Physical Access to BT Sites and Buildings by 3rd Party Companies.

Content

1. Introduction

This document provides guidance information to the 3rd Party Company's Authorised Signatories to ensure that they are aware of their roles and responsibilities, the requirements of BT's Access Policy and how to access BASOL (Building Access Systems on-Line) Redside to apply for access cards, security keys and where applicable BT produced ID cards, for their own employees, contractors or sub-contractors, who have a requirement to access the BT estate.

2. The Authorised Signatory

As a 3rd Party Authorised Signatory you have been authorised by your BT Sponsor to apply on behalf of your organisations, and any of your contractors/sub contractors workforce for unhosted access to those areas within the BT estate where your organisation has an operational and contractual requirement to access. The BT Sponsor has already managed your access profile (Estate) and has created in BASOL a list of BT buildings and controlled areas for these buildings (Zones) that you will see in BASOL when you log on as an authorised signatory.

2.1 Roles and Responsibilities

The 3rd Party Authorised Signatory has overall responsibility for ensuring that:

- employees in their organisation and also the employees of any of their contractors/agents who need to access the BT estate are fully aware and comply with the requirements of the BT Security Access Policy, contained in this guidance document, and of the BT Security Handbook for 3rd Party Companies, copies of which can be obtained from the relevant BT Sponsor. Evidence of compliance to be made available at the request of BT to demonstrate that the information has been briefed, accepted and understood.

The 24 hour contact point is required for use by BT in exceptional circumstances where a security issue requires resolution, to verify the bona fides of an individual where 'pool' EAC cards are in use or to facilitate remote access release. Any validation of identity and authority to access will always be referred to the 24 hour contact number. See Appendix C – 24 Hours Contact Details

Unhosted access is wholly dependant upon a regular monthly validation of personnel data held on BASOL for all people, including any sub contractors, who have an authorised and clear operational need for frequent access to the BT estate. This validation is to ensure that any leavers are removed from the system and their access cards and keys recovered and returned.

On completion of the attached authorised signatory form (ASF1 form) the nominated person within the 3rd Party Company is accepting full responsibility for ensuring that:

- The requirements within the content of this document and any associated documents (including any subsequent amendments or specific requirements as may be imposed from time to time) are fully adhered to at corporate and individual level by the 3rd Party Company and its employees and contractors/agents and that they are made formally aware of these obligations.
- Individuals are formally made aware of their obligations when within BT areas and that they adhere to the appropriate BT security requirements.

A full audit trail of access card and mechanical key issue to individuals, together with evidence of receipt by the individuals, must be in place and be maintained at all times by the authorising signatory and be available for inspection by BT on demand. These audit requirements must also

be adhered to by all sub contractors when they receive cards and keys from the authorising signatory and then issue them out to their own employees or to any sub contractors.

3. BT Security Access Policy Requirements

The following relate to BT Security Access Policy requirements and must be fully adhered to at corporate and individual level by the 3rd Party Company and its employees and contractors/agents.

BT has the right to verify adherence through independent checks that will be completed without any prior notification. Any non-compliance with BT's requirements could result in an individual or organisation being denied access to the BT estate.

It is BT policy to take legal action in respect of any crime committed against BT property, people or interests.

3.1 Employee References

As a supplier you will be expected to comply with the policy and make a contractual commitment to that effect.

The full policy details are available in the pdf document Third Party Pre-Employment Checks Policy .

Please note: BT have the right to audit any 3rd Party Company processes and procedures which relate to the access application process and employees employment checks.

3.2 Wearing of Identity Cards

3rd Party Company personnel and those of their contractors/agents must be in possession of, and display, their own company photo ID cards at all times when within the BT estate. The ID card must comprise at least:

- Name of bearer
- Image (photo) of bearer – that must be clear and be a true likeness of the person
- Name of company
- Card number
- Enquiries contact number

3rd Party Company personnel must accept that they may be challenged by any BT person seeking to establish their bona fides for access to the BT estate. Where the BT employee considers that further checks are necessary then the 3rd Party employee must co-operate and provide any additional information required to ensure a speedy resolution.

3.3 Data protection & commercial confidentiality

Any information, which becomes available to the 3rd Party Company or its contractors/agents, is subject to both any confidentiality agreements signed by the 3rd Party Company and the Data Protection Act where appropriate.

3.4 Duty of care

Any 3rd Party Company employee or those of its contractors/agents are required to exercise a duty of care when operating on the BT estate and must not under any circumstances disconnect, make connection to or otherwise tamper with BT equipment.

In the event of any actual or suspected security incident or crime involving any BT property or asset must be reported immediately to BT Security on 0800 321 999. In circumstances where the incident involves 3rd Party Company property then the employee is also responsible for reporting the matter as required by their employers.

3.5 Health & Safety

3rd Party Company employees as well as those of their contractors/agents must exercise a duty of care towards BT property in the event of a fire or suspected fire being identified and take appropriate action.

