**MEMORANDUM – 2 MINUTE BRIEFING 3**

**TO:** CASEY G. CEGIELSKI, PH. D, CISSP, CISA, CRISC

**FROM:** CENSORED

**DATE:** 9/9/19

The most important policy to be in compliance for this particular problem is PCI DSS. By taking on all of the risk that comes with in-housing the electronic payment processing payment, you must perform risk analysis and regularly ensure that the systems that keep this secure information stays safe. Some important goals that are a part of PCI DSS are to build and maintain a secure network (make sure it’s PCI compliant), protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks and maintain an information security policy. This includes employee security (regular background checks, education on compliance regulations, etc.), testing network security with packet sniffers, installing a firewall, changing default passwords, etc. I don’t recommend this in my opinion, since I don’t believe a 5% income will be a large enough difference for the large portion of risk management that must be done; instead, it would be better to entrust a 3rd party company that specializes in that so that you have less to do.