SECURITY HANDBOOK

REQUIREMENTS FOR NON BT/OPENREACH ORGANISATIONS WHEN ACCESSING BT SITES AND BUILDINGS

1	**DEFINITIONS & CONTACTS**	
1.1	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.
1.2	Access Card	A card issued by BT in the form of either a combined ID/Access Card or a standard access card to operate the electronic access control system. The sharing of ID/access cards is forbidden and will result in access being denied.
1.3	Authorised Signatory (AS)	A person within the 3rd Party Company who has been authorised by a BT/Openreach Sponsor to manage unhosted building access, cards and keys for their agents. The individual (and their authorised delegates) must have: ➢ sufficient executive authority to ensure compliance with BT's requirements and ➢ the necessary level of knowledge to determine justified access to the BT estate by agents of the 3rd Party Company.
1.4	BT area	Any site, building or zone that is wholly occupied by BT Group plc.
1.5	Contract Liaison Manager (CLM)	A BT manager responsible and accountable for authorising and subsequent in-life management of building access, cards and keys to 3rd parties for use on a temporary basis (up to 28 days) for unhosted access to BT sites/buildings.
1.6	EAC	Electronic Access Control
1.7	Escorted access	Escorted access requires that a nominated BT/Openreach person or authorised security contractor continually escort an agent at all times when in BT areas.
1.8	Host	The Host is a person responsible for any visitor who is subject to hosted access for the duration of the visit.
1.9	Hosted access	Permits access to a BT area when the requirements for unhosted access cannot be met or are not appropriate, the host is responsible for providing access and compliance with security requirements.

1	**DEFINITIONS & CONTACTS**	
1.10	ID card	3rd Party company ID cards which must include as a minimum: • 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 • ID cards are not to be used by anyone but the named bearer, any person found doing so will be removed from BT property immediately New access card requests for agents of BT/Openreach suppliers will require submission of a passport style photo so that a BT/Openreach contractor photo ID card can be provided, until this is fully implemented a standard access card will be provided.
1.11	Key	Key for use operating a mechanical lock.
1.12	Law Enforcement Agency "Dawn Raids"	Any official body demanding entry to BT premises with permission from a Court, or other legal right of access.
1.13	PIN	Personal Identification Number used in conjunction with an access card to gain entry to specific EAC areas that are controlled with a 'PIN and Prox' reader. A PIN must never be written on the access card, doing so is a disciplinary matter.
1.14	Sponsor	A permanent BT/Openreach employee holding a management position with responsibility for the work activity for which unhosted access is required.
1.15	Unhosted Access	Permits movement within agreed and designated BT areas without the need for either a permanent escort or host.
1.16	UIN	Unique Identification Number issued by BT's identity management systems – the Contingent Worker system (CWK) for contractors and Identity Services Portal (ISP) for tenants/communication providers
1.17	Visitor	Any non-BT/Openreach person requesting access to BT sites and buildings on an infrequent/irregular basis who does not have either an Access Card, Key, or ID card to gain authorised unhosted access.
1.18	**Contact Details:** Security Control Centre	UK Freephone - 0800 321999 Rest Of The World Freephone - 00800 0032 1999 International Direct Dial = 0044 1908 641100

SECURITY HANDBOOK

REQUIREMENTS FOR NON BT/OPENREACH ORGANISATIONS WHEN ACCESSING BT SITES AND BUILDINGS

1	**DEFINITIONS & CONTACTS**	
1.18	**Contact Details:** Property and Facilities Services Helpdesk (service provided by CBRE)	England, Scotland and Wales - 0800 223388 Northern Ireland - 028 9021 5555 Republic of Ireland - 00353 1 432 5566 International - https://intra.bt.com/bt/propertyandfacilities/international
1.19	Denial of access	BT retains the right to refuse access to any of its sites at any time

2	**GENERAL**	
2.1	Adherence to BT requirements	• The security requirements specified by BT policy will be adhered to at all times, including amendments or specific requirements that may be implemented from time to time. Security policy requirements can be found at https://intra.bt.com/bt/security/policy/security-policies/Pages/index.aspx and can be provided by BT/Openreach Sponsors for 3rd parties who cannot access the URL. • It is the responsibility of the CLM or 3rd Party Company AS to clearly brief the contents of this handbook to each agent working on their behalf before access to BT areas is provided AND to ensure that the requirements are enforced. • BT has the right to verify compliance through independent checks that may be carried out without any prior notification.
2.2	Sites with Electronic Access Control (EAC) systems - Use and custody of access cards.	• Access cards remain the property of BT Group plc and will only be issued to the CLM or 3rd Party Company AS. • Issued cards and associated PINs are only to be used by the agent that they have been formally issued to and only at the designated buildings where authorised access has been granted to enable the 3rd Party Company to carry out their business. • The PIN should be committed to memory and **under no circumstances should the PIN be written on the issued card.** Failure to comply with this requirement will result in the immediate deactivation of non-compliant cards or removal of all access cards if this practice is found to be widespread. Exceptionally, where a written record is kept, this must be held separately from the access card at all times. • The 3rd Party Company and its agents are responsible at all times for the safe custody of the access card and PIN. Loss, compromise or damage must be reported immediately to the Security Control Centre.

