Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Changing wireless encryption keys whenever someone with knowledge of the key leaves the organization or moves to a role that no longer requires knowledge of the key, helps keep knowledge of keys limited to only those with a business need to know. Also, changing wireless encryption keys whenever a key is suspected or known to be comprised makes a wireless network more resistant to compromise. **Good Practice** This goal can be accomplished in multiple ways, including periodic changes of keys, changing keys via a defined "joiners-movers-leavers" (JML) process, implementing additional technical controls, and not using fixed pre-shared keys. In addition, any keys that are known to be, or suspected of being, compromised should be managed in accordance with the entity's incident response plan at Requirement 12.10.1.
2.3.2 For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: • Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. • Whenever a key is suspected of or known to be compromised.	**2.3.2** Interview responsible personnel and examine key-management documentation to verify that wireless encryption keys are changed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Knowledge of wireless encryption keys cannot allow unauthorized access to wireless networks.		