3.6 On Site Security Responsibilities

Details of the security responsibilities of individuals when on a BT site are contained in the Security Handbook for 3rd Party Companies. The authorising signatory of the 3rd Party Company must ensure that a copy of the Security Handbook is provided to all individuals of their own company or of any sub contractors which they may use, whom access the BT estate. An audit trail demonstrating that the handbook has been issued to individuals must also be in place, which demonstrates that handbooks have been received and that the content has been read and understood.

3.7 Use of EAC tokens/PINs

The issued token and associated PIN is only to be used by the named employee; the PIN should be committed to memory. Under no circumstances should the PIN be written on the issued token. Failure to comply with this requirement will result in the immediate deactivation of any ‘guilty’ cards or possible removal of all access tokens if this practice is found to be widespread.

When despatching EAC tokens and PIN it is essential that they be sent under separate cover.

3.8 Action to be taken in respect of 'Leavers' & EAC token/key Loss

When any person ceases to have a requirement for access to the BT estate it is the responsibility of the Authorised Signatory to:

- ensure recovery of EAC token/security key
- ensure that EAC tokens issued to named individuals are immediately deactivated - this being achieved by ceasing the UIN of the person using the appropriate proces or by removing the card(s) access and recoveresd as soon as possible thereafter.
- ensure that 'pool' cards are immediately recovered and immediately deactivated using BASOL Red side, this being achieved on BASOL Red side by removing the card(s).

The Authorised Signatory is responsible for ensuring that all employees (including those of its contractors/agents) are aware that the loss of any EAC token/security key is reported immediately to BT Security on 0800 321 999.

3.9 Action to be taken when there is a change to the BT sponsor or authorised signatory.

When there is a change to the Authorised Signatory in the 3rd Party Company then a new ASF1 found at Appendix B in this document, must be completed and sent to the BT Sponsor for approval who will then forward to sam@bt.com for processing.

4 Audit of 3rd Party Company's assets

After a predetermined and definable level of time, set by BT, the authorised signatory of the sponsored organisation will receive a request to audit their assets as listed on BASOL Red side and for confirmation to be acknowledged that this has been completed. If the authorised signatory does not confirm that this task has been completed, then an escalation e-mail is automatically sent to the BT Sponsor to action and if the BT Sponsor does not acknowledge this e-mail, it could result in all access cards/token and privileges being revoked.

5. Author Details

Security Access Management
Secure BT
e-mail: sam@bt.com

6. Document History

Version	Date	Details of Change
Issue 01	May 2009	First issue.
Issue 02	May 2015	Revised

This form provides the BT Security Access Control Management team with the BT approved nominated names, addresses, company details and signatures required for the authorisation of Non BT Access Application requests.

RedSide Company- Details of Company and who is or will be the Main Authorised Signatory

Contract Number		**Company Name**	
Name of the Main Contact at the company and Tele Number:		**Full Address (inc Country if outside the UK)**	
Is the address above where people will be located and that assets are to be delivered to?			**Yes/No** (If no please provide address in box below)
Contract Description			
Contract Start Date		**Contract end Date**	
Is the Connecttosystems clause included in the contract?			**YES / NO**
The authorised signatory/delegate must be compliant with BT's Level 2 Third Party Pre-employment Checks Policy (attached to this document) subject to in-country law. You must retain evidence to show compliance if requested by BT. The BT sponsor will send you an email requesting a declaration.			

Authorised Signatory- Details of who will be the New Authorised/Delegate Signatory

Name of Person(s) who will be accessing the Access Control System		
Position Held		
Address (Inc post Code, if different from above)		
Tele. No.		
e-mail Address		
Date		
Have you read and understood the requirements in the Security Handbook attached to this document?		**Yes / No**
Have you read and accepted the system access requirements for using BT systems attached to this document?		**Yes / No**

BT SPONSOR

Name		**OUC**	
EIN		**Tele Number**	
3rd Party Pre-employment checks **Have you received an email from the Redside Basol Company confirming the Authorised Signatory/Delegate is compliant with all the required BT Level 2 pre-employment checks as documented in the Third Party Pre-Employment Checks Policy (attached to this document) subject to in-country law, and these checks are complete and clear.** **N.B. – refer to the 'sample emails' in the attached document.**			**YES / NO**

BT SECURITY


Third Party Pre-Employment...
Security Handbook
Connecttosystems
Sample emails.docx

Appendix B

OLO/MOLO/Third Party 24 Hour Contact Details - CON1

Provision of a 24 hour contact number is a mandatory requirement of BT's Access Security policy as outlined in the access application process to BT areas by 3rd Party Companys process document. This contact number will be used by the BT Security Management Centres in Milton Keynes and in Bedfordshire for the validation of third parties accessing.

Company Name	
24 Hour Contact Number	
Contact Name (if applicable)	
National/Region Number (please delete)	
Project Name:	Local Loop Unbundling Project Reach Other (please specify)

When completed please email the form to sam.customer.services@bt.com

Any queries please contact the BT Security Access Management Team on 0800 321999.