2	**GENERAL**	
		• Cards that are no longer required must be deactivated and returned to Security at this address for secure disposal/reuse (no stamp required): 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 before returning them.
2.3	Sites with Mechanical Locks - Use and custody of keys	• Security keys remain the property of BT Group plc and will only be issued to the CLM or 3rd Party Company's AS. • The key is only to be used by the agent it has been formally issued to. • No form of labelling should be applied to the key which in any way attributes its connection with BT • The 3rd Party Company and its agents are responsible at all times for the safe custody of the key. • Loss, compromise or damage is to be immediately reported to the Security Control Centre, BT reserves the right to charge for replacement keys • Keys that are no longer required must be returned to Security at this address for secure disposal/reuse (no stamp required): Business Reply RTTY-KCXR-RAHE, PP SH15, Bletchley Admin Block D, 82 Tavistock Street, Bletchley, Milton Keynes, BUCKS, MK2 2AP
2.4	Recruitment of employees - references.	• 3rd Party Companies must comply with the 3rd Party Pre-Employment Checks Policy and exercise due care when recruiting agents who will have access to BT premises. Note: Tenants and communication providers should implement L1 checks as described in the Policy.
2.5	Contact Procedure	• 3rd Party companies are to ensure they provide and maintain, a current 24-hour x 7-day contact number for use as required by BT to verify an agent or manage a security incident.

2	**GENERAL**	
2.6	Authorised Agents	• 3rd Party companies are required to maintain up to date records of all agents who have an authorised requirement to access their areas on BT property: ➢ Permanent and long term access (in excess of 28 days) will only be provided to an agent an active with a UIN. As soon as access is no longer required, the agents UIN must be terminated or modified to ensure that access is revoked promptly by the automated leaver process. ➢ Card user information must be maintained via BASOL for pool/temporary access cards to register them to an identifiable individual. Where card users are not identifiable, access will be revoked. • These details enable: • The issue and replacement of permanent and temporary building access, cards and keys. • BT to validate the identity and right of access of the agent concerned. • Failure to provide and routinely maintain these details could result in an agent being denied access to a site/building and/or refusal of an access/card/key request.
2.7	Access by law enforcement and emergency services	• Any request by law enforcement or emergency services for access to BT areas should be referred immediately to a BT agent or alternatively to the Security Control Centre.
2.8	Construction Work on Site	• Any construction work that affects, or may affect, the external or internal security of the building (e.g. scaffolding, hoists, ladders etc) may require its own security measures. Further advice should be sought from the Property and Facilities Services Helpdesk.
2.9	Commercial Confidentiality & Data Protection Act	• 3rd Party companies must ensure that their agents are aware that any information they may have access to while working in BT areas is to be considered confidential. • This information may also be subject to the General Data Protection Regulations
2.10	Environmental Policy	• 3rd party companies must ensure that their agents are clearly briefed and comply with BT's environmental policy.

3	**ACTIVITY ON SITE**	

3.1	**Wearing of ID cards**	• At all times when on BT property, all agents must display a valid ID card. 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.
		New/replacement access card requests for agents of BT suppliers will require submission of a passport style photo so that a BT/Openreach contractor photo ID card can be provided, until this is fully implemented a standard access card will be provided. For other 3rd parties, if requested, BT can provide a combined access/ID card that can be used and displayed at all times whilst on BT premises.
		• Agents must accept that they may be challenged by any BT/Openreach agent seeking to verify their identity and right of access to the BT building/site/internal area. Where the BT/Openreach agent considers that further checks are necessary, the 3rd party agent must co-operate and provide any additional information required to ensure a speedy resolution.
		• If an agent's identity/right of access cannot be established, that individual may be required to leave site and surrender any access cards and/or keys held until the situation can be resolved.

