**D2 - Design a network security policy for a small organisation.**

**Network security policy for a cleaning firm**A network security policy is used to strengthen a networks security. A policy is a set of rules that organisations expect users to follow to ensure that the network is not put at risk. A network policy should be reviewed regularly to adapt to any changes or experiences that might affected the network.

**Data Integrity**Data integrity is the affirmation that data in the network can only be accessed by those with the authority to do so. Data integrity can be controlled through the physical environment of the network – installing security systems around the building will prevent servers and networked terminals from being accessed by unauthorised personnel. Clearance levels can be set on a user’s account so that they can only access resources that match the clearance level they have and are necessary for their job. Confidential files must be password protected and have a set clearance level on them to stop the data being accesses by unauthorised users. Regular reviews of user access and rights can identify what files and resources each specific user can access and change their rights if there are resources they shouldn’t have access to. Access control lists should be used to monitor what resources are viewed and changed by each user, and log the information. During security audits, the access control lists should be used to check if the security system is tight enough and that any issues with the security of data are fixed.

**Confidentiality**Confidentiality in the network is paramount and measures to ensure confidentiality should be taken seriously. Access to data in the network should be restricted so that only the authorised users of the network can access the data. There are several measures that can be implemented to ensure that only people with the authorisation to view the data can see it.   
Data encryption should be used on all files on the network and only the users authorised to view the data should have the decryption software.   
Confidential files on the network should ask for a username and password then cross-match it with the access control list to see if the user should have access to the file. If someone who does not have access to the file tries to view the file, their username should be shown on the access control list log and flagged so that the network administrator can take action to stop the person attempting to access the file.  
Use security cards to reduce the risk of unauthorised users accessing the server/network terminals and accessing restricted data.  
Security measures that are implemented to keep data secure and confidential should be checked regularly in penetration tests and security audits to ensure that data and resources are protected.

**Reviewing of user access and rights**The network manager must systematically review the access rights of each user of the network and ensure that any data they access is appropriate to their role. If an employee of the cleaning firm has had their contract reviewed/revised or their role in the organisation has changed, their access rights must change with them. This includes reviewing their rights and access to resources that they may use, any resources that they do or do not need should be added or removed.

**Penetration testing**Penetration testing should occur on a regular basis (e.g. a set number of times every 3 months or so). Penetration testing should also occur whenever a change is made to the network security features to prevent any issues from going undiscovered. Any issues uncovered during a penetration test should be formally identified and reviewed to locate the source of the problem and resolve it. Penetration testing should help ensure that the information on the network (e.g. client details) is not accessible by people outside the company or by people without the required clearance levels.

* **Security audits**  
  Security audits are a formal review of all parts of the network. The security audit should:
* Define what assets will be inspected during the security audit
* List all of the risks that could potentially damage the security of the network
* Review previous threats and security issues to determine if there is a trend in security flaws and to identify any potential causes of security threats
* Order and analyses assets depending on the number of vulnerabilities they have and how serious they are to devise a network security response plan
* Apply a security system that uses clearance levels to control the access to confidential files/documents about clients
* Apply an intrusion prevention system to safeguard the network and the data it holds; to stop unauthorised access of the firewall
* Regularly backup data stores and restoration systems to minimise network downtime and protect clients information in the case of a major security threat
* Ensure that any information stored outside the network on laptop devices or other computer devices, is encrypted and stored in a password protected file
* Ensure that the buildings security system is functioning properly and will prevent the building from being penetrated by people other than employees

Security audits should occur regularly and will show how secure the network is. If any issues with the network are discovered during the security audit, then they should be addressed quickly to ensure the network is not at risk and to keep data stored on the network safe and secure.

**Reviewing of firewall access**A secure firewall is needed in order to protect the information stored on the network from hackers and viruses. The firewall is able to identify the attacks that hit it, these attacks include:

* Reconnaissance attacks where intruders attempt to identify and position the systems services and vulnerabilities in the network.
* Access attacks where intruders attack the network to gain data or users attempt to change access rights.
* Denial of Service attacks where the attack damages the network to a point where the computer systems become corrupt and deny users access to the network.

The firewall is a key feature of a network and ensures that the data inside of the network is protected. Only the network manager and network administrators should be able to access the firewall settings and know the password to access the web interface.Reviewing who has access to the firewall is important as the firewall any unauthorised changes to the firewall can drastically affect the networks security. This means that the access control list for the firewall needs to be updates regularly to remove ex-users who might try and attack the firewall or change its settings. This also means that old, outdated devices covering the firewall need to be removed or replaced so that they cannot be the cause of a firewall breach.

**Access control list policies**Access control lists should restrict users from accessing files that they have no need to view, but enable users who are authorised to view these resources etc. The access control list should record what resources are accessed by each user and log them in a database that the network manager has access to. This log should show if any users are able to access information that they are not authorised to view, and allow the network manager to alter the resources the user can access; the ACL should define the rights of a user and prevent them from accessing the resources. Some resources in the network may be read-only for some users but be read/write for others, the access control list should manage the users and give the correct access rights. For instance, a cleaner should be able to view the list of their clients but not be able to change/edit the list, only their manager should be able to change the information.