Semi-Annual Firewall & Segmentation Review

PCI DSS 4.0 | Required every 6 months | One-page checklist

Business Name: _____ **Reviewer:** _____

Review Date: _____ **Review Period:** _____ *(Suggested: January + July)*

FIREWALL RULES

- [ ] Review all active firewall rules. Remove any rules no longer needed.
- [ ] Confirm inbound rules only allow traffic required for the cardholder data environment (CDE).
- [ ] Confirm outbound rules restrict CDE traffic to payment processor endpoints only.
- [ ] Verify default-deny is in place (block everything not explicitly allowed).
- [ ] Check for any "permit all" or overly broad rules and remove them.
- [ ] Confirm remote management access (if enabled) requires MFA and encrypted connection.

VLAN & NETWORK SEGMENTATION

- [ ] Verify POS / payment devices are on their designated VLAN and cannot reach other VLANs.
- [ ] Confirm no new devices have been connected to the CDE VLAN since last review.
- [ ] Test isolation: attempt to ping or access CDE devices from a non-CDE VLAN.
- [ ] Verify guest Wi-Fi, cameras, and office devices remain on separate VLANs.
- [ ] Review DHCP leases or static assignments for unexpected devices on the CDE VLAN.

DOCUMENTATION & FOLLOW-UP

- [ ] Update the network diagram if any changes were found.
- [ ] Update the CDE scoping document (list of all in-scope systems).
- [ ] Log any findings or changes made during this review.
- [ ] Schedule the next review date (6 months from today).

FINDINGS / NOTES:

Reviewed by: _____ **Date:** _____