Terminal Security Staff Training

A free sample program and coverage roster · helps document PCI DSS v4.0.1 Requirement 9.5.1.3

Requirement 9.5.1.3 asks you to train the people who work around your payment terminals so that tampering and substitution get noticed and reported. It is short in the standard and easy to underestimate, and it is one of the requirements merchants most often have no evidence for — not because the training never happens, but because nobody wrote down who received it.

What the requirement is actually asking for

The standard names four things staff in a point-of-interaction environment should be trained to do. A program that covers these four, and can show who completed it, is answering the requirement directly:

- Verify the identity of any third party claiming to be repair or maintenance personnel before giving them access to a terminal.
- Never install, replace, or return a device without verification that it is legitimate and expected.
- Be alert to suspicious behaviour around devices — people attempting to unplug or open a terminal, or lingering at one without paying.
- Report suspicious behaviour, and any indication of tampering or substitution, to the right person.

Who needs it

Anyone whose work puts them near a card reader: cashiers and shift leads, forecourt and floor staff, bar and service staff, duty and store managers, and any contractor or agency worker doing the same job. Head-office staff who never touch a terminal generally do not. If someone can be standing next to a reader while a stranger opens it, they are in scope.

How often

The standard does not fix a cadence for 9.5.1.3 itself. Most programs align it with the security-awareness training cadence in Requirement 12.6.3 — on hire and at least once every twelve months — and refresh sooner after an incident or a change in how terminals are deployed. Confirm the cadence you intend to use with your assessor rather than assuming it.

What counts as evidence

An assessor is generally looking for four facts per person: who was trained, on what content, when, and how you know they received it. That is why the roster on page 3 has those four columns and nothing decorative. Delivery method matters less than the record — a fifteen-minute shift briefing that is signed for is better evidence than an hour-long course nobody logged.

Sample program outline

Six short modules · roughly 30–40 minutes total · adapt freely to your operation

Use this as-is, or as a skeleton for your own. Each module is written to be deliverable as a shift briefing by a manager who is not a security specialist. Timings are indicative.

Module 1 — Why terminals get targeted (4 min)

Set the context without theatrics. The goal is that staff understand the terminal is an asset someone wants access to, not that they feel frightened.

- A card reader is attacked because it is the point where card data exists in a readable form.
- Attacks are usually quick and quiet — minutes, in the open, during business hours.
- The person doing it will look like a customer, a technician, or a delivery driver.

Module 2 — What tampering looks like (6 min)

Show real hardware if you can borrow a retired terminal. Otherwise use photographs of your own devices as they should look.

- Overlays: a false keypad or card-slot fascia sitting on top of the real one. Usually a slightly wrong colour, height, or texture.
- Internal devices: fitted inside the housing. From the outside there is often nothing at all to see — which is why the seal, screw, and casing checks matter more than a visual sweep.
- Substitution: the whole terminal swapped for a prepared one. Only caught by checking the serial against your inventory.

Module 3 — The physical check (8 min)

Walk the six checks on a real terminal, with each person doing it once themselves. Muscle memory is the point; most tampering is found by touch.

- Seals · Labels · Serial · Casing · Wiring · Overlay — the same six every time, in the same order.
- Pull gently on the bezel and the keypad. An overlay usually lifts.
- Compare the serial on the device against the one recorded for that position, every time.
- A terminal is only a pass when all six checks pass.

Module 4 — Visitors and service calls (6 min)

This is the module that most often prevents an incident, and the one staff are least likely to have been told about.

- Nobody touches a terminal without an expected, scheduled work order — including people in branded clothing.
- Verify identity against the work order and against a phone number you look up yourself, never one the visitor supplies.
- A device is never accepted, installed, swapped, or handed back without that verification.
- It is always acceptable to make a visitor wait while a manager confirms. Say so explicitly — staff need permission to be the obstacle.

Module 5 — If you find something (5 min)

The instinct to fix it is the thing to train out. Preservation and escalation, in that order.

- Stop using the terminal. Do not remove, open, or clean anything.
- Photograph it as found, before anything moves.
- Tell the named person on your escalation list — name them in the training, do not say 'management'.
- Do not confront anyone. Note descriptions and timings instead.

Module 6 — Writing it down (4 min)

Close by showing the actual record your staff will complete, filled in once in front of them.

- Which device, who checked it, when, the outcome, and what was done about anything that was not a pass.
- An inspection that is not recorded cannot be evidenced later, and for an assessor it did not happen.

SkimGuard

Training coverage roster

Who was trained, on what, when, and how you know · one sheet per site

Keep one roster per site and add a row per person per session. The four columns an assessor asks about are the four that must never be blank: name, content and version, date, and the person's own acknowledgement.

SITE OR LOCATION

DELIVERED BY

PROGRAM / CONTENT VERSION

Name (print)	Role	Date	Delivery	Check passed	Next due	Signature

Delivery: in person · shift briefing · e-learning · written. Check passed: the short knowledge check, or the person's acknowledgement that they received and understood the content. Signature is the person's own — a manager signing on someone's behalf is not evidence that the person was trained.

Knowledge check and next steps

Five sample questions, and what to do once the roster starts filling up

Sample knowledge check

Five questions, verbally or on paper. The point is not to grade people — it is to produce a defensible record that the content landed. Answers in brackets.

- A technician in branded uniform says head office sent them to swap a card reader. There is no work order. What do you do? [Do not allow access. Verify with a manager and a number you look up yourself. It is fine to make them wait.]
- Name the six physical checks. [Seals, labels, serial, casing, wiring, overlay.]
- Five of six checks pass and the casing has a new gap. Is the terminal a pass? [No. All six must pass.]
- You find an overlay on a keypad mid-shift. What are your first three actions? [Stop using the terminal; photograph it as found; escalate to the named person. Do not remove it.]
- Why does the serial number get checked against the inventory? [Because a substituted terminal can look completely normal. The serial is what catches it.]

Once the roster starts filling up

A paper roster works well for one site. Across several sites the questions that get hard are the ones an assessor asks: who is overdue right now, what content version did each person actually receive, and how do you know a row was not added afterwards. Those are record-keeping problems rather than training problems, and they are where most programs come apart.

Staff training is included in every SkimGuard business tier

Terminal-security modules in 22 languages that your staff take in the app — or record your own program instead — with tracking of who is trained, who is overdue, and coverage per location, and an export of the record for your assessor. Meeting 9.5.1.3 usually means buying a separate training system; here it comes with the subscription. skimguard.io/pci-staff-training

The rest of the free set

- Printable terminal tamper inspection record — the six checks on one page, for a clipboard walk. skimguard.io/pci-terminal-inspection-log
- Payment device inventory template (CSV) — the 9.5.1.1 device list, spares included. skimguard.io/pci-device-inventory-template
- Inspection cadence assessment — a two-minute estimate of how often to inspect, with the written justification 9.5.1.2.1 expects. skimguard.io/poi-inspection-schedule-wizard

SkimGuard, Inc. is not a Qualified Security Assessor and does not perform PCI assessments. This pack is a free sample program and record template intended to help you document and evidence staff-training activity under PCI DSS v4.0.1 Requirement 9.5.1.3. It is not an attestation or certification of PCI compliance, it does not cover the other requirements in your cardholder-data environment, and using it does not make an organisation compliant. Your compliance is assessed by your QSA or acquirer. Reproduce and distribute this pack freely.