BT Physical Access Application Process For Non-BT/Openreach Organisations

Contents

1 Introduction

This document provides guidance on the process and the roles and responsibilties for managing building access, cards and security keys for Non-BT/Openreach people organisations with a requirement to access BT sites and buildings.

2 Definitions

ACM	Access Control Management Team, supporting those involved with the management of access for Non-BT/Openreach organisations, arranging BASOL Redside access, issuing cards and keys and ensuring compliance with security requirements. The team can be contacted via sam.customer.services@bt.com for enquiries about this process/help with the BASOL Redside application or 0800 321999 for first line support relating to access issues/general security advice.
Agent	Refers to any person employed directly by the 3rd Party Company or to any person employed as a direct or indirect sub-contractor on behalf of the 3rd Party Company.
AS	Authorised signatory/delegates in a Non-BT/Openreach organisation authorised to manage building access, cards and keys for people who need access to BT sites and buildings.
BT	All BT Group companies including EE and Plusnet.
BASOL Redside	Building Access System OnLine – a redside application used by approved individuals within a Non-BT/Openreach organisation to manage access to authorised areas of BT sites/building on behalf of their community.
CLM	Contract Liason Manager - a BT manager authorised to manage temporary access cards for short term use by a Non-BT/Openreach agent (up to 28 days).
Identity Management Process	For BT suppliers this is the HR process at https://hr.bt.com/en-gb/recruiting-resourcing/non-employee-classifications/non-employee-uin-request For Communication Providers and Tenants this is self-managed via the Identity Services Portal

3 Overview

Where agents of a Non-BT/Openreach organisation require access to BT sites or buildings, they must obtain authorisation by adhering to the BT Security Access Policy.

BT has put in place processes intended to protect the assets of BT/Openreach and the Non-BT/Openreach organisation. These processes enable authorised unhosted access to BT's sites and buildings and allows the Non-BT/Openreach organisation to obtain access, cards and keys from BT either directly or via a BT/Openreach Line Manager/Contract Liaison Manager (CLM).

When an agent from the Non-BT/Openreach organisation enters BT sites or buildings they should be aware of their obligations to maintain the integrity of BT's assets. A BT Security Handbook and

Best Practice Guide for Non-BT People provides general guidance concerning the responsibilities to ensure that site security is maintained. It also gives advice on how to contact BT security and contacts for fault reporting. All people granted access to BT's estate under this process must be familiar with these documents – any queries should be directed to the AS, CLM or Line Manager as appropriate.

4 Options for managing access to the BT Estate

All people accessing the BT estate must be in possession of, and display, their own company photo ID if they not using BT provided combined photo ID/access cards. This is a mandatory requirement (BT Security Policy 1 – Personal Security); failure to comply could result in removal from site.

4.1 **Option 1 (Redside)**

Requesting access directly via the BASOL Redside System

This option provides the flexibility necessary for Non-BT/Openreach organisations to administer their own requests for access to BT buildings and sites.

An Authorising Signatory (AS) and up to 10 delegates can apply for building access, cards and keys on behalf of their employees/agents using the BASOL Redside System.

The AS and delegates are approved by a BT/Openreach manager who sponsors the company and is responsible for ensuring compliance with security policies.

- The Sponsor will raise a request to the Access Control Team for the company to have access to the BASOL Reside System. An ASF1 form must be completed for each AS/delegate to provide the required information, assurance and approvals.
- Up to date records of all personnel who need access to the BT estate for more than 28 days must be maintained using the Identity Management Process. This ensures that access, cards and keys can be managed effectively for the Non-BT/Openreach organisations community.
- Access, cards and keys can be requested using the BASOL Reside System.
  - Access and keys requested should be the minimum required for the person's role and access should be removed when it is no longer required.
  - For BT/Openreach Suppliers: During 2018 new card requests will require submission of a passport style photo for so that a BT/Openreach contractor photo ID card can be provided, until this is fully implemented a standard access card will be provided. You will be advised by the Access Control Management Team when the process change affects you.
- For people with a short term or occasional access requirement, the AS can request approval to manage temporary access, cards and keys that can be allocated via BASOL Redside for a period of up to 28 days. These arrangements must comply with the requirements of the Pool Card Policy.

