Call Centre Standard

General Terms

(A) These Requirements should be read in conjunction with the Implementation Matrix in Appendix 1 of this document below, which provides more detail on the behaviours and outcomes that BT will typically deem acceptable when considering the Supplier's compliance with the Requirements.

(B) BT may carry out risk assessments for the contact centre as contemplated by section 3.10 of the BT Supplier Security Requirements (the "Security Requirements") at any time, whether before or during provision of the services. Without prejudice to any other remedies which may be available to BT, BT may stipulate remedial actions, compensating controls and countermeasures to address any identified risks and/or unsatisfactory or non-compliance with these Requirements, which shall be implemented by the Supplier and documented as an appendix to this standard; any costs associated with the implementation of new security requirements to be agreed by both parties.

(C) BT shall be entitled on request to review the Supplier's policies and procedures that discharge the requirements of this standard as part of carrying out risk assessments for the contact centre. Such policies may include, but are not limited to: Computer use policy, IT disposal, Customer Authentication, Pre-employment checks, Risk Assessment and Management process etc.

1. Physical Security

1.1 The Supplier must ensure that the contact centre areas (see Glossary) used for the operation of the BT/EE account are Physically Segregated from all other business areas by specific Physical Access Controls.

1.2 The Supplier must have an auditable process for access in place to request and approve new physical access or removal of physical access to the contact centre area. [1]

1.3 The Supplier must ensure that in order to assess physical access rights to contact centre areas (including internal moves and changes) and as part of the supplier 'leavers process', the auditable process for access is reviewed every three (3) months and the date of each review is recorded.

1.4 The Supplier shall ensure that Lone Working in the contact centre area is prevented. This requirement includes cleaners and other third party employees.

1.5 The Supplier must have an auditable process that ensures that Tailgating through access controlled doors and/or barriers is prevented. The process should be enforceable and repeated non-compliance will be subject to discipline action.

2. Security passes and Visitors

2.1 The Supplier must ensure that employees, permitted (as part of their job role) to carry and use mobile phones, laptops, iPads and/or tablets in the contact centre areas must be easily recognisable to other employees and supervisors.[2]

[1] See Implementation Matrix for examples of an auditable process for access

[2] See Implementation Matrix for examples of what constitutes easily recognisable

2.2 The Supplier must have an auditable process in place for the issue and management of Security Passes and also Temporary Security Passes to contact centre employees when necessary, which includes automatic cancellation of access rights when the period of time the pass is required for expires.

2.3 The Supplier must ensure security passes and lanyards do not identify an employee's place of work.

2.4 The Supplier must ensure that an auditable visitor process is in place and published to all employees. A visitor log must be maintained as evidence.[3]

2.5 Security passes issued to visitors must distinguish them from employees, and must be recovered when the visitor leaves the contact centre, with any security passes not immediately returned being disabled by next working day.

2.6 The Supplier must ensure that visitors to the contact centre area are escorted at all times and wear visible visitors' badges/passes.

3. Employees

3.1 The Supplier must ensure that all Personal Items (including mobile devices) are stored in Designated Lockers away from the contact centre area.

3.2 The Supplier must allow for necessary personal medicines/basic medical equipment such as inhalers, insulin, or cough medicine to be permitted within the contact centre area.

3.3 Unless authorised following a risk assessment, staff working within the contact centre area are not permitted to carry mobile phones or mobile devices unless they are authorised. The Supplier must implement regular observational spot checks on staff to ensure that mobile phones and mobile devices are not taken into the contact centre area, and signage prohibiting the use of such devices must be implemented. In addition, security awareness training programmes should make this requirement clear and there must be a disciplinary process in place to deal with non-compliances.

3.4 The Supplier must ensure that a process is in place to enable external parties to contact employees in the event of a personal emergency.[4]

3.5 There must be an auditable process for the authorisation and use of pens, pencils and paper within the contact centre area. Pens, pencils and paper are not permitted unless employees are authorised by their manager to do so as part of their job role.

