P1 - Explain the issues organisations must consider when planning computer systems maintenance

Issues  
There could be issues organisations deal with such as fires that would be a concern, so for example if there were to be a fire in an organisation, they should consider having some policies and procedures set out for employees to follow (such as guides on how to leave the building via fire exits, or by having health and safety policies set out) if a disaster like so were to happen. By having policies and procedures it would alert employees on what to do if issues occur, otherwise they’d be in bad situations and may even be in danger if a fire were to occur.  
Health and safety  
There can be many issues to do with health and safety in an organisation, for example there may be loose wires around, and if an employee were to come into contact with them, the main risk and issue of this would be electrocution. An employee could be seriously hurt by electrocution and would result in making the organisation looking bad and seeming unsafe. Therefore there should be policies and procedures for risks like these to inform employees on what to do when issues like electrocution could occur.

Sustainability and Environmental issues  
In an organisation, (for example) when a computer breaks down it would have to be thrown out and replaced. Before throwing out the computer, the organisation would have to consider whether they would want to completely throw out the whole computer, or if they would like to recycle its useful parts in order to sustain it and allow its parts to be useful in the future. A company can’t just throw out a computer or massive piece of hardware as it may even be harmful to the environment, so therefore the organisation would need to plan exactly how they are going to recycle their broken or old hardware and decide where they should be transported and how exactly their parts are going to be used. Also apart from recycling old pieces of hardware, they can decide to sell them to other companies willing to accept them.

Reporting and documentation and problem escalation procedures  
When issues occur in an organisation, specifically to do with a computer related issues, these issues have to be reported and also documented into a fault log, specifying the problem and a date and time of when it has happened, and even a solution. By reporting issues such as a the monitor not working, it may be that it needs to be plugged in, or needs to be replaced, and by having it documented down these issues are then looked at and solved. If issues are not documented down then it causes escalation problems. For example if an issue such as a computer isn’t working due to a dodgy fuse is not written into the fault log, then this issue will get worse and also dangerous as it would blow if abandoned. Therefore it is important to consider reporting any problems found in an organisation.

P2 - Assess the health and safety risks facing the practitioner when maintaining computer systems  
In order to make sure that employees are safe in their working environments they should be aware of health and safety risks in their organisation.

Electrocution

In a workplace employees should make sure that whilst working with equipment that they are fully aware of risks that could occur, for example if an employee were to be fixing hardware, they should make sure that no fuses are plugged in/switched on or connected to the piece of hardware that they are working on in order to prevent electric shocks, which would be putting them in danger. Consequently, by following company policies on health and safety, they should carry out such tasks with gloves, and full awareness of any other risks that may happen apart from electrocution.

Fire

No matter what situation, fires may occur, whether it is from a drink spilling over to a blown fuse, a fire could happen. Again, health and safety policies and procedures are to be followed in order to ensure that all employers are aware of what exactly to do if a fire were to occur, and also to ensure that everyone will be safe. If a fire were to occur, this would damage the organisation both ways, all equipment’s and documents will be burned and damaged, and it also means that the company would have to pay for all damages (if they do not have insurance of course). In order to prevent fires from happening, fire extinguishers should be present at all times, and in order to ensure safety for all employees if a fire were to get out of hand there should be many clear fire exits for employees to use to get them out of danger.

Fires and fire fighting equipment and training

In case of a fire, there should be plenty of fire equipment around in order to prevent them, and/or to keep an employee safe, for example fire alarms should be in all around an organisation so that everyone inside is alerted of any fire that occurs and should leave the building once the alarm is heard. It is critical for an organisation to consider having fire training for employees because if there isn’t any training then everyone would be at risk. As a result practise alarms should be help in order to direct employees on what to do if an actual fire were to take place, keeping them out of risk if it were to happen.

Electrostatic discharge (ESD)

What ESD is, is electrical discharge of current which if a person were to come into contact with, it could be very dangerous. ESD can happen when a person is working on the inside of the computer, and can be prevented by wearing an antistatic wristband to protect you. ESD is able to damage parts of a computer or even the entire computer the hardware to fry and breakdown and problems to the user such as electrocution. In order to prevent electrostatic discharge, the organisation must set a policy for this matter, insuring that it is followed in order to keep employees safe whilst maintaining their computer systems in the workplace.

First-aid training

Every organisation should have staff trained to handle first-aid needs, for example if someone in the organisation has hurt themselves whilst working on fixing hardware, if they were to seek medical attention then an employee with trained with being able to deal with first-aid should be ready and available to help that person. There should be a well experienced team in the organisation that has first-aid training ready to help out at any time when needed.

M1 – Explain the need for policies and procedures to control the maintenance of computer systems

Health and safety  
All organisations must have health and safety policies and procedures. By having these policies and procedures it ensures that the organisation is a safe environment for employees to work within. An example of a health and safety procedure would be that in the working environment, it would be a policy that staff would need to work with adjustable chairs for their needs and so that they won’t get any problems such as a backache. Also a procedure such as fire drills would be necessary in case of fires, therefore alerting employees what to do if an actual fire were to happen.

Backups  
Whilst using IT systems in an organisation, there should be policies for employees to always backup their work whilst working on computers. By backing up work it ensures that no files will be damaged lost or deleted, for example if there are natural disasters such as fires, or if a computer breaks down then the files would have been backed up and ready to restore. There should be a policy that a backup should be carried out at least once a day so that the company won’t be losing important data and files.

Security  
In an organisation, in order to maintain a computer system safely is by having good security. Security is an important factor when it comes to maintain computer systems, and policies on these should be enforced. For example on a computer without an antivirus, it would be easy for viruses to be caught onto the computer system, which means that important files on the computer could be at risk of being deleted or even tampered with, due to the fact that there is a virus on the computer. By having an antivirus installed secures the computers’ security, making sure that all files are scanned and protected from any viruses.

Confidentiality  
A policy on confidentiality should be enforced, ensuring that employees in the organisation do not share any pieces of work to anyone outside of the company, as it can lead to consequences affecting both the employee and the company, such as the employee being sued for sharing confidential information. So for instance, if an employee shares information to another or even publically, the information can then be stolen and used by those others. Therefore if there aren’t any policies on confidentiality then this means that the organisation would be badly effected as it means that all their private information and even ideas will be known to others and can be used against them. Also as mentioned above, the employee would be facing legal charges.

Training

A policy and even procedure should be set that all staff that enters the organisation should go through a training process before actually carrying out their jobs and tasks in the organisation. This means that if a brand new employee is being introduced to their position, they should be trained by the organisation, for example on how to use a computer correctly, they should be trained to perform tasks properly, such as how to function the computer, what to do, and what not to do on a computer, and to be able to maintain their computer systems well, and most importantly not to download programs from the internet or deleting important files stored on the computer system. Another reason why training should be done is that no employees hurt themselves whilst carrying out jobs, for example an working with hardware should be trained before being able to work on such tasks before they hurt themselves badly, which would affect the organisation.