A BASOL Redside System User Guide will be provided and support will be available from the Access Control Management Team.

4.2 **Option 2 (Greenside)**

Obtaining access via a BT/Openreach Line Manager/CLM

Suitable for smaller contracts where it is practical for a BT/Openreach manager to administer access requirements for the contracted personnel.

Under this option a designated BT/Openreach Line Manager/CLM can obtain all of the necessary access, cards and keys on behalf of the contracted personnel.

- For people who need to access to BT sites for more than 4 weeks, a UIN should be requested via the Identity Management Process and the necessary access, cards and keys can be requested by the registered BT/Openreach Line Manager using the BASOL system.
- For people with a short term or occasional access requirement, the BT/Openreach Line Manager can request approval to be registered as a CLM to manage temporary access, cards and keys that can be allocated via BASOL for a period of up to 28 days. These arrangements must comply with the requirements of the Pool Card Policy.

5 Roles and Responsibilities

5.1 **Sponsor**

A permanent BT plc or Openreach Ltd employee, normally holding a management position or above, with responsibility for the work activity for which unhosted access is required. In exceptional circumstances, the ACM Team may agree to a person who is not a manager taking on the Sponsor role subject to them having sufficient authority and influence to ensure compliance with security requirements.

The Sponsor has overall responsibility for ensuring that:

- the Authorised Signatory (including nominated delegates) have sufficient authority within the 3rd Party Company to ensure compliance with BT's requirements. They must also have appropriate knowledge to manage access to the BT estate by their agents.
- the Authorised Signatory fully understands the responsibilities (implied and stated) outlined in the documentation provided by BT.
- updates to BT policy and guidance documents are issued to Authorised Signatories for implementation and compliance. See section 8.
- the (ASF1) Authorised Signatory Form is correctly completed following the guidelines included on the form.
- the ACM team is immediately notified of any changes in the 3rd Party Company such as Authorised Signatory changes, Company name change and the ceasation of any existing contracts between the 3rd Party Company and BT/Openreach.
- access is only provided to the necessary buildings/areas. Information relating to the sponsored companies access profile (estate) must updated in BASOL or passed to the ACM Team so that they can configure and maintain the access profile on behalf of the Sponsor.
- any UIN requests are approved before processing and UINs are promptly ceased when an individual no longer requires access to buildings/systems
- that a replacement is found to take over the role of Sponsor should the current Sponsor move to a different post or leave the company.
- any issues regarding access to the BT estate by the 3rd Party Company are resolved.
- Audits requested by BT are completed as required.

5.2 Authorised Signatory and Delegates (AS)

A 3rd Party AS has been approved by a Sponsor to apply for and manage unhosted access to areas of the BT estate where the Non-BT/Openreach organisation has an operational/contractual requirement for access.

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

- Agents who need to access BT sites and buildings are fully briefed about and comply with the security requirements outlined in the Security Handbook for Non BT Organisations, the Pool Card Policy, the Environmental Policy and other policy/guidance documents issued by BT.
- The requirements within the reference documentation must be fully adhered to at corporate and individual level by the 3rd Party Company and its agents who must be made aware of their obligations when within BT areas and ensure that they adhere to the appropriate BT requirements.
- A 24 x 7 contact point is provided for use by BT in exceptional circumstances where a security issue requires resolution, to verify the identify and rights of access of an agent. This may be used to manage a security incident 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 A – 24 Hours Contact Details
- Unhosted access is approved for people with a BT UIN (Unique Identification Number) and for occasional users managed under the pool card controls who have an authorised and clear operational need for infrequent access to the BT estate.. This validation is to ensure that any leavers are removed from the system; their access cards and keys must be recovered and returned to the address at 8.8
- Evidence of compliance is made available at the request of BT to demonstrate that the information has been briefed, accepted and understood.
- A full audit trail of access card and mechanical key issue to agents, together with evidence of receipt by the individuals, is in place and maintained at all times by the authorising signatory and be available for inspection by BT on demand.
- Audits requested by BT are completed as required.

