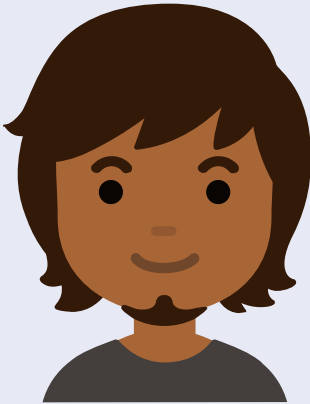
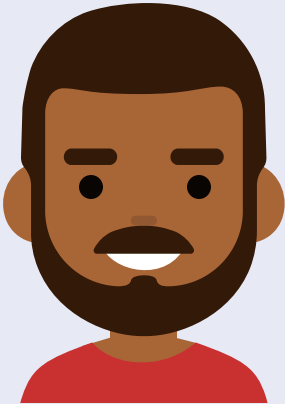


A TALE OF TWINS:

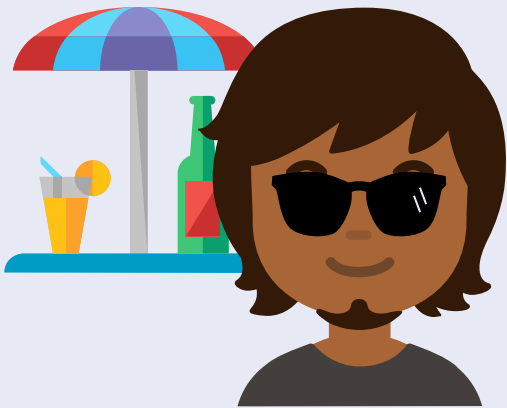
CONTACT CENTRE DATA SECURITY CHECKLIST

Meet twins Dave & Dom.



Dave and Dom both lead security efforts at separate contact centres. Dave decided to achieve PCI compliance the hard way. Dom called **pci/pal/6**.

Now, Dave is exasperated. His compliance to-do list haunts him in his dreams - and that's when he has time to sleep. Dom, on the other hand, is sitting somewhere under a cabana on the Mediterranean. Thanks to the power of descoping, he knows **pci/pal/6** has it covered.



Don't make Dave's mistake.

Descope your contact centre environment from the requirements of PCI DSS. Otherwise, you could be facing a growing to-do list like Dave.

	Contact Centre Staff (and Back Office Staff) Who Have Access to Systems
<input type="checkbox"/>	Lead staff training to ensure staff are aware of the sensitivity of card payments and report anything suspicious
<input type="checkbox"/>	Carry out criminal record checks on staff
<input type="checkbox"/>	Have a clean desk policy, restricting agents to taking notes on a digital computer notepad that is flushed from the computer memory as the agent logs off
<input type="checkbox"/>	Prohibit bags from being allowed on premise
<input type="checkbox"/>	Require mobile phones to be stored in lockers away from the contact centre
	Contact Centre PC/Desktop
<input type="checkbox"/>	Lock down USB ports on agent PCs
<input type="checkbox"/>	Run anti-virus software on agent PCs
<input type="checkbox"/>	Implement website whitelists – these stop agents from sending sensitive emails containing card data to external website emails (such as Gmails)
<input type="checkbox"/>	Scan for malware – need to especially look out for keyloggers, which are malicious software programs that track and record keystrokes from other computers
	Telephony System
<input type="checkbox"/>	Pause call recordings while card details are taken
<input type="checkbox"/>	Ensure phone systems are in locked and monitored in a secure area
	Network
<input type="checkbox"/>	Encrypt traffic, so sensitive card data is not sent over the contact centre network as plaintext packets
<input type="checkbox"/>	Implement Network Segmentation (VLANs/ACLs) to stop sensitive card data from being transmitted across the whole network
<input type="checkbox"/>	Scan email servers and databases for stored card data
	Wi-Fi
<input type="checkbox"/>	Ensure Wi-Fi is protected with strong encryption
<input type="checkbox"/>	Regularly search for ‘rogue’ Wi-Fi devices
	Contact Centre Building
<input type="checkbox"/>	CCTV access systems
<input type="checkbox"/>	Require access card entry into the contact centre
<input type="checkbox"/>	Ensure visitors are clearly identified with visitors’ badges and escorted at all times

Ready to get descoping so you can sit back and relax like Dom? Contact **pci/pal/6** today at info@pcipal.com.