PYCO • RENEW
SECURE IT ASSET DISPOSAL

Certificate of Network Equipment Sanitisation

PYCO-NSAN-2026-DEMO-FW-01 · 24 July 2026

NETWORK SANITISATION VERIFIED

Configuration, credentials, keys & logs removed — device returned to factory-default state

DEVICE INFORMATION

Asset Tag	DEMO-FW-01
Make / Model	Fortinet FortiGate 80E (FG-80E)
Type	Networking Equipment
Serial Number	SN-DEMO-FW-01

SANITISATION CONTEXT

WTN Reference	WTN-DEMO-2026-0001
Customer	Sample Customer Ltd
Method	Vendor secure-erase / factory reset
Date	24 July 2026

DEVICE INFORMATION

Asset Tag	DEMO-FW-01
Device Type	Next-Generation Firewall / UTM appliance
Model	Fortinet FortiGate 80E (FG-80E)
Serial Number	SN-DEMO-FW-01
CPU	ARM Cortex-A9, 1000 MHz
RAM	2 GB DDR SDRAM
Boot Firmware (BIOS)	Version 05000007

SANITISATION DETAILS

Date	22 July 2026
Method	BIOS-level "Format boot device". The device console was credential-protected, so the boot device was formatted directly from the FortiGate BIOS configuration menu, which erases the entire boot flash without requiring the administrator password.
What was erased	the entire contents of the boot device - the FortiOS firmware and the full configuration partition, including administrator credentials, VPN pre-shared keys and certificates, firewall policies, the local user database, network/interface configuration and all stored settings. No firmware, configuration, credentials or network data remains on the device.
Console	Serial console, 9600 8N1

VERIFICATION

Pre-wipe state	In-service firewall (member of a high-availability pair) with an active production configuration present; console access was credential-protected.
Post-wipe state	Boot device empty - no firmware and no configuration present; the device no longer boots.
Checks Performed	The BIOS format operation completed and reported "Formatting..... Done." A subsequent boot attempt returned "No default firmware. You may try backup. Please power cycle. System halted." - confirming the boot device, including the configuration partition holding all credentials, keys and settings, was erased and the device no longer boots. (Note: the unit is intentionally left without firmware; a purchaser would load a fresh FortiOS image.)

Declaration of Sanitisation

This certificate confirms that the network equipment identified above has been **sanitised** using the vendor-provided secure erase method. All configuration data, user credentials, log files, SSH keys, licenses, and certificates have been removed.

The sanitisation process has been verified by confirming the device returned to factory default state. This process meets the requirements of:

- NIST SP 800-88 Rev 1 – Guidelines for Media Sanitization (“Clear” level for network equipment)
- UK Data Protection Act 2018
- EU General Data Protection Regulation (GDPR)

AUTHORISATION

Verified by PYCO Renew
PYCO RENEW LTD

Date: 24 July 2026 · Ref: PYCO-NSAN-2026-DEMO-FW-01

PYCO RENEW LTD | Company Registration: 16774881 | Waste Carrier Licence: CBDU607333
Unit D13, D Block Building, Fieldhouse Industrial Estate, Fieldhouse Rd, Rochdale, OL12 0AA
Tel: 0161 888 0862 | Email: compliance@pycorenew.co.uk | Web: pycorenew.co.uk

This certificate was generated on 24 July 2026 and is valid as proof of network equipment sanitisation.