5.3 Line Manager

Line managers are responsible for ensuring:

- Compliance with Security policies found at https://intra.bt.com/bt/security/policy/security-policies/Pages/index.aspx
- Identitity Management Processes are implemented effectively for new joiners/leavers.
- Audits requested by the ACM team are completed as required.

5.4 CLM

A CLM must:

- Ensure that the Line Manager/BASOL Redside process is used where access is required for more than 28 days.
- Adhere to the requirements of the pool card policy at https://intra.bt.com/bt/security/policy/security-policies/policydocs/Pool%20Card%20Policy%201a.docx

- Ensure that pool card users are fully briefed about and comply with the security requirements outlined in the Security Handbook for Non BT Organisations, the Pool Card Policy, the Environmental Policy and other policy/guidance documents issued by BT.
- Keep accurate records for pool card allocation by following the user guide at https://intra.bt.com/bt/security/me/howdoi/Documents/basol-pool-card-management-changes.docx
- Ensure that audits requested by BT are completed as required.

6 Getting started

6.1 Redside Company Process

Although we aim for this to be as quick and easy as possible, there are a number of steps and approvals to be completed and you should allow 5-10 days for the end to end process to be completed. The timeframe can reduce if everyone involved responds promptly with information and approvals but if there are delays in up/down stream provisioning processes this could extend the timescale.

6.1.1 Sponsor

The Sponsor role can be requested by contacting the ACM team and submitting a completed ASF1. Further information will be provided by the ACM team.

The existing Sponsor is responsible for ensuring that the role is properly handed over if they are changing roles or leaving the business. - The new Sponsor must submit an ASF1 form for each AS for processing by the ACM team – this will include the setting up the necessary system access arrangements.

The Sponsor defines the access profile (estate) that the Non-BT/Openreach organisation is allowed to request access to. This can be configured in BASOL by the Sponsor or by the ACM team on behalf of the Sponsor.

6.1.2 Authorised Signatory

The AS should ensure that the appropriate Identity Management Process has been followed to create the community of agents that they will manage. This may be carried out in consulation with the Sponsor. In some cases UINs are raised manually by an HR team and you should allow time for that work to be completed.

Once the UINs have been created, they will flowed into the BASOL Redside company in an overnight batch update. Then the AS can order cards, keys and access as required (ensuring that access is kept to the minimum required to do the job). Where photoID cards are required, digital photos (passport style) saved as the individuals UIN as the filename should be submitted to photos.soc@bt.com.

Cards and keys will be issued by the ACM team and sent to the address provided.

Access requests may require approval and could therefore be subject to delay – you can see a status update for each order in BASOL.

The Security Handbook for Non BT Organisations covers that requirements for accessing BT sites and buildings – all card/key users must be briefed on the requirements.

Access must be removed when it is no longer required and cards/keys/tokens that are no longer required must be returned to the ACM team at the address in section 8.8.

When there is a change to the Authorised Signatory or delegate in the 3rd Party Company, a new ASF1 must be completed and sent to the Sponsor for approval who will then forward to sam.customer.services@bt.com for processing. If the authorised signatory or delegate is a replacement, the ACM team should be notified so that system access rights can be ceased when they are no longer required. UINs for AS/Delegate must be ceased when access is no longer required.

6.2 Greenside Line Manager Process

The Line Manager role is automatically granted to anyone who has people reporting to them that are not managed via the BASOL Reside process.

You can order cards, keys and access just as you would for your direct reports (contractors will be listed on BASOl under a contractor heading). The same processes, rules and policies apply as if you were ordering for yourself or your direct reports.

It is the responsibility of the losing manager to transfer identities to a new manager – see https://hr.bt.com/en-gb/recruiting-resourcing/non-employee-classifications/third-party-identities-guidance-for-managers

6.3 CLM Process

The CLM role can be requested by raising an order on BASOL. A member of the ACM team will contact you to establish that pool cards is an appropriate process for managing the access requirements. You will be provided be asked to comply with the Pool Card policy and confirm that you will make card users aware of their security, health, safety and environmental responsibilities. For an AS this is requested by a Sponsor in discussion with the ACM team.

