| ID | Risk | Owner of Risk | Cause | Effect | Probability | Impact | Severity | Mitigation |
|---|---|---|---|---|---|---|---|---|
| 1 | Data in inventory inputted incorrectly. | Manager | Human Error | Snowball effect of incorrect data inputted in initial table to related tables. | 4 | Miscommunication between company and customer. | 3 | Ensure proper communication is practiced throughout the organisation when relative to the inventory database. |
| | | Employees with access to the inventory database | Incorrect knowledge/information transmitted | Customer may receive the wrong order | 3 | Customer may lose trust in the company's ability to hold and organise personal/sensitive information. | 3 | Ensure customer data is inputted correctly by double checking with the customer and checking their information is correct with them. |
| | | | Incorrect data received | Customer receives wrong quantity. | 3 | Customer receives an inappropriate amount of product, either more than or less than the customer had ordered. This causes confusion and makes the process longer and more tedious for the customer to deal with, as they need to deal with either waiting for the right quantity of products, or having to send the rest of the quantity back to the company. | 3 | Ensure that any major changes to the inventory database/tables are ran through the inventory manager or that the manager is the only one who would have the capability to finalise the changes on the database. |
| | | | | Customer information is incoherent and unusable. | 3 | Unable to finalise order, therefore customers won't be able to receive their products in the alloted time | 3 | Professional and appropriate communication is carried between the business and the customer, to ensure the correct information is received. Have processes in place to check the information multiple times, before being inputted into the system. |
| 2 | Database deleted. | Manager | Human Error (Accident) | No information to be found. | 3 | The workforce is delayed and no clear goal or objective is highlighted for the workers. | 3 | Reduce the number of personnel that have accessibility to such a command of the database. Something so detrimental should only my accessible by managers. |
| | | Employees access to the database | Misinterpretation of instructions | Compounding effect onto any other databases, linked with the database that had been deleted. | 3 | All information within that database is lost, and it may not be possible to be recovered. | 4 | Have backups or scheduled saves for the database, to recover any data that would've been lost if a database had been deleted. |
| | | | | | | Customers are "lost", some may not appear in the system again, but some may appear back up to continue using the company's services, however a handful of customers may not come back due to the ignorance of the company with their information. | | Proper training is provided to staff, who may have access to database commands and alterations. |
| 3 | Security is breached and the databases are exposed to an inappropriate party. | The Business. | Ignorance and negligence towards different types of technological security breaches. | Private and personal information is leaked to the public. | 2 | The company loses credibility. | 4 | Educate staff on proper data security, and the laws(acts) associated with data handling of personal/vulnerable information. |
| | | The individual the information is referring to. | Inappropriate security surrounding the information. | The companies personal information is leaked to the public, as well as to its competitors. | 2 | The company loses customers due to lack of trust and mis protection of vulnerable information. | 4 | Company takes the appropriate precautions when creating a database, making sure that they apply the appropriate security |
| | | | | A lot of information becomes very | | Reputation of the company decreases and becomes known to the public, making it more difficult for future and current customers to trust the company again. | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | Lack of information segregation. | vulnerable, being in one place at once, means it is easily accessible. | 2 | The company now has to spend more money on reassuring that the security breach does not occur again. Which any extra costs could've been avoided if proper precautions were taken in the first place. | 4 | appropriate security procedures surrounding the database. |
| 4 | Faulty Equipment | Store managers | Low-quality equipment purchased. | Systems are delayed and certain processes cannot move forward. | 2 | Company/store cannot receive orders or contact suppliers regarding orders, so the needs of the business and customer aren't fulfilled. | 2 | Make sure the store is provided with good quality equipment before operations so that the chances of technical issues decrease. |
| | | Store Employees access to the database. | incompetent behaviour surrounding the equipment, leading to heavy damage or damage over time. | Equipment is unable to function and therefore cannot be used by the employee to access the databases and any appropriate information. | 3 | Specific store has to spend more money on new equipment, which add up the extra costs of the business. | 2 | Staff is trained on handling equipment appropriately and precautions are taken to ensure that damage to equipment is decreased. Staff are given rules and instructions on handling the hardware. |
| | | Specific Store with the faulty equipment. | Equipment is old and may need a hardware/software update, depending on the appropriate need. | Processes are slower than usual, and the progress of the specific store begins to falter behind other stores. | 2 | Customer needs aren't met, along with lack of contact with main branches and the suppliers, so the store may struggle with further orders until new equipment is obtained. | 2 | Monthly or yearly inspections are taken within each store, to ensure that equipment is up to date and any faulty equipment is promptly replaced. |
| 5 | | | | | | | | |