

How does PCI DSS apply to individual PCs or workstations?

PCI SSC FAQ | Article 1115 | June 2012

All system components in the network are considered part of the cardholder data environment unless adequate network segmentation is in place that isolates systems that store, process, or transmit cardholder data from those that do not. Without proper network segmentation, the entire network is in scope for the PCI DSS. Where there are many PCs or workstations in an environment and all PCs do not need access to the cardholder data environment (CDE), the network segmentation should provide access to the CDE only for the PCs that need access, and should prohibit access for all other PCs. Where segmentation is used to reduce PCI DSS scope, the assessor must verify that the segmentation controls are effective and working as intended. The assessor would need to determine whether the connected systems provide a path for other systems into the CDE. If there are other systems on the network which are not adequately segmented (isolated) from the CDE, they could also be brought into scope. Once it has been validated that adequate segmentation is in place, PCI DSS requirements would be relevant to, and should be applied to, the PC population which is in scope. While all connected systems should be considered in scope for a PCI DSS review, the particular PCI DSS requirements applicable to each system may vary depending on the function of the system and the presence of any additional controls that are implemented. (For example, controls could be in a place that prevents the system from accessing cardholder data or from influencing the security of the CDE in any way). All such controls would need to be verified as part of PCI DSS scope verification.

Source: <https://www.pcisecuritystandards.org/faqs/1115/>