**Englische Version: Um die Einführung eines eigenen BugBounty-Programmes zu erleichtern, stellt die IHK München und Oberbayern Muster zur Verfügung.**

**Versionierung des Dokumentes:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Datum** | **Bearbeiter** | **Änderungen** | **Vertraulichkeitsstatus** |
| 1.0 | 24.07.2023 | Bernhard Kux, IHK München und Oberbayern | Erstversion | Öffentlich |

**Rechtliche Hinweise zur Benutzung:  
Bitte beachten Sie für die Verwendung des hier bereit gestellten Musters Folgendes:**

* Das Muster wurde mit größter Sorgfalt erstellt, erhebt aber keinen Anspruch auf Vollständigkeit und Richtigkeit.
* Das Muster ist als Formulierungshilfen zu verstehen und soll nur eine Anregung bieten, wie die eigene Aktivität zur IT-Sicherheit sachgerecht gestaltet werden kann. Dies entbindet Sie jedoch nicht von der sorgfältigen eigenverantwortlichen Prüfung.
* Das Muster ist nur ein Vorschlag für eine mögliche Gestaltung. Sie können auch andere Formulierungen wählen. Vor einer Übernahme des unveränderten Inhaltes muss daher im eigenen Interesse genau überlegt werden, ob und in welchen Teilen gegebenenfalls eine Anpassung an die konkret zu gestaltende Situation erforderlich ist.
* Auf diesen Vorgang hat die Industrie- und Handelskammer keinen Einfluss und kann daher naturgemäß für die Auswirkungen auf keine Haftung übernehmen. Auch die Haftung für leichte Fahrlässigkeit ist grundsätzlich ausgeschlossen.

Um das Muster weiter zu verbessern sind wir für Anmerkungen und Verbesserungsvorschläge sehr dankbar.   
Bitte schicken Sie diese an Bernhard Kux, [kux@muenchen.ihk.de](mailto:kux@muenchen.ihk.de)

**Muster:**

**Indications of Vulnerabilities: YOUR\_COMPANYNAME BugBounty Program**YOUR\_COMPANYNAME offers a wide range of digital services. The security of data and processes is of the highest priority. However, despite our best efforts, these digital services may still contain vulnerabilities that are not yet known to the YOUR\_COMPANYNAME. Therefore, we are very grateful for any indications of Vulnerabilities!  
  
Please note: Searching for vulnerabilities may possibly constitute a criminal offense. To avoid legal difficulties, we kindly ask you to adhere to the following rules.

## What is the YOUR\_COMPANYNAME BugBounty Program? "BugBounty programs" are important tools for improving the security of digital services, as they encourage a community of "ethical hackers" or security researchers to help uncover potential vulnerabilities before they can be exploited by malicious actors. The "YOUR\_COMPANYNAME BugBounty Program" is an initiative by YOUR\_COMPANYNAME to reward individuals who uncover and report errors, security vulnerabilities or "bugs" in the YOUR\_COMPANYNAME digital services. The term "Bug Bounty" means "bounty for bugs". The reward, also known as "bounty", varies based on the severity and type of the uncovered failure. Anyone who adheres to the rules stated below can participate in the YOUR\_COMPANYNAME BugBounty Program.

## Which digital services are included in the YOUR\_COMPANYNAME Bug Bounty Program? The following domains (including any existing subdomains) are relevant for the Bug Bounty Program of the YOUR\_COMPANYNAME:

* List of Domains of YOUR\_COMPANYNAME
* …

## Some of the above mentioned domains redirect to websites not administered by the YOUR\_COMPANYNAME. In these cases, the YOUR\_COMPANYNAME BugBounty program only covers the domain managed by the YOUR\_COMPANYNAME, but not the online service (e.g. basisbox.de). Please note that digital services not included in the above list are not part of the YOUR\_COMPANYNAME BugBounty Program. Any Bug Hunting within those domains may potentially be considered unlawful and could be penalized accordingly.

## Rules for the Bug Bounty Program! Participation in the YOUR\_COMPANYNAME BugBounty Program requires strict adherence to the following general rule: No harm must be done to the YOUR\_COMPANYNAME due to activities within the framework of the YOUR\_COMPANYNAME BugBounty Program. This means:

* While searching for vulnerabilities, the availability, confidentiality, and integrity of the data and processes of the YOUR\_COMPANYNAME must not be compromised. Therefore, please do not execute any phishing mailing, DDoS, or brute force tests, etc. Do not change any data.
* No backdoors or similar programs, which allow permament access, must be installed.
* Identified vulnerabilities will be published only after they have been rectified by the YOUR\_COMPANYNAME.

Furthermore, the following applies:

* Only the initial report of a vulnerability is eligible for a bug bounty payout.
* Current and former employees of the YOUR\_COMPANYNAME, as well as service providers and suppliers, are not eligible to participate in the BugBounty Program.
* The YOUR\_COMPANYNAME determines the payout amount (see 4.). A payout can only be made if the participant in the YOUR\_COMPANYNAME BugBounty Program provides an appropriate invoice that complies with the applicable sales taxation.

**4. This is how you can send us a vulnerability report**When making contact, please provide us with the following information:

* Exact domain on which you found the vulnerability.
* As many details as possible, so we can reproduce the vulnerability, facilitate our analysis and thus speed up the payout of the reward. For example, the IP number from which the tests were carried out, proof-of-concept sketches etc.

Please contact us via e-mail: bugbounty@MAILDOMAIN\_OF\_YOUR\_COMPANY

**5. What does the YOUR\_COMPANYNAME do with vulnerability reports?**The submitted vulnerability report is evaluated by the YOUR\_COMPANYNAME and classified into a category of criticality, which is determined by its potential for danger. Guidance is provided by the „Common Vulnerability Scoring System Calculator“ ( <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator> ), which can be used to categorize vulnerability reports.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vulnerability Classification** | **Low** | **Medium** | **High** | **Critical** |
| CVSS-Score | 0.1 - 3.9 | 4.0 - 6.9 | 7.0 - 8.9 | 9.0 - 10.0 |
| Bug Bounty (Net amount before sales tax) | up to 100 € | 100 – 500 € | 500 – 1.000 € | over 1.000 € |

In this regard, the YOUR\_COMPANYNAMEis particularly interested in vulnerabilities that allow unauthorized individuals to access, modify, or delete confidential data.

**Examples of relevant vulnerabilities** can be found at OWASP, ( <https://owasp.org/www-project-top-ten/> ) including the following:

* Cross-site request forgery (CSRF / XSRF) ( <https://de.wikipedia.org/wiki/Cross-Site-Request-Forgery> )
* persistent Cross-Site-Scripting (XSS) <https://www.enisa.europa.eu/topics/incident-response/glossary/cross-site-scripting-xss>
* SQL Injections ( <https://owasp.org/www-community/attacks/SQL_Injection> )

**The following submissions are not relevant for the YOUR\_COMPANYNAME BugBounty program and are not eligible for a Bounty payout:**

* General accessibility of digital services
* Phishing emails and similar threats, especially those that abuse the email addresses of the YOUR\_COMPANYNAME
* Vulnerabilities without proof of exploitability
* Vulnerabilities that only affect browsers which are outdated or only have limited security features
* Reports generated by scanners that do not provide specific and fully traceable references to a vulnerability
* Unused best practices in headers, SSL/TLS, DNS