3.6 The Supplier must ensure that, if produced as part of an employees' job role, any handwritten notes are not left unattended, and must be securely stored (as per information and classification handling) or disposed[5] of at the end of the working day in order to demonstrate a 'Clear Desk Policy'[6].

http://www.selling2bt.bt.com/working/ThirdPartySecuritystandards/index.htm

3.7 The Supplier must arrange for white boards & wipe-able notepads (including dry wipe pens and cloths), to be provided as an alternative to pens, pencils and papers, so as to allow for notes to be taken during calls. The Supplier must ensure that these notes are erased as soon

[3] See Implementation Matrix for information to be retained in the Visitor log

[4] See Implementation Matrix for examples of personal emergency processes

[5] See Implementation Matrix for examples of secure storage or disposal

[6] See Implementation Matrix for an example of what should be included in a Clear Desk Policy

as the customer query is concluded and all notes must be removed from white boards at the end of each advisor's shift. Managers and supervisors must walk the floor and carry out spot checks to ensure compliance with this requirement.

3.8 The Supplier must ensure that any temporary notes recorded online or in electronic tools (in order to support customer calls) are automatically deleted at the end of each advisor's shift or at the end of the working day. This must either happen automatically, or a daily record must be kept to ensure compliance with this requirement.

3.9 The Supplier must ensure that an auditable process for the use of whiteboards/paper is established and in place to ensure:

- Papers are securely stored or removed and disposed of at the end of the working day; and
- White boards are cleaned at the end of each shift and at the end of the working day. [7]

3.10 The Supplier must arrange for all interactions with customers to be recorded on the account (memo or notepad depending on the system used).

3.11 The Supplier must ensure that any interactions with customers are not recorded in any Microsoft Office Applications unless employees are authorised by means of a risk assessment to do so as part of their job role.

3.12 The Supplier must ensure that any role authorised to perform any of the following activities within the contact centre area must be risk assessed in accordance with the requirements set out in section 11. Activities include but are not limited to:

- Use of Microsoft Office Applications
- Use of business mobile devices
- Use of company laptops
- Use of personal items (as defined in the glossary)
- Ability to print or copy customer information
- Ability to download call recordings from call recording server(s)
- Access to internal, external email or other communication tools e.g. instant messaging
- Use of pens/pencils and paper for note taking
- Sending multiple text messages to customers
- Remote access to customer equipment

3.13 The Supplier must ensure that the ability to send multiple text messages (one text message to multiple customers) is not permitted, unless employees are authorised to do so as part of their job role. If such texts are transmitted records must be kept to demonstrate when these occurred, the recipient(s) and the reasons for sending.

3.14 The Supplier must ensure that the downloading of call recordings from the call recording server(s) to desktops/laptops is not permitted or possible unless the individual is authorised to do so as part of their job role. If authorised, a record must be maintained of who has approval to perform this function, and if call recordings are downloaded, records must be kept to demonstrate why this occurred, the actual downloaded call, and the reasons for download. Authorised advisors, and any non-compliances must be reviewed for validity on a regular basis.

[7] See Implementation Matrix for examples on what an audit of whiteboards/paper should incorporate

4. Equipment

4.1 The Supplier must ensure that all advisors have protected computer screens which are not visible from outside the segregated contact centre area.[8]

4.2 The Supplier must ensure that printers and fax machines are located in secure areas, restricted to authorised individuals only and used only for strictly necessary purposes. The list of authorised users and the use of the machines must be reviewed on a regular basis to ensure on-going validity. Any hard copies should be securely stored as per the information classification and handling standard and must not be removed from the contact centre unless authorised by BT.

4.3 The Supplier must ensure that any printing and copying requires a User ID and security code so that all prints can be monitored and logged for audit purposes.

4.4 The Supplier must ensure that cross-cut shredders and confidential waste bins are provided in areas where printers and fax machines are located. The shredders and waste bins must be emptied regularly and the contents disposed of securely.

4.5 The Supplier must ensure that any hardcopy information is securely disposed, either by shredding or by placing it in the confidential waste bins in accordance with section 4.4.

4.6 The Supplier must ensure that any Physical Assets assigned to individuals at the beginning of their employment are recovered/removed prior to termination of their role within the contact centre area, or upon the individual leaving the BT/EE contract, and a Physical Assets inventory must be maintained.[9]

4.7 The Supplier must ensure that Physical Assets that have been recovered or removed must be securely disposed of and in-line with secure disposal requirements.[10]

5. Access to systems

5.1 In order to protect customer data, all advisors must record their User ID when accessing a customer account/record as well as the reason for such access. Access must only be granted after approval from a System Owner or line manager. In addition, access to customer accounts must only be allowed if it is required for an advisor’s role, and must be set at the minimum level needed for an advisor to carry out their job. Anyone who does not need access to a BT and/or EE system to view customer records shall not be permitted access for any purpose whatsoever.