3.2	**Entry to/Exit from Site**	• Access to site will only be via the designated gate, using the padlock (where provided). • When the site is unmanned the gate must always be secured following entry or exit. • Where a site is externally alarmed, agents must contact the Security Control Centre before entering to prevent any false alarms.
3.3	**Entry to/Exit from Building**	• Unescorted access to designated buildings will only be permitted when an agent has an ID card and an appropriate access card/key. In all other circumstances the agent will either be permanently escorted or be allowed hosted access. • The correct procedures for operation of the EAC and intruder detection systems must be observed for each entry and exit. • Only designated and previously agreed entry points are to be used. • Agents must not allow the entry of an unhosted individual to BT premises, deliberately or negligently, unless that person can prove that they have authorisation to enter the building by means of an ID card and a valid access card/key.

3	**ACTIVITY ON SITE**	
3.4	**Movement within Building**	• Agents are permitted to access only their own designated accommodation and must not access any other areas that they are not authorised to enter to deliver the requirements of their contract. • There is no right of access to welfare facilities but these may be used where they are located en-route to the designated area and do not require access to other areas not approved for use by the 3rd party company. • If the building alarm system goes into auto-set a local sounder will activate. If this happens while on site, the agent must ring the Security Control Centre to register their presence on site. • Internal or external alarmed doors must not be propped open, if you are unsure please contact the Security Control Centre
3.5	**BT & 3rd Party Equipment**	• Agents must not under any circumstances disconnect, make connection to, remove or tamper with BT/Openreach equipment or equipment of other third parties unless they are authorised.

4	**ACTIONS WHEN UNABLE TO ACCESS A SITE/BUILDING**	• If an agent is unable to access a designated site/building using a correctly programmed access card allocated to them, the issue should be reported to the Security Control Centre. • If an agent's card is not correctly programmed for the designated site or they have not been provided with an appropriate key, they should contact their company representative (AS/CLM) as appropriate.

5	**REPORTING OF SECURITY INCIDENTS AND CRIME.**	• Actual or suspected security incidents/crimes involving BT or 3rd Party Company property should be reported immediately to the Security Control Centre. • The 3rd Party Company must give their full co-operation to BT/Openreach to investigate any breaches or suspected breaches of security which involve BT property or BT assets. • Where a security incident involves 3rd Party Company property, the agent is also responsible for reporting the issue within their own organisation and/or police as appropriate. BT is not responsible for safeguarding or investigating the loss of any property belonging to the 3rd Party Company (including money) brought onto BT's premises.

6	**REPORTING OF LOST/STOLEN ACCESS CARDS OR KEYS**	• The loss of an access card or key must be reported immediately to the Security Control Centre. Replacements can be requested from BT by the AS or CLM via BASOL (Building Access System On-Line). BT reserves the right to charge for replacement cards and keys.

7	**REPLACEMENT OF DAMAGED ACCESS CARDS OR KEYS**	• Any access card or key which is damaged to an extent where it does not reliably function must also be reported to the Security Control Centre. Replacements can be requested from BT by the AS or CLM using BASOL and the damaged card/key should be returned to BT at the following address (no stamp needed): Business Reply RTTY-KCXR-RAHE, PP SH15, Bletchley Admin Block D, 82 Tavistock Street, Bletchley, Milton Keynes, BUCKS, MK2 2AP

8	**BT PROSECUTION POLICY**	• It is BT policy to take legal action in respect of any individual identified as having committed a crime against BT property, assets (including information), people or interests.

9	**FIRE SAFETY PRINCIPLES**	The 3rd Party company is responsible for briefing agents that: • There is no smoking in BT buildings • All paper and other waste is to be removed from site on the same day as the waste is created. • Only correctly installed equipment that meets all necessary electrical and safety standards may be kept on the BT site. • Agents must exercise a duty of care towards the BT/Openreach property in the event of a fire or suspected fire being identified and take appropriate action.

10	**ACCESS BY AND ESCORTING OF VISITORS (INCLUDING CONTRACTORS)**	• Pool/Temporary access cards can be issued by authorised AS/CLMs for use by people with a short term access requirement (up to 28 days). The AS/CLM is responsible for ensuring compliance with the Pool Card Policy. • Agents who have authorised unhosted access to a designated BT building may host visitors provided that: ➢ The visit is in direct connection with their work areas/responsibilities. ➢ Names and details of the visitor(s) or contractor(s) is supplied to the Security Guard/Reception Team and day passes obtained (where appropriate). ➢ The visitor(s) or contractor(s) must be directly supervised at all times by the agent with authorised access when in BT areas. ➢ The visitor(s) or contractor(s) must comply with the same requirements as an agent on BT property.

