**Payconiq**

***Coordinated Vulnerability Disclosure***

**Document Information**

|  |  |
| --- | --- |
| **Document ID** | PQI-SEC-POL-002 |
| **Classification** | Internal and external Use |
| **Registered on** | 14-04-2023 |
| **Last Modified on** | 21-07-2023 |
| **Business Owner** | CTO |
| **Author** | Vinit Patal |
| **Contact** | security@payconiq.com |
| **Version** | 1.0 |
| **Status** | Ready for PRC Approval |

**Document Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Change | Author |
| 14-04-2023 | 0.1 | Draft | Vinit Patil |
| 04-07-2023 | 0.2 | Review | Jeffry Laan |
| 21-07-2023 | 1.0 | Review | Approved by Campfire |

**Updated Changes**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Change | Author |
| 04-07-2023 | 0.3 | Cosmetic | Jeffry Laan |

Table of Contents

[1. Overview & Purpose 1](#_Toc1420060239)

[2. Authorization 2](#_Toc431319715)

[3. Guidelines 2](#_Toc969036237)

[4. Our Commitment 2](#_Toc1753409418)

[5. Test Methods 3](#_Toc431478900)

[5.1. Unauthorized 3](#_Toc2005634496)

[5.2. Out Of Scope 3](#_Toc1614952357)

[5.3. Assets in Scope 3](#_Toc2033650145)

[5.4. Severity Calculation 4](#_Toc709505353)

[5.5. Awards 4](#_Toc1179712669)

[6. Policy Compliance 4](#_Toc1275820291)

[6.1. Control Measure 5](#_Toc1031856732)

[6.2. Exceptions 5](#_Toc1508792109)

[6.3. Non-Compliance 5](#_Toc1687170091)

[7. Annex 5](#_Toc1644634529)

# Overview & Purpose

Payconiq highly values the security of our systems and platform, and the effort security researchers put in to improve it.

Even though we continuously take the utmost care of our systems, it might just happen that you have found a vulnerability or weakness. In order to resolve this swiftly, we kindly request that you follow this guideline to report it to us.

Only Payconiq owned and administered services are in the scope of this policy. That includes payconiq affiliated web domains like payconiq.com and other payconiq domains, except payconiq.be

# Authorization

If the security researcher makes a good faith effort to comply with this policy during the security research, Payconiq will consider the research they perform to be authorized, Payconiq will work with the researcher to understand and resolve the issue quickly, and *Payconiq* will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.

# Guidelines

Under this policy, "research" means activities in which you:

* Send the details in an email to [cvd@payconiq.com](mailto:cvd@payconiq.com) .
* Make a good faith effort to prevent privacy violations, destruction of data and interruption/degradation of any of our services.
* Do not download, read, share or modify any information or data that does not belong to you.
* Do not share details that relate to the vulnerability with others until fully mitigated.
* Destroy all remaining private data, resulting from your research, immediately after reporting the vulnerability.
* Do not use any research attempt that involves breaching or attacking physical security or the use of social engineering, DOS, spam, fishing or any involvement of third parties.
* Provide details of the vulnerability so that we can reproduce it, including a Proof of Concept (POC), information on the URL, endpoint and IP address, and other necessary information.
* Allow us to respond and mitigate within a reasonable amount of time.

Note that you will still have to abide by any applicable law and that potential law enforcement consequences are not within our control.

# Our Commitment

We will put effort to

* respond within 3 business days
* handle your report and personal details in a confidential manner
* keep you posted on the progress
* reward you in cases of serious and unknown vulnerabilities, containing enough information to swiftly reproduce

Note that people who are in any way involved with designing, regulating, auditing, creating or maintaining our services or platform are not eligible for reward.

# Test Methods

## Unauthorized

The following test methods are not authorized:

* Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
* Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing

## Out Of Scope

The following is specifically out of scope and not eligible for reward either:

* reports without clear description of potential exploits
* vulnerabilities concerning other sites and domains than the ones affiliated with Payconiq
* CSFR issues on public and non-authenticated web pages
* The absence of best practice security headers, like HSTS, HttpOnly, CSP, XSS or click-jacking related headers
* possible old/vulnerable third party/off-the-shelf systems without evidence that they are exploitable and impacting our platform security
* TLS/SSL related configuration issues
* payconiq.be and Payconiq by Bancontact mobile app

## Assets in Scope

The following assets are eligible to be included in the program scope.

|  |  |  |
| --- | --- | --- |
| Type | Identifier | Eligible up to |
| Domain | api.ext.payconiq.com/v2/\* | Critical severity |
| Domain | api.ext.payconiq.com/v3/\* | Critical severity |
| Domain | app.ext.payconiq.com | Critical severity |
| iOS: | .ipa com.payconiq.ext | Critical severity |
| Android: | .apk com.payconiq.customers.external | Critical severity |
| Domain | bankapi.ext.payconiq.com | Critical severity |
| Domain | signature.ext.payconiq.com | Critical severity |
| Domain | portal.ext.payconiq.com | Critical severity |
| Domain | ext.payconiq.com | Critical severity |

## Severity Calculation

The Severity calculation shall be based on CVSS3 technical vulnerability scoring system as mentioned in below table:

|  |  |
| --- | --- |
| Severity | Base Score Range |
| Low | 0.1 - 3.9 |
| Medium | 4.0 - 6.9 |
| High | 7.0 - 8.9 |
| Critical | 9.0 - 10.0 |

## Awards

The following bounty awards shall be adapted in the payout.The finance team shall payout the bounty to the security researchers after the report verifications by the Security Team. The payouts in monetary forms to be made using bank and wire transfers as feasible to the locations where the Security Researcher belongs.

|  |  |
| --- | --- |
| Severity | Bounty |
| Low | $200 |
| Medium | $500 |
| High | $1500 |
| Critical | $4000 |

# Policy Compliance

## Control Measure

The Information Security Officer will verify compliance to this policy through various methods, including but not limited to, periodic system and log analysis, reports, internal and external audits, penetration tests, and testing employees with internal tools.

