



Security & Control Guidelines for Point of Sale Devices

The Point of Sale (POS) is an important piece of site operational equipment. It has therefore been designed in such a way that the risks of exposing the POS or other equipment that it is connected to, either on site or remotely are adequately safeguarded or controlled.

As a POS user it is essential that you follow the guidance that you are given on operation of the POS. These recommendations reinforce some essential points relating to Security & Control. **If you have any concerns about these discuss them with your Site Manager.**

Remember:

Your User-id (or access card where used) and password are your security. Safeguard them as one of your own possessions.

The following are some recommended best practices

You should:

- Only log on using the unique user-id and password that you have been given.
- Change your password periodically, every 35 days is recommended (may need a new password to be issued).
- If you suspect that the POS or one of the attached devices has been misused or tampered with in anyway report it immediately.
- Check any seals or tags on any equipment (such as card readers or pinpads) daily and ensure these have not been tampered with.
- Look out for any suspicious devices (e.g. concealed cameras near pinpads) placed close to the POS or in such a way that they can view it or any of the attached devices.
- Ask those seeking to work on the POS or attached devices for ID or contact the helpdesk to confirm that they are authorized.
- Only discuss the operation of the POS with known staff, helpdesks or maintenance engineers and only give remote access following approved procedures.

And you shouldn't:

- Don't share your password or write it down in such a way that others may be able to discover it.
- Don't remove from or add any equipment to the POS unless specifically authorized. (This excludes normal service items - e.g. changing paper till rolls).
- Don't tamper with any related equipment (e.g. communications equipment) and do not disconnect any cabling or connect anything to it.
- Don't attempt to use the POS for any other purposes - you will not be able to and may cause damage.
- Don't drink or eat at the POS; apart from giving a poor image to customers this may cause damage.
- Don't place mobile (cell) phones or similar transmitting devices near the POS or pinpads.
- Don't give any information about the equipment on site or its use to strangers.
- Don't accept calls from third parties seeking remote access to the equipment unless they are a known helpdesk following agreed procedures.