Public QR Security Standard

PQSS 1.0

Published	2026-11-11
Publisher	EZQR (Canada), ezqr.ca
This version	https://pqss.ca/1.0
Comments	feedback@pqss.ca

© 2026 EZQR. This document is licensed under the Creative Commons Attribution 4.0 International licence (CC BY 4.0, creativecommons.org/licenses/by/4.0/). You may copy and adapt it, including in your own procedures, if you credit PQSS 1.0 and say what you changed.

There is no PQSS certification. Organizations assess themselves against this standard.

Contents

0. Purpose

1. Scope

2. Terms

3. Requirements

- Requirement 1: Keep a placement register
- Requirement 2: Assign a risk tier and an inspection schedule
- Requirement 3: Inspect safely
- Requirement 4: Respond to a mismatch
- Requirement 5: Make your codes easier to check
- Requirement 6: Keep records
- Requirement 7: Assign responsibility

4. Self-assessment

5. Changes and versions

6. Relationship to other guidance

Appendix A: Example inspection round

Appendix B: Tools

0. Purpose

Anyone can print a QR code on a sticker and put it over a real one. People who scan the fake are taken to a site of the attacker's choosing, often a copy of a payment or login page. This is called *quishing*. It targets places where people expect to scan and pay: parking meters, EV chargers, transit, utility notices, restaurant tables.

Advice to the public, such as the Canadian Centre for Cyber Security's *Security considerations for QR codes* (ITSAP.00.141), teaches people to scan with care. PQSS covers the other side: **what the organization that posted the codes should do.**

PQSS is a **detection** standard. It makes sure you uncover and resolve quishing on a known schedule, respond in a known way, and keep a record. Inspections cut down how long a fake stays up. They can't bring that time to zero.

The key words MUST, MUST NOT, SHOULD and MAY are used as described in RFC 2119.

1. Scope

PQSS applies to any organization that **posts QR codes in places the public can physically reach**: on signs, meters, machines, tables, walls, vehicles, doors or screens.

In scope:

- Fixed placements: signs, decals, plaques, meters, kiosks, table tents.
- Semi-fixed placements that stay up for more than 7 days: posters, window decals, event signage.
- QR codes shown on physically reachable screens (a sticker on a screen is still a sticker).

Out of scope:

- Codes on material handed to one person: receipts, mailers, business cards, tickets, packaging. These have no "placement" for someone to cover.
- Codes shown only on screens the public can't touch.
- Product authentication and anti-counterfeiting.
- The QR symbology itself (see ISO/IEC 18004).

PQSS doesn't care which tool made a code, whether the code is static or dynamic, or what it links to.

2. Terms

- **Placement:** one physical spot where a QR code is posted. One code printed in 300 places is 300 placements.

- **Expected content:** the exact data a placement's code should decode to (for a web link, the full address including the domain).
- **Inspection:** a person physically visiting a placement and checking its code against the expected content.
- **Inspection reader:** a scanning tool that **shows** what a code decodes to, and ideally compares it with the expected content, **without opening it** (no browser launch, no app action).
- **Mismatch:** a placement whose code doesn't decode to its expected content.
- **Inspection period:** the time window in which every placement of a given tier must be inspected once.
- **PQSS lead:** the person accountable for the organization's PQSS program.

---

3. Requirements

Requirement 1: Keep a placement register

1.1 The organization MUST keep a register of every in-scope placement, with at least: a unique ID, a location description a stranger could follow ("Meter 1142, north side of Queen St W at Bathurst"), the expected content, the risk tier (Requirement 2) and the date it was posted.

1.2 Placements MUST be added to the register before or on the day they are posted, and marked removed within 30 days of being taken down.

1.3 The register MUST be checked against reality at least once a year. Placements found that aren't on the register MUST be added or removed.

1.4 Placements SHOULD have map coordinates where practical.

Requirement 2: Assign a risk tier and an inspection schedule

2.1 Each placement MUST get one tier:

Tier	The code leads to…	Examples	Inspection period
High	Payment, login, account access, or collection of financial or government ID details	Parking, EV charging, tolls, utility bills, donations, tips, pay-at-table	Every **31 days**
Medium	Collection of other personal information, or ordering	Sign-up and contact forms, surveys, booking, menus with ordering	Every **92 days**
Low	Information only	Menus without ordering, maps, product information, social links	Every **183 days**

2.2 If unsure, choose the higher tier.

2.3 If what the code leads to changes (e.g. a menu gets ordering), the tier MUST be reviewed at the same time.

2.4 A placement MUST be inspected **outside its schedule** within 2 business days (High) or 5 business days (Medium, Low) of any report from staff or the public that it looks altered, scans strangely, or led somewhere unexpected.

2.5 After any mismatch, Requirement 4.2 sets the follow-up inspections.

2.6 A placement recorded as missed (6.2) MUST be inspected within 2 business days (High) or 5 business days (Medium, Low) after its period ends. Its next period starts from the date of that inspection.

Requirement 3: Inspect safely

3.1 Every placement MUST be inspected in person at least once in each of its inspection periods.

3.2 Inspections MUST use an inspection reader. The inspector MUST confirm that the decoded content matches the expected content exactly, including the domain. **An ordinary phone camera that opens the link does not meet this requirement:** a fake code would take the inspector to the attacker's site, and a near-copy domain is easy to miss in a quick glance.

3.3 The inspector MUST also check the placement by eye and by touch for a sticker on top of the original, raised or lifting edges, misalignment, a second code nearby, or damage. A placement that has been physically altered MUST be treated as a mismatch even if it decodes correctly.

3.4 Inspectors MUST NOT open, visit or test the content of a mismatched code on any device.

3.5 A placement that can't be read MUST be recorded as failed and replaced or repaired. "Unreadable" doesn't count as inspected.