5.2 Unless required for operational reasons ‘view only’ access should be prevented. Authorised ‘view only’ access must be logged and monitored to prevent inappropriate usage.

5.3 The Supplier must ensure that employees are not permitted access to the internet, personal email or external email, social media (such as Facebook) or other communications tools such as messenger or communicator unless authorised by BT and is required as part of their job role.

5.4 The Supplier must ensure that all text messages sent from within suppliers systems are logged and monitored. If texts are transmitted records must be kept to demonstrate when these occurred, the recipient(s) and the reasons for sending.

[8] See Implementation Matrix for examples of what constitutes ‘protected computer screens’

[9] See Implementation Matrix for examples of what should be included in the Physical Assets inventory

[10] See Implementation Matrix for an example of what secure disposal requirements should incorporate

5.5 The Supplier must ensure that only pre-approved remote access tools, used to access customer devices for support purposes are permitted and that these are restricted to staff who need it to perform the role. Access should be reviewed every 3 months and such access revoked if no longer needed to perform the role. Solutions must be implemented to identify non-approved remote access tools.[11]

5.6 The Supplier must not permit remote access to contact centre employees work email or to any system to access customer records.

5.7 The Supplier must ensure that employees are permitted 'read only' access to shared drives only provided and managed by BT and/or EE. No other shared drives shall be used within the contact centre. The downloading, copying, removal or modification of customer information from any BT and/or EE system, app or database is not permitted.

6. Call recordings

6.1 The Supplier must ensure that all customer calls are recorded. The Supplier must ensure that call recordings (voice and screen) are protected during transmission from PC desktop to call recording server(s).[12]

6.2 The Supplier must ensure that call recordings are securely stored, particularly if this includes Payment Card Information (PCI) in order prevent the loss or inappropriate use of this customer data. PCI data must be encrypted and a key management solution implemented to protect this using industry best practice. BT and/or EE may review encryption and protected storage solutions from time to time, to ensure these are adequate and appropriate. .

7. Customer authentication

7.1 The Supplier must ensure an approved customer authentication process is defined and in place for 'inbound' and 'outbound' calls. [13]

7.2 The Supplier must ensure that pins or passwords used by customers to authenticate their identity are not visible to other contact centre employees, for example through the use of protected computer screens or physical segregation.

7.3 The Supplier must ensure that customer authentication is automated in such a way that it does not require the customer to reveal their full pin or password to the advisor e.g. through a system generated request for random password digits/letters such as 1st, 3rd and 5th. BT and/or EE may review the customer authentication process from time to time, to ensure compliance with these Requirements.

7.4 The Supplier must ensure that, where a customer has forgotten their pin or password and needs to reset this, any reset does not occur until the customer has correctly passed additional authentication checks.[14]

7.5 The Supplier must ensure that systems for setting up a customer's account pin or password are automated, and do not require interaction from a contact centre employee.

[11] See Implementation Matrix for examples of behaviours to identify and remote access tools

[12] See Implementation Matrix for examples of how call recording transmissions should be protected.

[13] See Implementation Matrix for examples of what the customer authentication process should involve.

[14] See Implementation Matrix for examples of what additional authentication checks should involve.

7.6 The Supplier must ensure that the creation of new pins or passwords are generated by an automated system and that any new pins or passwords are sent directly to a customer by either text or email, without the need for advisor intervention.

7.7 The Supplier must ensure that password or pin account resets can be implemented by customers either online or via an Interactive Voice Response (IVR) system.

7.8 The Supplier must ensure that an 'employee assistance reset' facility exists, allowing customers to reset their pin or password with the assistance of a contact centre employee. The ability to reset a pin or password must be restricted to a limited number of employees.[15]

7.9 The Supplier must be able to generate, on request, an audit trail showing customer pin and password resets, as well as the system used to perform the reset (online, IVR or employee assistance) and which employee was involved in the transaction.

8. Data Privacy

In addition to the mandatory BT Security and Data Protection training (see Annex 2) that all Supplier employees must complete and acknowledge they understand, the following requirements must also be met:

8.1 The Supplier must ensure that employees within the contact centre area have easy access to relevant and applicable security and data protection information, on the front page of their intranet home page (or in the event they do not have intranet, via regular email updates and training).

