Software Engineering Methods

Coursework 1 Part 2

40087220

When designing the new system, there should be security measures put in place that protect both the system and its users (the customers).

Firstly, gaining access to the system should require the users to register with a username/e-mail address and password and have the user confirm the registration via confirmation e-mail. This should be put in place to protect the users’ bank details and reduce the risk of hacking.

In conjunction with the username and passwords users should also validate their card details upon the transaction every time and location to be delivered to, this makes sure the good are delivered to the correct address in case the users details such as their address changes.

The system also requires validation checks in areas like the product quantity field as the user may make an error and rather than ordering the desired amount they order too much or too little.

Physical security of the system must also be taken into account. Access to the computer room should be limited to permitted staff only and controlled via some sort of passcode system i.e. the use of ID swipe cards. The room itself should also be monitored via CCTV to ensure no unpermitted people gain access. The computers themselves should also be protected via sign-in and sign-out procedures, only permitted staff should have usernames and passwords to gain access to the system.

Data should also be backed up on a fairly regular basis in case any data is lost or the system malfunctions.

The physical system should also be protected from things such as power cuts and fires etc. A guaranteed power supply is needed and fire alarms will also be needed.

The system will also need protection against viruses, this can be done by identifying specific code patterns in transmissions. Firewalls are also needed in order to put up a barricade between the system and network and external sources such as the internet. The aim is to prevent unauthorised communication in to and out of the network. This does not 100% secure the system but is an extra layer of security.

Employees must abide to any laid down procedures, for this reason any employees that have access to the system must be firstly screened if they are allowed access to sensitive data to see whether they understand the importance of security measures.

Behaviour of employees should be monitored and history logs kept. Logs of failed sign-in attempts should also be monitored. Information on what security measures and why should be distributed.