

	CNS Responsibility	Customer Responsibility
1. Install and maintain a firewall configuration to protect cardholder data	No	Yes
2. Do not use vendor-supplied defaults for system passwords and other security parameters	No	Yes
3. Protect stored cardholder data	Yes	Yes
4. Encrypt transmission of cardholder data across open, public networks	No	Yes
5. Use and regularly update anti-virus software or programs	No	Yes
6. Develop and maintain secure systems and applications	No	Yes
7. Restrict access to cardholder data by business need-to-know	No	Yes
8. Assign a unique ID to each person with computer access	No	Yes
9. Restrict physical access to cardholder data	No	Yes
10. Track and monitor all access to network resources and cardholder data	No	Yes
11. Regularly test security systems and processes	No	Yes
12. Maintain a policy that addresses information security for employees and contractors	Yes	Yes