Physical Security Policy - Pool Card Requirements

Scope

These requirements apply to and are to be used by any BT/Openreach employee or BASOL Redside company who manage and facilitate access for non-BT/Openreach people using pool cards and keys.

Requirements

Pool cards are only permitted to be used for short term access to BT sites and buildings (no longer than 4 weeks) and can only have temporary access assigned to them. For other access management options please refer to a copy of the BT Physical Access Application Process for Non-BT Organisations available from sam.customer.services@bt.com.

Security Directives

1. Pool cards **must** be strictly controlled to ensure that physical security is not compromised and BT/Openreach and 3rd party assets and people remain in a secure environment.
2. Pool assets must only be used where personalised issue is not viable.
3. All pool cards/keys must be issued by an approved 3rd Party Authorised Signatory (AS) or a BT Contract Liaison Manager (CLM); A CLM must be a permanent BT employee of Band 1 Manager or above.
4. An AS/CLM can only order access cards and keys for contractors working on behalf of their organisation and are responsible for authorising unhosted access to the BT estate, in accordance with the Physical Security Policy Access Requirements.
5. Contractors using pool assets must display a valid photographic company ID Card in order to gain unhosted access to a BT building or site, this photographic ID card must be worn and clearly displayed at all times when within the BT building or on a BT site.
6. Pool access cards must not be de-activated and immediately re-activated against the same person; instances of this happening will result in the card being removed and no further pool cards being issued.

Contract Liaison Manager/Authorised Signatory Responsibilities

1. Ensuring access to BT's property is controlled and given only to authorised personnel where there is an operational or business need.
2. Ensuring that people who are issued with pool cards have received, and have declared receipt, of information relating to health, safety, environmental and security requirements when working on our managed estate. This should be in the form of a signed receipt or email template completed by the named individual. Further information can be found in the Security Handbook for non-BT organisation (available from BT Sponsors or at http://snip.nat.bt.com/SecurityHandbook) and the Safety, Health and Environment Booklet (at http://snip.bt.com/SafetyHealthEnvironment)
3. Accounting for all access tokens listed under their assets on BASOL at all times
4. Ensuring BASOL is updated to reflect name, company, contact number, contract end date and pre employment check level for each token issued
5. Ensuring pool assets are not anonymously assigned e.g "Pool Card", "Spare". Any cards considered to be anonymously registered will be de-activated.
6. Ensuring that pool cards are de-activated on BASOL when not in use.
7. Briefing contractors on BT Security Access Policies and the Security Handbook for Non-BT Organisation at http://snip.nat.bt.com/SecurityHandbook. Examples include displaying their company ID cards, not tailgating or allowing anyone else to tailgate, only accessing areas they are authorised to access, and ensuring that these areas are secured on exit as per policy.
8. Ensuring that the access on the pool card is kept to the minimum to allow the operational role to be undertaken and does not contain access to areas not required. Audits will be regularly carried out on access assigned to a pool card and will be removed as necessary.
9. Ensuring the AS/CLM role and associated responsibilities are handed over to a new AS/CLM when roles change.
10. Completing six monthly audits of tokens and access rights assigned to them.
11. Immediately reporting lost/stolen access cards and keys to BT Security on 0800 321 999 or +44 1908 641100.