**Security Policies Mark Scheme**

1.

You need to identify potential risks

e.g. viruses / fire / natural damage / hacking / systems failure / fraud, etc

Understand the likelihood of risk occurring

some things such as power cut are inevitable but explosions much less likely - senior managers have to assess the likelihood of each risk occurring and put in the necessary security

What are the short and long term consequences of threat?

resources (staff equipment, etc) need to be directed towards recovering the data / may have to pay compensation / financial loss due to loss of business through not being able to take orders / embarrassment/ prosecution / loss of integrity / bankruptcy / cost of replacing equipment

How well equipped are you to deal with the threat

has to be reviewed periodically because of changing needs - disaster recovery program – backup strategy

2.

Logical (software) methods

User ids, passwords, levels of access ( e.g. who can update web pages) firewalls, encryption.

Auditing for detection

Query any transactions that are out of the ordinary for customers, access logs

System Access

Establishing procedures for accessing data such as log on procedures, firewalls.

Personnel administration

Training (including prevention of accidental misuse) , fitting the employee to the task, ensuring that staff are controlled, staff screening.

A code of conduct

A list of roles and responsibilities that an employee should follow when using ICT equipment

Operational procedures

Including disaster recovery planning and dealing with threats from viruses, backup, updating antivirus.

Disciplinary procedures

Warnings / dismissal / prosecutions etc.

3.

|  |  |
| --- | --- |
| Threat | Consequence |
| Terrorism  Natural disasters  Sabotage  Fire  Theft | Loss of business and income  Loss of reputation  Legal action |

4.

|  |  |
| --- | --- |
| **Operational Procedure** | **How to carry out procedure** |
| Screening potential employees | * Ensure staff are controlled * Fit employee to the task * CRB checks |
| Routines for distributing updated  virus information and virus  scanning procedures | * Ensuring virus signatures are updated daily and distributed around the network when a station logs in * Establish firewalls |
| Define procedures for downloading  from the internet, use of removable  media, personal backup  procedures | * Staff code of conduct * Penalties for misuse * How often done, have they got to use special machines, off site etc |
| Operational Procedure | * How to carry out procedure |
| Establish security rights for  updating web pages | * Who/what/when |
| Establish a disaster recovery  programme | * Who does what and when, including checking the standby equipment * Backup plans, i.e. how often * NOT RISKS ANALYSIS |
| Set up auditing procedures (Audit  trails) to detect misuse | * Who/what when * Contiguous investigation of regularities * Query any transaction out of the ordinary |