## Exceptions

Any exception to Rules of the policy shall be approved by Business Owner of the policy. Any other exception to the policy requires approval by both PQS and PQI Management Board.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Annex

Following legal terms shall be included in the program details.

**Program Terms**

Please be aware that your participation in the Vulnerability Disclosure is voluntary and subject to the terms set forth on this page. When submitting a vulnerability to Payconiq you acknowledge that you have read and agreed to these Policy Terms.

These Policy Terms supplement the terms of and any other agreement which you may have entered into with Payconiq (collectively “Payconiq Agreements”) insofar these apply, including but not limited to the Payconiq Consumer Terms and Conditions. If any inconsistency exists between the terms of the Payconiq Agreements and these Program Terms, these Policy Terms will control, but only with regard to the Vulnerability Disclosure Program.

To encourage responsible disclosures, Payconiq commits that, if we conclude, in our sole discretion, that a disclosure respects and meets all the guidelines of these Policy Terms and the Payconiq Agreements, Payconiq will not bring a private action against you. Please see the section on “Safe Harbour” for more information. When you are investigating one of our systems, bear in mind the proportionality of the attack. As part of your research, do not modify any files or data, including permissions, and do not intentionally view or access any data beyond what is strictly needed to prove the existence of the vulnerability.

**Disclosure**

By providing a Vulnerability Report or agreeing to the Program Terms, you agree that you may not publicly disclose your findings or the contents of your Vulnerability Report to any third parties in any way without Payconiq's prior written approval. Failure to comply with the Program Terms will result in immediate disqualification from the Vulnerability Disclosure Program and ineligibility for receiving any Bounty Payments.

**Termination**

In the event (i) you breach any of these Policy Terms or the terms and conditions of the Payconiq Agreements; or (ii) Payconiq determines, in its sole discretion that your continued participation in the Program could adversely impact Payconiq (including, but not limited to, presenting any threat to Payconiq's systems, security, finances and/or reputation) Payconiq may immediately terminate your participation in the Program and disqualify you from receiving any Bounty Payments.

**Confidentiality**

Any information you receive or collect about Payconiq or any Payconiq user through the Program (“Confidential Information”) must be kept confidential and only used in connection with the Program. You may not use, disclose or distribute any such Confidential Information, including, but not limited to, any information regarding your Submission and information you obtain when researching the Payconiq sites, without Payconiq's prior written consent.

**Indemnification**

In addition to any indemnification obligations you may have under the Payconiq Agreements, you agree to defend, indemnify and hold Payconiq, Payconiq International S.A their subsidiaries, shareholders, affiliates and the officers, directors, agents, joint ventures, employees and suppliers, harmless from any claim or demand (including attorneys’ fees) made or incurred by any third party due to or arising out of your breach of these Program Terms and/or your improper use of the Program.

**Changes to Program Terms**

The Program, including its policies, is subject to change or cancellation by Payconiq at any time, without notice. As such, Payconiq may amend these Program Terms and/or its policies at any time by posting a revised version on our website. By continuing to participate in the Program after Payconiq posts any such changes, you accept the Program Terms, as modified.

**Bounty**

You may be eligible to receive a monetary reward (“Bounty”) if: (i) you are the first person to submit a site or product vulnerability; (ii) that vulnerability is determined to by a valid security issue by Payconiq's security team; and (iii) you have complied with all Program Terms.

Bounties, if any, will be determined by Payconiq, in Payconiq's sole discretion. In no event shall Payconiq be obligated to pay you a bounty for any Vulnerability Report. All Bountiesshall be considered gratuitous.

Payconiq retains the right to determine if the bug submitted to the Program is eligible. All determinations as to the amount of a bounty made by the Payconiq are final. Bounty ranges are based on the classification and sensitivity of the data impacted, ease of exploit and overall risk to Payconiq customers, Payconiq brand and determined to be a valid security issue by Payconiq's security team.

Payconiq will determine all Bounties based on the risk and impact of the vulnerability.

**Safe Harbor**

Any activities conducted in a manner consistent with this policy will be considered authorized conduct and we will not initiate legal action against you. If legal action is initiated by a third party against you in connection with activities conducted under this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

If you discover a weakness and investigate it, you might perform actions that are punishable by law. If you observe the rules for reporting weaknesses in our IT systems, we will not report your offence to the authorities and will not submit a claim.

It is important for you to know, however, that the public prosecutor’s office – not Payconiq – will decide whether or not you will be prosecuted, regardless of whether we report your offence to the authorities. We cannot promise that you will not be prosecuted if you commit a punishable offence when investigating a weakness and we advise you to act in accordance with the relevant guidelines from the National Cyber Security Centre of the Netherlands on coordinated vulnerability disclosures.