه السياسة، فإننا نعتبر أن هذا البحث الذي يتم إجراؤه بموجب هذه السياسة هو:

- مُصرح به فيما يتعلق بأي قوانين معمول بها لمكافحة القرصنة، ولن نبدأ أو ندعم أي إجراء قانوني ضدك بسبب الانتهاكات العرضية بحسن نية لهذه السياسة؛

- مُصرح به فيما يتعلق بأي قوانين ذات صلة بمكافحة التحايل، ولن نرفع دعوى ضدك بسبب التحايل على ضوابط التكنولوجيا؛

- معفى من القيود الواردة في شروط الخدمة (TOS) و/أو سياسة الاستخدام المقبول (AUP) التي من شأنها أن تتداخل مع إجراء البحوث الأمنية، ونحن نتنازل عن هذه القيود على أساس محدود؛ و

- قانوني ومفيد للأمن العام للإنترنت، ويتم إجراؤه بحسن نية.

يُتوقع منك، كما هو الحال دائمًا، الالتزام بجميع القوانين المعمول بها. إذا تم اتخاذ إجراء قانوني من قبل طرف ثالث ضدك والتزمت بهذه السياسة، فسنتخذ الخطوات اللازمة للإعلان عن أن أفعالك قد تمت وفقًا لهذه السياسة.

إذا كانت لديك مخاوف في أي وقت أو لم تكن متأكدًا مما إذا كانت أبحاثك الأمنية متوافقة مع هذه السياسة، فيرجى إرسال تقرير عبر إحدى قنواتنا الرسمية قبل المضي قدمًا.

> لاحظ أن الملاذ الآمن ينطبق فقط على المطالبات القانونية الخاضعة لسيطرة المنظمة المشاركة في هذه السياسة، وأن السياسة لا تلزم أطرافًا ثالثة مستقلة.