11	**PROTECTION OF BT ASSETS**	• The 3rd Party Company is responsible for ensuring the protection of BT/Openreach assets when on a BT site including: ➢ information ➢ property ➢ BT/Openreach supplied items ➢ the safety of on-site personnel. • Where the 3rd Party Company holds or stores property on behalf of BT/Openreach, physical security measures must be provided to give an appropriate level of protection against theft or damage. BT reserves the right to examine these arrangements, where necessary, and inspect all BT/Openreach property being held by or on behalf of the 3rd Party Company.

12	**VEHICLE PARKING**	• There are no parking rights for non-BT/Openreach vehicles on BT property unless there is a specific contractual agreement. • Any parking is entirely at 'own' risk. Where it is possible for an agent to park on site, the rights of BT/Openreach vehicles are given priority at all times and the agent may need to relinquish a space that they have occupied. • Non-BT vehicles should not be parked on BT property unless the agent is present on site and actively engaged in tasks directly related to the 3rd Party Companies activities. • Any 3rd Party vehicles that are parked on BT premises are required to display the Driver Name, the Company they are working on behalf of and a Contact Telephone Number. • An agent does not have rights to the release of CCTV should a private vehicle be accidently damaged on BT premises while parked at their own risk

13	**INSTALLATION OF STAND-ALONE ALARM SYSTEMS IN 3RD PARTY COMPANY'S ACCOMMODATION**	• Installation of any alarm system by the 3rd Party Company must be subject to prior permission from BT. • All work carried out in respect of these installations must meet industry best practice and all relevant British Standards. • All installations must be subject to expert maintenance, the minimum period being annually. • Any system fault or false alarm must be investigated and rectified as a matter of priority to ensure full effectiveness and minimal environmental impact. • Repeated false alarms of an installed alarm system may result in BT requiring that the system is disconnected until the fault is permanently cleared, particularly where this may impact on surrounding properties or police response to the BT/Openreach area of the site.

14	**TRAINING - SECURITY EQUIPMENT USE**	• If required, BT can provide documentation for the 3rd Party Company to brief it's agents on the correct use of BT's proximity electronic access control and building alarm systems. • The 3rd Party Company is responsible for ensuring their agents are fully trained in the use of the access and alarm system at a BT site before access is required. • Each 3rd Party Company must have in place adequate processes to ensure that all new agents are properly trained on these systems before access is required.

15	**MISUSE/ABUSE OF BT SECURITY SYSTEMS & REQUIREMENTS**	• It is the responsibility of the 3rd Party Company to carry out remedial training for any agents who are shown to have repeatedly misused any security system. This will be managed by the AS/CLM with repeat offenders refused access to BT sites.

16	**SECURITY BREACHES**	• BT/Openreach reserves the right to exclude any agents from its premises if they have intentionally misused or abused any security equipment and/or committed a breach of security likely to have an impact on BT/Openreach or BT/Openreach customers. A security breach includes an agent access an area of the BT estate that they are not authorised to access.

17	**FAULT REPORTING**	• Any fault in BT security equipment should be reported as soon as possible; direct to the Property and Facility Services Helpdesk or via the Security Control Centre.

SECURITY HANDBOOK

REQUIREMENTS FOR NON BT/OPENREACH ORGANISATIONS WHEN ACCESSING BT SITES AND BUILDINGS

Document Control:

Owner:	Sarah Arnold, Physical Access Control and Identity SME	sarah.arnold@bt.com
Approver:	Andy Miller, Head of Global Physical Security and Behaviours Risk	andrew.r.miller@bt.com
Location of Published Document:	http://www.selling2bt.bt.com/working/third_party_access/default.htm	

Change log: - Changes for most recent versions:

SECURITY HANDBOOK

REQUIREMENTS FOR NON BT/OPENREACH ORGANISATIONS WHEN ACCESSING BT SITES AND BUILDINGS

ISSUE	DETAILS	DATE	Approved By
5	Revised and updated to reflect current organisational changes within BT Group plc.	November 2009	N/A
6	Updated Visitor definition.	March 2010	N/A
7	General review and update team names and telephone numbers.	January 2013	N/A
8	Updated vehicle parking and owner	February 2015	N/A
9	Reviewed and reissued	May/June 2015	N/A
10	Tone of voice updated and approval introduced.	May 2018	Circulated for approval by Andy Miller
10.1	Incorporating feedback from Peter Calvert, VQH1	23 May 2018	For approval
10.2	Approved with some minor updates.	31st May 2018	Andy Miller, VQA.
11 draft a	For review by key stakeholders	3rd May 2019	Annual review and changes to reflect the introduction of Openreach as a separate legal entity.
11	Updated to include feedback from key stakeholders.	31st May 2019	Andy Miller, VQA.