

# Attestation of Scan Compliance

Field	Value
ASV Company	Foregenix Limited
ASV ID	ASV-2025-FORE-001
Merchant	PaperWorks Online Ltd.
Merchant Contact	Pam Kelleher – <a href="mailto:pam@paperworks.io">pam@paperworks.io</a>
Scan Customer ID	PWL-IE-Q4-2025
Scan Date	15 December 2025 02:00 UTC
Rescan Date	22 December 2025 02:00 UTC (after fixes)
Scope	External IPv4: 3.250.123.10, 3.250.123.11, FQDN: <a href="https://paperworks.io">paperworks.io</a> , <a href="https://www.paperworks.io">www.paperworks.io</a>
Total Hosts Scanned	2
Pass / Fail	PASS – no CVSS ≥ 4.0 findings remaining

ASV Sign-off	Digitally signed by John Smith, Lead ASV, 24 Dec 2025
--------------	---

2. Executive Summary

TableCopy

Host	OS	Open Ports	High	Medium	Low	Info
3.250.123.10	Amazon Linux 2023	80, 443, 22	0	0	1	2
3.250.123.11	Amazon Linux 2023	443	0	0	0	1

Key Points

- Zero failures (CVSS ≥ 4.0) after remediation.
- Low-1: Weak cipher support on port 22 (SSH) – CVSS 3.7 – accepted risk (office VPN bastion, MFA enforced).
- Info-1: Server banner revealed “nginx” – not a failure per ASV Program Guide v4.0.
- PCI DSS 11.3.2.1 quarterly requirement satisfied for Q4 2025.

3. Detailed Results (CSV export)

Host	Port	Protocol	Service	Severity	CVSS	Plugin Name	Status	Last Detected	Synopsis	Solution
------	------	----------	---------	----------	------	-------------	--------	---------------	----------	----------

250.... ▾	22	tcp ▾	ssh	Low ▾	3.7 ▾	SSH Weak Algorithms Supported	Active	4 De... ▾	The SSH server is configured to allow weak algorithms.	it /etc/ssh/sshd_config to remove diffie-hellman-group1-sha1 and restart SSH.
250.... ▾	80	tcp ▾	http	Info ▾	0.0 ▾	Web Server Allows HTTP	Closed	2 De... ▾	Port 80 redirects to HTTPS.	direct already implemented.
250.... ▾	443	tcp ▾	https	Info ▾	0.0 ▾	Web Server Type	Open	4 De... ▾	Server header is "nginx".	t a failure server_kens already off.

4. Remediation Log (required evidence)

TableCopy

Finding	Action Taken	Evidence Location	Date Closed
TLS 1.0/1.1 enabled (CVSS 5.0)	Removed from Nginx config; only TLS 1.2/1.3 left	Git commit <a href="#">a4f2c1e</a>	18 Dec 25
Missing HSTS	Added <code>max-age=63072000; preload</code>	<code>/etc/nginx/conf.d/security.conf</code>	18 Dec 25

Weak DH 1024	Generated 2048-bit DH param & deployed	<code>/etc/nginx/ssl/dhparam.pem</code>	20 Dec 25
Exposed <code>/setup.php</code>	Deleted installer files; blocked <code>*.php</code> in DOC root	PR #112	21 Dec 25

---

## 5. False-Positive / Exception Requests (none pending)

No disputes filed – all CVSS  $\geq 4.0$  findings were fixed and re-scanned successfully on 22 Dec 2025.

---

## 6. Next Scan Due

31 March 2026 (Q1 2026) – calendar invite already sent to Pam.

---

## 7. Document Control

File-name: `ASV-Report-Q4-2025-PWL-v1.pdf`

Stored: `.../ISMS/PCI/ASV-Reports/`

Retention: 3 years (PCI DSS 10.3)

You can now append this report to your SAQ A or SAQ D submission and show acquiring bank proof of quarterly external scanning compliance.