8.2 The Supplier must provide regular reminders, at least twice a year, to all employees within the contact centre area reinforcing positive behaviours and supporting security best practice.

9. Monitoring

9.1 The Supplier must arrange for a call monitoring 'quality check' by supervisors/managers on a random selection of customer telephone calls (inbound and outbound) to occur every week, to ensure amongst other Requirements, that the correct customer authentication process has been used.[16]

9.2 The Supplier must ensure that calls are deemed 'failed calls' if the correct customer authentication process has not been followed. Following any failed calls the Supplier should have in place a feedback process to remind contact centre advisors of their responsibilities to authenticate customers correctly and/or keep passwords secure (as the case may be).

9.3 The Supplier must have an auditable process in place in the event a contact centre employee has repeatedly 'failed calls' and failed to carry out the correct customer authentication process. This should include the consequences of an advisor repeatedly failing to carry out correct customer authentication or correct record maintenance and may be used as evidence for performance management or disciplinary procedures involving the relevant individuals.

[15] See Implementation Matrix for examples of what an employee assistance reset facility should incorporate.

[16] See Implementation Matrix for examples of what must, as a minimum, be included within any quality check

10. Compliance

10.1 The Supplier must ensure that a documented auditable process is in place to conduct and manage regular local site security compliance checks and/or compliance spot-checks to check compliance with this standard and the BT Security Requirements e.g. walking the floor, clear desk etc.[17]

10.2 The Supplier must implement a process to ensure that quarterly evidence based reviews (based on 10% of the intake) are conducted on contact centre employees or any individuals working on a BT and/or EE contract, to ensure the pre-employment screening process and security training (as part of the induction process) are completed and operating effectively. This is to ensure that employees working within the contact centre area have been adequately background checked (in-line with BT's pre-employment check policy) and security trained in order to have confidence that sensitive customer information is adequately protected.

10.3 The Supplier must implement a process to ensure that quarterly evidence based reviews (based on 100% of the intake) are conducted on contact centre employees or any individuals working on a BT and/or EE contract, to ensure annual mandatory Security and Data Protection training has been completed.

10.4 The Supplier must ensure that quarterly refresher briefings covering employees' Security and Data Protection obligations are undertaken and evidence of employee participation and understanding must be documented.

10.5 The Supplier must ensure that relevant policies, standards, guidelines and processes are made available to contact centre employees to ensure compliance to this standard and BT's Security Requirements.

11. Risk Assessment

The Supplier must ensure that any non-compliances, authorisations, or specific exceptions to these requirements are risk assessed by the supplier and documented in accordance with the risk management process. The risk assessment must include:

- Reason why the activity is required, and why any non-compliance to these Requirements is justifiable;
- Status of any non-compliance e.g. permanent or temporary;
- If temporary, the date by which controls will be implemented and the date the activity will be completed;
- Individuals' function/role and why the activity is appropriate to this role (and why they are excluded from compliance with controls);
- Mitigating controls in place to minimise risks arising from the activity;
- Justification for the implementation of certain controls and/or not implementing the necessary control(s); and
- Evidence of Senior Management Approval.

[17] See Implementation Matrix for examples of what should be included as within compliance spot-checks.

