Requirements and Testing Procedures		Guidance
2.3 Wireless environments are configured and managed securely.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If wireless networks are not implemented with sufficient security configurations (including changing default settings), wireless sniffers can eavesdrop on the traffic, easily capture data and passwords, and easily enter and attack the network. **Good Practice** Wireless passwords should be constructed so that they are resistant to offline brute force attacks.
2.3.1 For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults. • Any other security-related wireless vendor defaults.	**2.3.1.a** Examine policies and procedures and interview responsible personnel to verify that processes are defined for wireless vendor defaults to either change them upon installation or to confirm them to be secure in accordance with all elements of this requirement.	
	2.3.1.b Examine vendor documentation and observe a system administrator logging into wireless devices to verify: • SNMP defaults are not used. • Default passwords/passphrases on wireless access points are not used.	
Customized Approach Objective	**2.3.1.c** Examine vendor documentation and wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable.	
Wireless networks cannot be accessed using vendor default passwords or default configurations.		
Applicability Notes		
This includes, but is not limited to, default wireless encryption keys, passwords on wireless access points, SNMP defaults, and any other security-related wireless vendor defaults.		