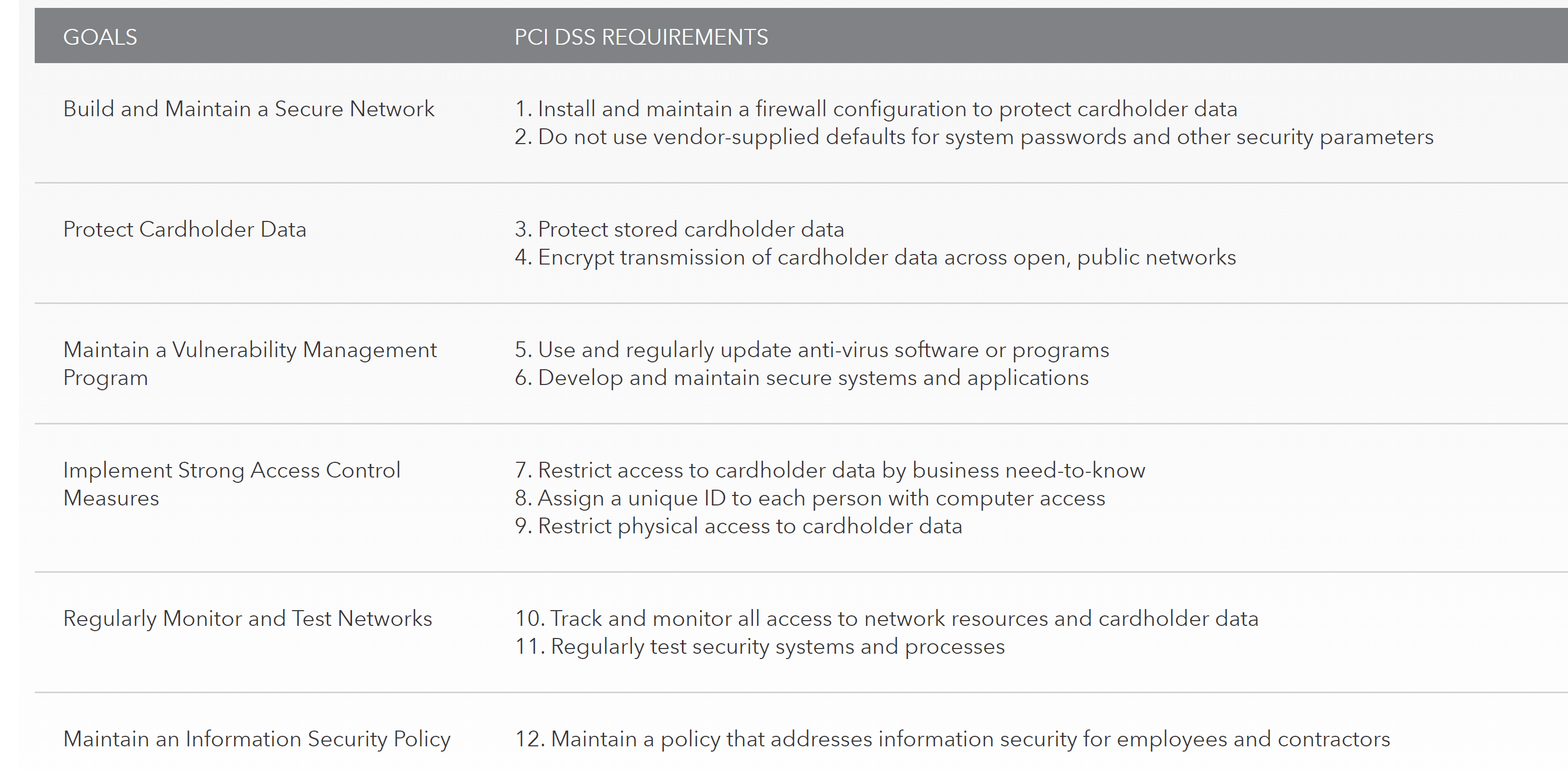
1. Comply with the [PCI Data Security Standard](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml) to the letter, which means:
   1. Nobody gets unauthorized physical access to your servers
   2. Everything is behind a firewall that blocks everything except what's absolutely essential
   3. Change all of the passwords yearly, and never use default passwords
   4. Nothing goes over a wire unless it's encrypted, not even on your LAN
   5. Log everything
   6. Have a written policy
   7. Hire an outsider to test it
2. Nothing touches the hard drive--not even the swap file--unless it's encrypted
3. If you absolutely must store a card number in searchable form, use [key strengthening](http://en.wikipedia.org/wiki/Key_strengthening) methods and turn it up as high as you can bear
4. Consider throwing away all but the first six and last four digits of the card number. You may be able to search for the original order with just these, the date of the transaction and the dollar amount
5. Have a really good PR agency



Quick Steps to Security

A model framework for security, the PCI Data Security Standard integrates best practices forged from the years of experience of security experts around the world.

*The standard works for some of the world’s largest corporations. And it can work for you.*

* Buy and use only approved [PIN entry devices](https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices) at your points-of-sale.
* Buy and use only [validated payment software](https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications) at your POS or website shopping cart.
* Do not store *any* sensitive cardholder data in computers or on paper.
* Use a firewall on your network and PCs.
* Make sure your wireless router is password-protected and uses encryption.
* Use strong passwords. Be sure to change default passwords on hardware and software – most are unsafe.
* Regularly check PIN entry devices and PCs to make sure no one has installed rogue software or “skimming” devices.
* Teach your employees about security and protecting cardholder data.
* Follow the PCI Data Security Standard.