TERMS, CONDITIONS AND CODE OF CONDUCT
PUBLIC INTRUSION TEST (PIT)

The Swiss Post e-voting system adheres to the highest security and quality standards and has already undergone multiple security testing campaigns. Our system is ready to meet the challenge of a public intrusion test (PIT).

We are therefore inviting security researchers to register and participate in our PIT programme and to use their skills to search for unknown weaknesses and vulnerabilities. They will receive financial compensation for their security findings.

1. Introduction

The goal of the PIT is to promote security and trust in the Swiss Post e-voting system. Furthermore, the PIT is a requirement by the Swiss government and the cantons and is therefore co-organized and supervised by the Swiss government and a specific group of Swiss cantons.

SCRT SA is your single point of contact when challenging Swiss Post's next generation e-voting system. SCRT acts as contractor on behalf of the Swiss Confederation and the cantons. SCRT runs the online portal where you can register and submit your findings. SCRT is mainly responsible for registration, issue management, classification of findings, first level support and any queries you have regarding the PIT.

The scope of the PIT is strictly limited to the dedicated e-voting test system that is modelled 1:1 on the productive systems. Any other Swiss Post services and infrastructures and any services and infrastructures of its customers, suppliers and any other public or private entities are off-limits.

A separate source code access programme accompanies the PIT. For source code access, sign up to the source code access programme (https://www.swisspost.ch/evoting-sourcecode)

Swiss Post have elaborated these Terms, Conditions and Code of Conduct (TC&CoC) with representatives of the Swiss Federal Chancellery, representatives of the state chancelleries of the cantons and with support of experts in the field.

2. Agreement with the TC&CoC

By signing up to the PIT programme, you agree to be bound by these TC&CoC for the duration of the PIT programme and thereafter. If you do not agree with the rules, do not register. We encourage you to provide feedback, but unfortunately cannot accept your participation at this time.

If you sign up to the source code access programme and there is a conflict between the E-Voting Solution Source Code Access Agreement and the TC&CoC, the latter shall take precedence.

3. Organization of the PIT programme

- The PIT programme is time-limited. It lasts for four weeks, i.e. the same duration as a Swiss public federal vote.
- SCRT serves as single point of contact for participants.
- The organizers of the PIT will make their best efforts to provide timely feedback on a submitted finding.

4. Registration policy

- Registration is mandatory for participation in the PIT. You can register via https://www.onlinevote-pit.ch (website operated by SCRT). If participating as a team, all members need to register separately.
- Registration will allow SCRT to provide you with your voting cards – required for submitting a vote – which you can use for your research.
- Registration for the PIT programme is open without restrictions to everybody willing to be bound by the TC&CoC as outlined in this document.
- The organizers will only use the registration data in order to ensure the proper running of the programme and compliance with the TC&CoC.

5. Testing policy

5.1 General

Swiss Post provides an e-voting system dedicated to the PIT programme. Participants will receive access to the dedicated e-voting test system. Even though participants may team up with other participants, the means of access and the voting cards are personal, and the original receiver will be held accountable for any use in conflict with the TC&CoC. All interactions with the system will be logged.

Participants are permitted to perform any tests and investigations on the dedicated e-voting system as long as they act in good faith and respect the scope of the test provisions (see par. 5.2).

Participants who have found or believe they have found a vulnerability are obliged to submit a report to the online portal operated by SCRT. Submissions may be compensated if the provisions of the compensation policy (see par. 6) are duly met. The publication of any vulnerability or other test findings must comply with the responsible disclosure policy (see par. 7).

5.2 Scope of the test

The scope of the PIT is limited to the public-facing services of the dedicated e-voting test system and its e-voting backend systems.

The following public-facing services are part of the programme:

*** pit.evoting-test.ch (voter access used by voter)**
*** pit-admin.evoting-test.ch (admin access used by secure data manager (SDM))**

The public-facing services are connected to backend e-voting systems that are also in-scope, but need to be accessed through the public-facing service.

