# Bring Your, LLC-Richtlinie zur Offenlegung von Sicherheitslücken

## Einführung

Bring Your, LLC freut sich über Feedback von Sicherheitsforschern und der Öffentlichkeit , um unsere Sicherheit zu verbessern. Wenn Sie glauben, eine Schwachstelle, ein Datenschutzproblem, offengelegte Daten oder andere Sicherheitsprobleme in einem unserer Assets entdeckt zu haben, möchten wir von Ihnen hören. Diese Richtlinie beschreibt die Schritte zur Meldung von Schwachstellen an uns, was wir erwarten und was Sie von uns erwarten können.

## Systeme im Geltungsbereich

Diese Richtlinie gilt für sämtliche digitalen Vermögenswerte, die Eigentum von Bring Your, LLC sind oder von Bring Your, LLC betrieben oder gepflegt werden.

## Außerhalb des Geltungsbereichs

- Vermögenswerte oder andere Ausrüstung, die nicht Eigentum von Parteien sind, die an dieser Police teilnehmen.

Entdeckte oder vermutete Schwachstellen in Systemen außerhalb des Geltungsbereichs sollten dem entsprechenden Anbieter oder der zuständigen Behörde gemeldet werden.

## Unsere Verpflichtungen

Wenn Sie gemäß dieser Richtlinie mit uns zusammenarbeiten, können Sie von uns Folgendes erwarten:

- Reagieren Sie umgehend auf Ihren Bericht und arbeiten Sie mit Ihnen zusammen, um Ihren Bericht zu verstehen und zu validieren.

- Wir bemühen uns, Sie über den Fortschritt der Behebung einer Sicherheitslücke auf dem Laufenden zu halten .

- Wir arbeiten daran, entdeckte Schwachstellen zeitnah im Rahmen unserer betrieblichen Möglichkeiten zu beheben.

- Erweitern Sie Safe Harbor für Ihre Schwachstellenforschung, die mit dieser Richtlinie in Zusammenhang stehen.

## Unsere Erwartungen

Wenn Sie in gutem Glauben an unserem Programm zur Offenlegung von Sicherheitslücken teilnehmen, bitten wir Sie um Folgendes:

- Halten Sie sich an die Regeln, einschließlich der Einhaltung dieser Richtlinie und aller anderen relevanten Vereinbarungen. Bei Unstimmigkeiten zwischen dieser Richtlinie und anderen geltenden Bedingungen haben die Bedingungen dieser Richtlinie Vorrang.

- Melden Sie jede Schwachstelle, die Sie entdecken , unverzüglich;

- Vermeiden Sie die Verletzung der Privatsphäre anderer, die Störung unserer Systeme, die Zerstörung von Daten und/oder die Beeinträchtigung des Benutzererlebnisses ;

- Nutzen Sie nur die offiziellen Kanäle, um Informationen zu Sicherheitslücken mit uns zu besprechen;

- Geben Sie uns eine angemessene Zeitspanne (mindestens 90 Tage ab der ersten Meldung), um das Problem zu lösen, bevor Sie es öffentlich machen;

- Führen Sie Tests nur an Systemen durch, die im Rahmen des Geltungsbereichs liegen, und respektieren Sie Systeme und Aktivitäten, die außerhalb des Geltungsbereichs liegen.

- Falls eine Sicherheitslücke einen unbeabsichtigten Zugriff auf Daten ermöglicht: Beschränken Sie die Menge der Daten, auf die Sie zugreifen, auf das für die wirksame Demonstration eines Proof of Concept erforderliche Minimum. Wenn Sie während des Tests auf Benutzerdaten stoßen, beispielsweise personenbezogene Daten (PII), persönliche Gesundheitsinformationen (PHI), Kreditkartendaten oder geschützte Informationen, brechen Sie den Test ab und reichen Sie sofort einen Bericht ein.

- Sie sollten nur mit Testkonten interagieren, die Ihnen gehören oder für die Sie die ausdrückliche Erlaubnis des Kontoinhabers haben.

- Beteiligen Sie sich nicht an Erpressungen.

## Offizielle Kanäle

Bitte melden Sie Sicherheitsprobleme unter Angabe aller relevanten Informationen an <security@bringyour.com>. Je mehr Details Sie angeben, desto einfacher ist es für uns, das Problem zu bewerten und zu beheben.

## Sicherer Hafen

Wenn wir Schwachstellenforschung gemäß dieser Richtlinie durchführen, betrachten wir die im Rahmen dieser Richtlinie durchgeführte Forschung als:

- Wir sind hinsichtlich aller anwendbaren Anti-Hacking-Gesetze autorisiert und werden keine rechtlichen Schritte gegen Sie wegen versehentlicher, in gutem Glauben erfolgter Verstöße gegen diese Richtlinie einleiten oder unterstützen;

- Wir sind hinsichtlich aller relevanten Gesetze zur Verhinderung von Umgehungen autorisiert und werden keine Ansprüche gegen Sie wegen der Umgehung von Technologiekontrollen geltend machen ;

- Ausgenommen von Beschränkungen in unseren Servicebedingungen (TOS) und/oder unserer Nutzungsrichtlinie (AUP), die die Durchführung von Sicherheitsforschung beeinträchtigen würden, und wir verzichten in begrenztem Umfang auf diese Beschränkungen; und

- Rechtmäßig, hilfreich für die allgemeine Sicherheit des Internets und in gutem Glauben durchgeführt.

Von Ihnen wird wie immer erwartet, dass Sie alle geltenden Gesetze einhalten. Wenn ein Dritter rechtliche Schritte gegen Sie einleitet und Sie diese Richtlinie eingehalten haben, werden wir Schritte unternehmen, um bekannt zu machen, dass Sie diese Richtlinie eingehalten haben.

Wenn Sie zu irgendeinem Zeitpunkt Bedenken haben oder sich nicht sicher sind, ob Ihre Sicherheitsforschung mit dieser Richtlinie übereinstimmt, reichen Sie bitte einen Bericht über einen unserer offiziellen Kanäle ein, bevor Sie fortfahren.

> Beachten Sie, dass Safe Harbor nur für Rechtsansprüche gilt, die unter der Kontrolle der an dieser Richtlinie teilnehmenden Organisation liegen, und dass die Richtlinie für unabhängige Drittparteien nicht bindend ist.