12. Glossary

Term	Explanation
Customer Contact Centre	A contact centre (also referred to as a customer interaction centre or e-contact centre) is a central point in an enterprise from which all customer contacts are managed. The contact centre typically includes one or more online call centre's but may include other types of customer contact as well, including e-mail newsletters, postal mail catalogues, Web site inquiries and chats, and the collection of information from customers during in-store purchasing. A contact centre is generally part of an enterprise's overall customer relationship management (CRM).
Designated Lockers	Staff working in the contact centre area are not permitted personal items which are capable of recording customer information, such as mobile phones, at their work stations. These must be locked away in personal lockers (marked as such) away from the contact centre area.
Employee(s) / employee(s)	Employee means any individual working within the contact centre area, including permanent and temporary employees of the Supplier, agency staff, contractors and workers.
Escorted	There must be a formal visitor's process in place which ensures, as a minimum, that visitors to contact centres are escorted at all times; in order to prevent people getting lost, or wandering into areas where they are not allowed.
Implementation Matrix	The appended matrix which sets out, as a minimum, the outcomes and standards the Supplier must achieve when implementing certain processes, policies or procedures referred to within the Requirements.
Lone Working	There must be a process in place to ensure that the practice of an individual working within the contact centre area outside of normal operational working hours is not permitted without management authorisation. This includes cleaners and other noncompany individuals such as maintenance staff.
Microsoft Office Applications	Microsoft Office Applications include, but are not limited to Word, PowerPoint, Excel, Outlook and OneNote. In order to deny the exfiltration of data, customer interactions involving online systems must not be recorded on these applications (unless authorised) as information from these applications can be easily copied and extracted.
Personal Items	Any personal item that is capable of being used to capture/record customer information - this includes but is not limited to: mobile phones, smart watches. iPods, iPads, cameras, USB flash drive, pens and paper.
Physical Access Controls	Physical access controls utilised will depend of the area the contact centre is located in. Physical access controls may be technical (e.g. swipe card, keypad, biometrics), or procedural (e.g. keys with an auditable sign-out process, or a sign-in process where the person controlling access checks ID), however, the physical access controls utilised should be appropriate for the area.
Physical Asset	For the purposes of this document – physical asset refers to any asset that is capable of processing or storing customer data or information.

Physically Segregated	For the purposes of this document, physically segregated means that conversations cannot be overheard and information cannot be seen from other business areas. A physical barrier (walls, separate buildings etc.) with physical controls governing entry to the area must be implemented.
Security Incident	A security incident is a change in business as usual operations that impacts the confidentiality, integrity or availability or information assets, indicating that a breach of security policy, security standard /requirement may have occurred, or a security safeguard may have failed. Here's a few examples: System Misuse, Unauthorised Access, Lost/Stolen Equipment, and Malware Infection.
Senior Management Approval	Where it is necessary to agree an exception to these requirements, the circumstances should be risk assessed, and the approver should be someone who has the responsibility for management of the functional area, with the requisite authority.
System Owner	This means the official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Tailgating	The practice of following another, or allowing an unauthorised individual through an access controlled door/barrier or gate to gain access to an area; not using their own security pass to gain access to an authorised area of the suppliers premises used to undertake BT/EE contracts.
Temporary Security Passes	These must be issued as part of an auditable process (such as a book, log or spreadsheet), and must record all issuance of temporary security passes, as well as the date of issue, the name, department, contact number, and reason for issue, as well as the name of host and the date the temporary pass is returned. There must be a process in place to deal with cards that are not returned.
User ID	Printers and fax machines located within the contact centre area must require a user to enter a unique ID and security code, so as to allow for the monitoring of their use by users on an individual basis. In addition, employees must enter this unique ID when accessing customer accounts/records in accordance with section 5.1.

PROJECT KITE: Implementation Matrix for Supplier-facing Contact Centre Requirements.

Schedule Ref	Overall Description	Minimum Outcomes that are likely to be deemed compliant.
1.2	Auditable Process for Access	A spreadsheet or data log of names, including details around when the access was granted, the rationale behind the grant of such access, the date of removal of access, and the reasons for doing so.
2.1	Easily Recognisable	Staff permitted to use mobile phones, laptops, iPads, tablets, due to their job role, must be easily recognisable by methods such as a different coloured lanyard, or another distinguishing means of identification.
2.4	Visitor Logs	The following information should be recorded: i) name of the individual, ii) the organisation they are from, iii) date and time entry, and their departure, iv) the purpose of their visit, v) the name of the person they are visiting, vi) registration number of any vehicle brought onto the site, vii) mobile phone contact number, viii) the identification number of the visitor pass.
3.5	Personal Emergency	A system must be in place so that family and friends can still contact the employee in the event of a personal emergency. This contact system could be through the use of a dedicated switchboard number or a supervisor's number which could be used as a central point of contact.
3.7	Securely Stored or Disposed	Where notes are produced as part of an employees' job role, examples of secure storage or disposal include, but are not limited to, the use of shredders, confidential (and potentially locked) waste bins, and/or storage within permitted facilities which can be locked by employees.
3.7	Clear Desk Policy	All materials should be Securely Stored or Disposed immediately after use and no materials should be left on the desk at the end of a working day. Regular observational spot checks on staff must be implemented and there must be a disciplinary process in place to deal with non-compliances.
3.10	Audit of Whiteboards/Paper	With regard the processes in this section 3, a record (in a form such as a spreadsheet) must be maintained to demonstrate that the spot checks are being undertaken, and compliance with the requirements is ensured.
4.1	Protected Computer Screens	It must not be possible to view advisors screens within the contact centre environment, and information should not be capable of being read by persons within the contract centre not entitled to do so (such as cleaning and maintenance staff). Customer data on computers screens must be kept

