Gateway - The BBC Intranet

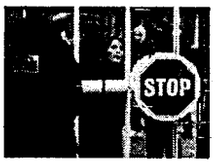
Gateway

You are in: Fraud Management > Preventing Fraud > Control > **Physical Security**

Contact: (02)26976

Physical Security

Report Fraud Here



You wouldn't leave your personal valuables unprotected, so why would you treat BBC equipment and information any differently?

It is everyone's responsibility to protect BBC equipment and information. If you are doing any of the following then you could increase the risk of theft occurring to BBC property. You could also allow sensitive information to fall into the wrong hands.

Useful links

Other useful links

Do you?

Do you ever leave your laptop unsecured on your desk overnight?

Do you ever leave security doors open?

Do you ever distribute production equipment without a record of who has taken which item?

Do you ever leave sensitive information on the printer or on your desk overnight?

A definition and examples of physical security controls follow.

Physical Security Controls

Physical security controls include a range of safeguards which help to reduce the risk of theft by making it physically difficult to carry out.

Examples of such controls include:

Access to BBC buildings (and certain areas within them – e.g. the cheque printing facilities at the BBC's outsourced finance partner) is restricted using security cards. All visitors must sign-in

BBC assets (such a cameras and laptops) are tagged and checked periodically against an asset register

Surveillance cameras are placed in strategic places to help identify and provide evidence of fraud occurrences. CCTV cameras are operated in accordance with the requirements of the Data Protection Act

Further details can be obtained from the **Security Code of Practice**.