Backend systems that are not clearly identifiable as part of the dedicated e-voting test system are not in-scope. If you are unsure, then please stop your operation and ask SCRT, (ask first). If any of your further operations are stopped due to a negative response, this will be taken into account when determining a possible award (see chapter compensation).

Attacks and scans that can harm other operations and services of Swiss Post and its subsidiaries are not in-scope, and strictly forbidden.

5.3 Out-of-scope

Everything that is not defined as in-scope (see par. 5.2), is out-of-scope by default.

In particular, the following items are out-of-scope:

- All attacks that fall in the broad denial of service and resource starvation categories.
- Social engineering attacks on operators or employees of Swiss Post, its subsidiaries and contract partners such as Scytl and SCRT.
- Attacks on the set-up of the vote and the clean-up after tallying of the e-voting results.
- Physical attacks on people, buildings and devices.
- Attacks that assume that a voter is not following the official instructions (e.g. hiding the return codes is out-of-scope).
- Attacks that exploit the client in order to spy on the vote of the individual voter (client-side privacy of the vote). Voter privacy attacks based on the use of keyloggers, screen recorders or other mechanisms for capturing the behaviour of the voter in the device.
- Attacks on the systems of SCRT.
- Attacks on administrative and surrounding systems that are not used for e-voting exclusively (this includes DNS, NTP, routers, systems of the ISP, etc.).
- Attacks on the systems used to distribute the e-voting cards electronically (the productive e-voting system distributes the voting cards physically on paper. For the PIT programme, the voting cards are distributed in digital format to eliminate registration via postal address).

6. Compensation policy

6.1 General

- **The maximum amount potentially compensated to PIT participants is CHF 150,000.**
- A security finding that matches a qualifying vulnerability (see par. 6.2) and that has been submitted according to the Submission Rules (see par. 6.4) is eligible to receive financial compensation within the limits of this compensation policy. Only participants who fully respect the provisions of the TC&CoC are eligible for compensation.
- People who work or have worked as employees, consultants or contractors for Swiss Post, Swiss Federal Chancellery, the cantons, SCRT and Scytl in the field of or in connection with e-voting are not eligible for compensation.
- Swiss Post will decide at their own discretion on the amount of compensation, and will commit to a minimum amount based on the category a finding falls under (see par. 6.2). It is not possible to appeal the decision.
- Duplicate findings will not be compensated. Only the initial submitter will be compensated (first come, first served).
- Swiss Post will make an effort to pay out the compensation in good time.
- If the definition of the scope prevents you from exploiting proven server-side vulnerabilities, this will be taken into consideration when calculating the compensation (e.g., you successfully pwn a server and you are ready for lateral movement, yet you do not exploit surrounding systems because they are out-of-scope).

6.2 Qualifying vulnerabilities

Findings are qualified in one of several categories based on their severity:

- **Manipulation that goes undetected by the voter and the system (between CHF 30,000 and CHF 50,000)**
  - Manipulation of individual votes after being recorded in the ballot box
    (without being detected by the proofs and logs generated by the e-voting protocol)
  - Manipulation of the tallying process (manipulating the results) without voters and auditors detecting it

- **Manipulation that goes undetected by the voter but not by the system (min. CHF 20,000)**
  - Manipulation of individual votes while maintaining universal verifiability mechanism (detected by trusted auditor)
  - Modifying the results of the election without being detected by a voter

- **Vote corruption (min. CHF 5,000)**
  - A vote is stored in the ballot box and that vote cannot be decrypted
  - A vote is stored in the ballot box in a way that gives the voter an unfair advantage
  - Destruction of the electronic ballot box

- **Voting privacy outside the voting client (min. CHF 10,000)**
  - The privacy of a voter is broken (identity of who voted) on the server
  - The privacy of a vote is broken (what he or she voted) on the server

