# Bring Your, LLC 漏洞披露政策

＃＃ 介绍

Bring Your, LLC 欢迎安全研究人员和公众提供反馈，以帮助改善我们的安全性。如果您认为您在我们的任何资产中发现了漏洞、隐私问题、暴露数据或其他安全问题，我们希望听到您的意见。此政策概述了向我们报告漏洞的步骤、我们的期望以及您可以期望我们提供的服务。

## 范围内的系统

此政策适用于 Bring Your, LLC 拥有、运营或维护的任何数字资产。

## 超出范围

- 不属于本保单参与方的资产或其他设备。

在范围之外的系统中发现或怀疑的漏洞应报告给适当的供应商或相关机构。

我们的承诺

与我们合作时，根据此政策，您可以期望我们：

- 及时回复您的报告，并与您一起理解和验证您的报告；

- 尽力让您了解漏洞处理的进展情况；

- 在我们的运营限制范围内及时修复发现的漏洞；以及

- 扩展与此政策相关的漏洞研究的安全港。

我们的期望

在真诚参与我们的漏洞披露计划时，我们要求您：

- 遵守规则，包括遵守本政策及任何其他相关协议。如本政策与任何其他适用条款有任何不一致之处，以本政策条款为准；

- 及时报告您发现的任何漏洞；

- 避免侵犯他人隐私、破坏我们的系统、破坏数据和/或损害用户体验；

我们讨论漏洞信息；

- 在公开披露问题之前，请给我们提供合理的时间（自首次报告之日起至少 90 天）来解决问题；

- 仅对范围内的系统进行测试，并尊重范围之外的系统和活动；

- 如果漏洞导致意外的数据访问：请将您访问的数据量限制为有效演示概念验证所需的最小值；如果您在测试期间遇到任何用户数据，例如个人身份信息 (PII)、个人医疗保健信息 (PHI)、信用卡数据或专有信息，请立即停止测试并提交报告；

- 您只应与您拥有的测试账户进行互动，或获得账户持有人的明确许可；并且

- 禁止敲诈勒索。

## 官方渠道

请通过 <security@bringyour.com> 报告安全问题，并提供所有相关信息。您提供的详细信息越多，我们就越容易分类和修复问题。

## 安全港

在进行漏洞研究时，根据本政策，我们认为在本政策下进行的研究是：

- 获得有关任何适用的反黑客法律的授权，我们不会因您意外、善意违反本政策而对您发起或支持法律行动；

- 获得有关任何反规避法律的授权，并且我们不会因规避技术控制而向您提出索赔；

- 免受我们的服务条款（TOS）和/或可接受使用政策（AUP）中可能干扰开展安全研究的限制，并且我们在有限的基础上放弃这些限制；以及

- 合法、有利于互联网整体安全并诚实守信。

我们一如既往地希望您遵守所有适用法律。如果第三方对您提起法律诉讼，而您已遵守本政策，我们将采取措施，让大家知道您的行为符合本政策。

如果您有疑虑或不确定您的安全研究是否符合此政策，请在继续操作之前通过我们的官方渠道之一提交报告。

> 请注意，安全港仅适用于参与此政策的组织控制下的合法索赔，并且该政策不约束独立的第三方。