		hidden by the positioning of the monitors or by the use of privacy screens.
4.6	Physical Assets Inventory	An inventory of all Physical Assets and other items assigned to individuals such as security passes, locker keys, laptops, desktops or remote access tokens must be maintained for audit purposes. When an advisor either leaves their employment or is removed from the contact centre, processes must be implemented to ensure that immediate steps are taken to remove all logical and physical access and recover any Physical Assets, keys, security passes. This must be completed as part of a 'Leavers' Checklist at the conclusion of their employment.
4.7	Secure Disposal Requirements	When Physical Assets are disposed of at the end of their useful life, a proprietary software such as ‘Tabernus’ or ‘Blanco’ must be used to ensure that any confidential or customer information has been wiped from the equipment permanently (where relevant), and to a standard as approved by BT and/or EE. If secure removal of the data cannot be undertaken using this software, then the equipment must undergo secure destruction using a process approved by either BT and/or EE. The BT and/or EE security contact can assist further in this area. Once any confidential or customer information has been removed, the Physical Assets can be either re-used elsewhere, or disposed of, as appropriate.
5.5	Remote Access Tools	In order to prevent unauthorised access to customer data, formal processes must be implemented to ensure that only remote access tools that have been pre-approved by BT and/or EE are capable of accessing customer devices. Solutions must be implemented to identify non-approved remote access tools and such solutions must be reviewed regularly to ensure that non-approved tools cannot and/or have not been utilised. Additionally, use of the approved remote access tools must be restricted to authorised individuals, with such individual’s only obtaining authorisation via a formal process, incorporating a risk assessment of the need for remote access.
6.1	Call Recording Transmission	It is essential to encrypt customer call recordings from the PC to call recording servers, and such encryption must include both the voice recordings and screen details.
7.1	Customer Authentication	All advisors must follow the customer authentication process as approved by BT/EE to ensure that the customer is the person they claim to be. This process will be made clear to the Suppliers and advisors, and may differ depending on the function(s) the contact centre is providing.

7.4	Additional Authentication Checks	Advisors must ensure that before they proceed to change a customers' PIN or password they additionally ascertain sufficient information from the customer in order to satisfy themselves they the person is who they say they are by asking certain security questions about their identity over and above their name and address, such as what recent activity has happened on their account, the amount of the last bill, or how long have they been a customer with BT or EE. However, these are only examples and this list is not exhaustive.
7.8	Employee Assistance Resets	In order to facilitate customers who are not able to reset their PIN or password either online or via IVR, it must be possible for resets to be facilitated with the assistance of a call centre employee. However there must be a formal process in place to ensure that the employee reset facility is restricted to a limited number of employees, and safeguards are in place to ensure that any employees with the ability to reset customer PINs or passwords are physically segregated from others within the contact centre and with appropriate controls in place. The list of approvers must be reviewed on a regular basis to ensure such approval is still required and being used with appropriate discretion.
9.1	Call Monitoring Quality Check	Managers must perform quality checks, including the weekly monitoring of a random selection of customer telephone calls (inbound and outbound) handled by advisors, and a monthly review of all records and process implemented by the Supplier. This should serve to ensure that the Supplier is compliant with these Requirements and, in particular, that employees are using the correct customer authentication process and maintaining the correct records.
10.1	Compliance Spot Checks	An auditable process must be implemented to conduct and manage local site security compliance checks and compliance spot-checks on all Requirements. As well as the obligation on Supplier to carry out such checks, BT and/or EE may also carry out compliance spot-checks at any time. Spot Checks to include but not limited to: • Security ID / security pass • Clear desk/clear screen • Use of personal lockers • Personal mobile devices • Use of whiteboards • Removal and disposal of printed or faxed confidential information • Customer authentication • Call monitoring quality checks • Password reset audit trails

		• Use of text messages • Compliance with data protection and security training Any spot check audit must include details of actions to be taken where discrepancies or non-compliances are highlighted. Any remedial plans requested by BT and/or EE must be tracked through to completion.