- **Intrusion (min. CHF 1,000)**
  - Intrusion into one of the servers (shell access)
  - Ability to execute arbitrary code on one or multiple servers
  - Ability to execute arbitrary code on one or multiple control components

- **Best practices (min. CHF 100)**
  - The configuration of a server or a service does not follow best practices of the security industry

6.3 Non-qualifying vulnerabilities

Findings are non-qualified if they are out of scope or if they are known and accepted characteristics of the e-voting system. The following is a non-comprehensive list of examples for non-qualifying vulnerabilities:

- Client-side hiding the return codes
- Stopping the voting session before sending the confirmation code

6.4 Submission Guidelines

- Submissions of vulnerabilities will only be accepted from registered participants.

- Vulnerabilities must be submitted exclusively through the SCRT submission portal (https://www.onlinevote-pit.ch).

- Submissions to other parties or through other channels are not allowed.

- If submissions are considered incomplete or insufficient, further information will be requested. Submissions can be rejected for formal reasons.

- If a submission is rejected (either incomplete on formal grounds or does not qualify), and you want to publish it, please confirm the date with us.

Submissions must contain:

- A basic description of the issue in question
- A tentative classification of the issue according to the categories given above
- A step-by-step guide that will allow the finding to be reproduced

Submissions should contain:

- Accompanying evidence, e.g. screenshots, videos, proof of concept code, dumps, etc.

7. Responsible disclosure policy

- This PIT programme follows a "responsible disclosure" policy.
- Participants / researchers are allowed to publish their findings following a publication date agreed with the organizers. This date will be 45 days after the initial confirmation of the reported finding at the latest.
- The organizers reserve the right to publish findings first and allow the participants to publish after Swiss Post.
- When findings are published, the original reporter of the finding will be credited. However, it is possible to request to remain anonymous or to use a pseudonym.

8. Behaviour of the participant

Besides the legal constraints as defined by the TC&CoC, there are also certain standards of behaviour that the organizers expect participants to follow and that they must comply with:

- No abusive language or harassment: we will not engage in and we will not tolerate any form of threats, profanity and hateful speech, discrimination based on ethnicity, nationality, religion, sexual or gender identity or orientation, as well as age, level of experience or personal appearance.
- No duplicate account abuse or duplicate registration.
- Use only official communication channels. Participants shall refrain from using any communication channel outside of those defined in the TC&CoC or those offered to participants explicitly by SCRT.
- Do not engage in any form of reputation framing or activities that create an unfair gain in reputation or rewards.

9. Consequences of complying with the TC&CoC

- Swiss Post will not take civil action or file a complaint with law enforcement authorities against participants for accidental, good faith violations of the TC&CoC.
- Swiss Post interprets activities by participants that comply with the TC&CoC as authorized access under the Swiss Penal Code. This includes Swiss Penal Code paragraphs 143, 143^{a} and 144^{a}.
- Swiss Post will not file a complaint against participants for trying to circumvent the security measures deployed in order to protect the e-voting services in-scope as outlined above.
- If legal action is initiated by a third party against a participant and the participant has complied with the TC&CoC as outlined in this document, Swiss Post and SCRT will take the necessary measures to make it known to the authorities that such participant's actions have been conducted in compliance with this policy.
- Any non-compliance with the TC&CoC may result in exclusion from the PIT programme. For minor breaches, a warning may be issued. For severe breaches, the organizers reserve the right to file criminal charges.

10. Entire Agreement

- This Agreement is the entire agreement between Swiss Post and the participant concerning the public intrusion test.
- Participants will only be allowed to participate if they accept these TC&CoC when registering for the public intrusion test as defined above.

11. Applicable law and jurisdiction

- This Agreement is governed by and construed in accordance with the laws of Switzerland.
- Any dispute arising out of or relating to the Agreement shall be submitted and finally resolved by the courts of Berne, Switzerland.

Post CH Ltd
Wankdorfallee 4
3030 Berne
www.post.ch/pit