Once you have been approved as a CLM you can create an order in BASOL for pool cards/keys and these will be sent to you at the address your provided by the ACM team. Note: Your order may be challenged by the ACM team to ensure that appropriate risk controls are in place.

Once you receive your pool cards/keys you can assign them for short term use by following the process documented at https://intra.bt.com/bt/security/me/howdoi/Documents/basol-pool-card-management-changes.docx

Where a Greenside CLM needs to transfer responsibilities to another manager, the new manager should first raise an order for CLM status on BASOL. The ACM team provide advice on next steps. You can set up a delegate in BASOL who can manage your pool cards/keys on your behalf.

For Redside companies, pool cards and keys are managed collectively by the AS and delegates.

7 Audits

7.1 Roles

Validation of Sponsor/AS/CLM roles will be required at intervals determined by BT and confirm that this has been completed. If the individual does not confirm that this task has been completed, then an escalation e-mail is sent to the individuals Line Manager/Sponsor to action

and if the audit is still not completed, it could result in all access cards/keys and access privileges being revoked.

7.2 Identities and Assets

The CLMs/AS of the Non-BT/Openreach organisation will required to audit company identities and assets as listed on BASOL at intervals determined by BT and confirm that this has been completed.

If the CLM/AS does not confirm that this task has been completed, then an escalation e-mail is sent to the CLM's Line Manager/Sponsor to action and if the audit is still not completed, it could result in all access cards/keys and access privileges being revoked.

8 Documents & Help

Authorised Signatories should contact the Sponsor for their organisation to obtain copies of documentation.

Line Managers, CLM's and Sponsors should refer to the Security and HR Websites at or contact **sam.customer.services@bt.com** for advice and reference documents as required.

8.1 BT Security Access Policies

https://intra.bt.com/bt/security/policy/security-policies/Pages/index.aspx

8.2 ASF1 – Authorised Signatory Form

8.3 Best Practice Guide for Non-BT People

Also available from
https://groupextranet.bt.com/selling2bt/Downloads/BestPracticeGuideforNon-BTPeopleV1.pdf

8.4 Pool Card Policy

8.5 Security Handbook for Non-BT Organisations

Also available from
https://groupextranet.bt.com/selling2bt/working/third_party_access/default.html

8.6 BASOL Redside System User Guide

Available on request from **sam.customer.services@bt.com** for an approved AS.

8.7 Photos

Digital images for ID cards should be submitted to photos.soc@bt.com – the photo specification can be found at https://fixit.bt.com/pages/article.aspx?articleid=353&viewed

8.8 Return Address

Cards/Keys/Tokens that are no longer required should be returned to
Business Reply RTTY-KCXR-RAHE, PP SH15, Bletchley Admin Block D
82 Tavistock Street, Bletchley, Milton Keynes, BUCKS, MK2 2AP.

Please don't cut cards up when you return them, just deactivate them on BASOL

9 Enquiries

Access Control Management Team
e-mail: sam.customer.services@bt.com

10 Document Control

Document Owner: Sarah Arnold, Physical Access Control & Security Manager – sarah.arnold@bt.com

Document Approver: Guy Voice, Senior Security Operations Manager – guy.voice@bt.com

11 Document History

Version	Date	Details of Change
Issue 01	May 2009	First issue.
Issue 02	May 2015	Revised
Issue 03	June 2018	Updated with Pool Card & Photo ID Policy changes and Greenside process included. ASF1 removed so that this document can be appended to that form as a reference document. Approved by Guy Voice, VQH1.
Issue 03.1	Aug 2018	Email address updated in section 6.1.2 to correct typo

CP/Reach/Tenant/Supplier Third Party 24 Hour Contact Details - CON1

Provision of a 24 hour contact number is a mandatory requirement of BT's Access Security policy.

This contact number will be used by the Access Control Management and Security Control Centre teams for the validation of third parties accessing BT sites and buildings and to manage security incidents.

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

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

Any queries please contact Security on 0800 321999.

Personal data will be managed in accordance with BTs Data Privacy Policy and will be retained for the duration of the contract or relationship with BT/Openreach