3.6 Inspections SHOULD record the inspector's location or other evidence that the check happened on site, not from a photo.

3.7 If a placement isn't where the register says, the inspector MUST check the spot and its surroundings for any code posted in its place; a substitute is a mismatch (Requirement 4). A placement confirmed gone MUST be recorded as **gone**, which counts as inspected for that period, and within 30 days the genuine code MUST be restored or the placement marked removed (1.2). If the inspector can't find the spot, the placement MUST be recorded as **missed**, not gone, and its location description corrected.

Requirement 4: Respond to a mismatch

4.1 On finding a mismatch, the inspector MUST, as soon as it's safe: photograph it, then remove or cover the fake code (or the whole placement if the fake can't be removed). The placement MUST stay out of service until a genuine code is restored.

4.2 The organization MUST inspect every other placement **at the same site** the same day, and every **High** placement of the same kind (e.g. all meters) within 2 business days.

4.3 The organization MUST report the incident to the **Canadian Anti-Fraud Centre** and SHOULD report it to local police and the **Canadian Centre for Cyber Security**. Organizations outside Canada report to their national equivalents.

4.4 If people may have entered payment or personal information on the fake site, the organization SHOULD warn the public where they would see it: on site, on its website, and through its usual customer channels.

4.5 The organization SHOULD report the fake address to the web browser makers' phishing-report services so browsers start warning people who visit it.

Requirement 5: Make your codes easier to check

These are SHOULD-level and don't replace inspection.

5.1 Placements SHOULD show a short web address or instruction next to the code, so people can reach the same place without scanning (ITSAP.00.141 advises typing addresses where possible).

5.2 The organization SHOULD publish on its website the domain(s) its QR codes use, so people and staff can check what a genuine code looks like.

5.3 High placements SHOULD use mounting or lamination that shows tampering, or that makes it hard to stick something flat over the code.

5.4 Placements SHOULD say how to report a code that looks altered.

Requirement 6: Keep records

6.1 Each inspection MUST be recorded with the placement ID, date and time, inspector, result (genuine, mismatch, altered, unreadable, or gone) and any action taken.

6.2 A placement that wasn't inspected in its period MUST be recorded as **missed**. It MUST NOT be left out or counted as passed.

6.3 Each mismatch MUST be recorded as an incident with its photo, its reports (Requirement 4.3) and the date the genuine code was restored.

6.4 Inspection and incident records MUST be kept for at least 12 months.

Requirement 7: Assign responsibility

7.1 The organization MUST name a PQSS lead.

7.2 Inspectors MUST be briefed on Requirements 3.2–3.4 and 4.1 before their first inspection.

7.3 The PQSS lead MUST review the register, missed inspections and incidents at least every quarter.

---

4. Self-assessment

There is **no PQSS certification**, and no organization, including the publisher, certifies or audits PQSS compliance. Organizations assess themselves.

An organization meets PQSS 1.0 for a period if it can answer **yes** to every question below for that period, with records to show it.

#	Question	Req.
1	Is every in-scope placement in the register, with ID, location, expected content and tier, and was every gone placement restored or marked removed within 30 days?	1.1–1.2, 3.7
2	Has the register been checked against reality in the last 12 months?	1.3
3	Was every placement inspected in person within its tier's period?	2.1, 3.1
4	Was every reported concern and every missed placement inspected within its deadline?	2.4, 2.6
5	Did every inspection use an inspection reader, plus a physical check?	3.2–3.3
6	Was every mismatch removed, followed up and reported as required?	4.1–4.3
7	Are missed inspections recorded as missed?	6.2
8	Are records kept for 12 months or more?	6.4
9	Is there a named PQSS lead, and were inspectors briefed?	7.1–7.2
10	Did the PQSS lead review the program in each quarter?	7.3

Making a statement. An organization that meets PQSS MAY say so in these words: *"We self-assess against PQSS 1.0, the Public QR Security Standard. Last assessed: [date]."* It MUST NOT call itself "PQSS certified" or suggest a third party has verified it.

5. Changes and versions

PQSS uses version numbers. A minor version (1.1) clarifies wording or adds SHOULD-level guidance. A major version (2.0) changes MUST-level requirements. A self-assessment always names the version it used. Feedback and proposed changes: feedback@pqss.ca.

6. Relationship to other guidance

- **ITSAP.00.141, *Security considerations for QR codes*** (Canadian Centre for Cyber Security): guidance for people who **scan** QR codes. PQSS is the counterpart for people who **post** them, and its reporting steps follow the same channels.
- **PCI DSS v4.0, Requirement 9.5.1.2:** card-payment devices are inspected on a schedule for tampering and substitution. PQSS applies the same approach to printed codes. PQSS isn't affiliated with the PCI Security Standards Council.

- **ISO/IEC 18004:** the QR code symbology. PQSS doesn't change how codes are encoded or printed.

Appendix A: Example inspection round

1. Open the register filtered to placements due this period. Sort by route.
2. At each placement: look and feel for overlays (3.3), then read with the inspection reader (3.2).
3. Genuine: record it and move on. Mismatch: without opening it, photograph it, remove it and record it, then start Requirement 4.
4. At the end of the period, record every uninspected placement as missed (6.2) and inspect it within 2 business days (High) or 5 (Medium, Low) (2.6).

Appendix B: Tools

PQSS can be met with a spreadsheet, a clipboard and a scanning app that shows codes without opening them. Software can automate the register, schedule, reminders, inspection reader and records.

The publisher's own implementation is **Code Census** by EZQR (ezqr.ca/code-census). Any tool or process that meets the requirements above is equally valid.