**Procedures for Security Concerns**

Narrative: This section outlines the security concern with the system and how our design addresses those concerns.

**Storage of Data**

All traffic for Sweet Karoline’s Cakes website should be secured though the use of SSL certificate connections for all secured pages on the website. A secured page includes any page that contains a form for information or for payment processing. All access to the database for administrators, and managers will be protected behind logins that require a username and password and are encrypted to meet AES 256-bit standards. Access to this data will be restricted to only users that need access for operational justification via permissions groups set up for users. This will ensure that the data that is stored is secured and is protected to minimize the risk of a data breach. Customers will also be able to access historical purchase data, and personalized accounts utilizing similar security methods as database access, but the information they see is restricted to their individual customer id.

**Back up of data**

All data that is stored in the database and backups of the website will be regularly backed up into the selected cloud platform, this minimizes the risk of data corruption and ensure that if a drive fails in any device used by Sweet Karoline’s Cakes, that the data on that machine is not lost. The long-term protection of the data is designed to be the reasonability of the service provider and will be outlined in the Service Level Agreement.

**Payment Processing**

All of the donor financial data that is processed for donations is handled by Pay-Pal. They store and manage all of the security that is required for the protection of consumer data, payment information, and payment methods. Pay-Pal and the bank that SKC utilizes will complete a secure transfer between the consumers, and SKC’s business bank account. This allows SKC to minimize the security risk associated with taking payments form donor over internet.