PUBLIC

PROTECTING BT

Our Standard in 3rd Party Contact Centres

Version: 2.0 **Owner:** Brian Webb

This standard sets the basic security controls in 3rd Party contact centres.

It applies to all Contact Centres run by 3rd party's working for or on behalf of BT Group, including Openreach, EE and PlusNet. To keep it simple we'll just say 'BT' for the rest of the document.

Introduction

This document focusses on security directives relevant for those directly engaged with the business of our Contact Centres and provides guidelines as to how they can be achieved. They are in addition to all standing company policies, standards, benchmarks and guidelines.

Who does this apply to?

This standard applies to anyone who works in a Contact Centre run by an outsourced partner working for BT. We may change this policy from time to time.

A Contact Centre is defined as an operation with a minimum of 15 advisors based in a single location whose primary purpose is to manage live customer contacts and where contacts are directed to the appropriate advisor via an automated system*. This includes inbound and outbound calls and online chats.

*Customer Facing Units may take a view that certain operations without automated call direction facilities are within scope as Contact Centres.

Definition of terms:

Term	Explanation
must	This word, or the terms 'REQUIRED' or 'SHALL', means that the definition is an absolute requirement
must not	This phrase, or the phrase 'SHALL not', means that the definition is an absolute prohibition
may	This word, or the adjective 'OPTIONAL', means that an item is truly optional
should	This word, or the adjective 'RECOMMENDED', means that there be a valid reason in certain situations to ignore a specific item, but the implications will be fully understood and carefully assessed before choosing a different option.
should not	This phrase, or the phrase "NOT RECOMMENDED" means every effort will be made to meet the requirements of a control, but it might not always be possible to avoid the action being described in all cases. Where a control can't be complied with the implications will be assessed and fully understood.

Scope

This document describes requirements for our Contact Centre people that are in addition to policies, standards and benchmarks that apply to all BT people.

If you have any queries about Contact Centre security please contact the Kite security team: (john.a.thompson@bt.com or sara.moody@bt.com).

What's included in this document?

1. Roles & Responsibilities.

Contact Centre people must be aware of and understand the requirements in this standard, along with all other relevant security policies and standards.

Managers are responsible for making sure their people (as described in "Who does this apply to?"), are familiar and comply with the requirements of this standard and associated policies and standards.

If requirements defined in this document are not adopted, BT Contact Centre senior leadership (Director level or above) must ensure that any associated risks are understood, recorded and signed off in the appropriate risk register and regularly reviewed.

2. Personal Devices

Our Acceptable Use Policy states that "We will not capture customer data on our personal devices. This includes (but not limited to) taking photographs, recording conversations, typing customer data into a personal device."

Our advice is personal mobile devices* (except smart watches) are not allowed on the Contact Centre floor; they must be stored in designated lockers away from the Contact Centre floor.

Occasionally the BT Contact Centre senior leadership, may allow personal devices to be stored out of sight in bags, pockets or desk drawers. And in this situation, a robust monitoring and enforcing regime must be in place. However, the 'out of sight' alternative must not be applied in Contact Centres where payment card information is visible, or in Contact Centres in India and the Philippines.

There is an exception to the advice: Specific people, such as Contact Centre managers, are authorised to use mobile devices whilst on the Contact Centre floor. These people should be readily identifiable; ideally by having some form of visible identification e.g. lanyards or badges. This is to avoid confusion and make it easier to spot an unauthorised person using a mobile device.

By the way, it's OK to use personal mobile devices in communal areas.

3. Handling personal information

Our Information Classification and Data Handling Standard has requirements for storing and working on hardcopy information in the office or at home. It states that "You must clear away when not in use and at close of business and store in an area that's restricted to authorised personnel only e.g. locker, locked drawer or restricted room."

It is recommended that Contact Centres should be paper free environments as far as is practicable. If agents need to write down customer information, they should use personal whiteboards and wipe them clear at the end of every working day.

4. Secure areas

Our Physical Security Requirements states that "All secure areas within a building must have an owner or zone approver. The owner is the only one who can decide upon who to grant access. In the case of the secure areas it is likely to be the operational manager"

Contact Centres are secure areas. Suitable owners or zone approvers must be appointed to manage access to our Contact Centres. This reduces the chance of access being granted to people who have no business reason to be there.

Our Physical Security Requirements states that "Where customer or business sensitive information is accessed and displayed and there is a risk of overlooking into the environment, screens should be positioned so as to face away from windows and window blinds should be used to minimise the risk of unauthorised viewing of information. It's up to the information owner or the individual CFU to determine the risk and action as appropriate."

We must make sure customer data can't be seen from outside the building. Our advice is to use security film or window blinds, and position computer screens away from windows where data is visible from outside the building.

5. First line assurance

We will carry out regular security assessments to make sure everyone is following expected standards of behaviour.

We recommend that assessments should be completed quarterly and check that:

- Personal mobile devices are stored in lockers or out of sight (depending on senior leadership agreement)
- Personal devices with the ability to store customer data are not connected to PCs
- Personal data is being disposed of correctly
- External doors are closed and secure
- Doors into the Contact Centre and other secure rooms are closed and secure
- Everyone is displaying their ID card
- Nobody tailgates into the contact centre
- Office furniture containing sensitive data is locked
- Desks are tidy and customer data isn't left lying around
- White boards have been wiped clean
- Pre-employment checks are completed for all Contact Centre people before they access customer data
- All Contact Centre people complete and refresh their mandatory Security and Data Privacy training

- Only people with a business need have access to the Contact Centre.
- Contact Centre people have no more than the system access they need for their role
- Leavers and Change of People Assignment processes are followed when people leave the company or change roles.

If assessments are completed less frequently, they would need to be supplemented by other activities to drive engagement & compliance.

6. Glossary.

Term	Definition
Contact centre floor	The area were contact centre advisors have customer contact. This does not include technical support or communal areas.
Personal mobile device	Any personal item that is capable of being used to capture/record customer information. This includes but is not limited to mobile phones. IPods, iPads, cameras and USB flash drives.

7. Change history.

Version no	Date	Change made by	Brief details of change
V2.0	17/04/20	John Thompson	Created

8. Document sign off

Name	Role	Date
	HR	
	Security Policy Committee	09/04/20
Brian Webb	BT Security - CSO BT Consumer, Kite programme owner	17/04/20
Dominic Wood	Senior Manager, Global Security Governance and Enablement	17/04/20
Adrian Setright	Senior Manager, Cyber Security Operational Risk	17/04/20
Ian Morton	Head of Security Policy & Compliance	17/04/20

9. Compliance

We appreciate most 3rd party employees act professionally and in line with BT's Values but if you behave in a way that's inconsistent with this standard, BT may terminate the arrangements we have with you for your services.

10. Useful Links and Information

Please report a 'Security Incident' via the Security Control Centre

Here is the link where you can see all relevant Standards and other security conditions.

If you need more information or guidance about this standard or any other security policy or standard, contact security.policy@bt.com

11. Ownership and Confidentiality

This document shouldn’t be shared with any other 3rd Party without the written consent of BT. This standard and any associated documentation remains the property of BT and should be returned if requested.