BT GLOBAL ICT BUSINESS SPAIN, S.L.U.
GENERAL PURCHASING CONDITIONS

These General Conditions are entered into by and between BT Global ICT Business Spain S.L.U, a company incorporated in Spain with Tax identification number B- 88625496 and having its registered office at C/ María Tubau, 3; 28050 Madrid ("BT") and the Supplier whose data is included in the signature paragraph (each individually named as a "Party" and together the "Parties"). Each Party agrees to these General Terms and Conditions.

1 PURPOSE AND SCOPE

1.1 These General Conditions of Purchase (hereinafter referred to as "GTC" and or the "Agreement" or the "Contract") establish the general legal framework of rights and obligations between the parties and apply to all Purchase Orders placed, awarded and issued by BT for the delivery of goods, the acquisition of services or the execution of works.

1.2 BT may purchase services either by entering into a contract or by placing a Purchase Order. In certain circumstances, these two types will be used simultaneously, with a contract being signed first and Orders being placed on that contract at a later time.

1.3 Notwithstanding, the supply of services or goods maybe initially be placed by telephone, BT will always make effective Purchase Order in writing and sending them to the Supplier by fax, ordinary mail, registered mail or e-mail. Every BT Supplier must have an e-mail address or fax number and must notify it to BT in advance.

1.4 Except when agreed on the contrary among the parties by means of an Annexes to these GTC or as agreed in the pertaining Purchase Order, these GTC will be the exclusive agreement governing the commercial relationship between BT and the Supplier, and are deemed to be the prime contractual document, especially when there are other GTC from the Supplier that may contradict these.

1.5 The Supplier agrees that any work or services carried out by him as a result of prior Purchase Orders to the acceptance of these GTCs shall be governed by the latter.

1.6 Supplier's GTCs can only modify or complement these GTCs when they have signed by BT and are included as an Annex or Addendum to this GTC.

2 CHARGES AND PAYMENT

2.1 The price that BT should pay the Supplier in accordance with what is set forth shall take place within this term of sixty (60) days from the date of receipt of invoice from supplier, by bank transfer to the account designated by the Supplier in the corresponding Purchase Order.

2.2 The correctly issued invoice shall be sent by the following ways (both of them) to facturas@bt.com and in hard copy to BT To: Accounts payable C/ María Tubau, 3, 28050 Madrid.

2.3 Invoices shall include the Supplier's address, its NIF (Tax Identification Code), the date, the Purchase Order number and the description of the services performed, as well as any other data required by the applicable regulations.

2.4 Invoices that do not comply with what is set forth in the above paragraphs will be returned to the Supplier, and will include the date of return and the reason for doing so, without this causing BT to incur in payment default.

2.5 The prices detailed in each Purchase Order or in its Annexes are closed and definitive. In the event that the price is stipulated in a foreign currency, it will be paid in that currency. However, if the services are provided on a regular basis, BT shall only be liable for fluctuations in the exchange rate prevailing at the time the Order is signed which do not exceed 5% of that exchange rate, and the price shall be reduced in proportion to the loss suffered by BT.

2.6 The accrual of the price payable by BT to the Supplier under this condition shall occur on the last day of each month for goods delivered in that month or for services actually rendered during that month.

2.7 The Supplier shall be liable for any difference in freight, carriage or other charges arising from the delivery of the goods which are the subject of the Order, and no such difference shall be passed on to BT unless otherwise agreed in writing.

3 TAXES

3.1 All taxes, fees and other levies shall be borne by THE Supplier, whether direct or indirect, except for VAT which shall be borne by BT. In the event of the occurrence of new taxes, they will be paid by the party to whom they apply in accordance with the law.

3.2 If, during the term of the Agreement, changes occur in the market that affect any of the services provided by the Supplier under the Agreement, BT may require a price review in the event that significant price deviations are identified that result in a significant loss of competitiveness for BT.

3.3 A significant loss of competitiveness is deemed to exist where BT submits one or more separate bids (a separate bid is not one in which the same operator is directly involved, in whole or in part), or public price information, formulated or prepared by undertakings which have authority and authorisation to provide the Services covering all the services which are the subject of the bid and which result in a total price which is at least 5% per 100 of that set out in the Contract.

3.4 For the purpose of verifying that the foregoing circumstances exist, and only in the event of any discrepancy in the verification of BT's judgement, either party may refer the matter to an auditor under the following principles:

a) Any party who requests the auditor to do so shall pay for it.

b) The auditor must be a person of recognised standing in the marketplace.

c) The auditor shall issue an opinion at the request of the requesting party within a period not exceeding 30 days.

d) The auditor shall express an opinion as to whether the bids or information submitted relate to the overall services contracted by BT and whether the prices offered are within those prevailing in that market.

e) The Parties undertake to comply with and act on the opinion of the independent auditor. To this end, within fifteen days of the written communication from the auditor to the parties assessing the compliance of the bids with the criteria set out in this section, if the Supplier does not match the bids submitted, BT shall be entitled to terminate the Contract early by simply notifying the Supplier in writing, without the latter having any right to compensation or any amount whatsoever in respect thereof, giving fifteen days' notice.

3.5 The Supplier shall make all appropriate payments, deductions and account to Employment, Insurance and tax authorities in a timely manner for tax and National Insurance contributions (employer and employee) and levies from or in respect of (as applicable) the remuneration or fees it pays its Supplier Personnel (none of whom shall be employees of BT) or their intermediary (such as a personal service company) and will procure that Subcontractors do the same.

3.6 The Supplier shall indemnify BT against any claim for damages or otherwise, and/or against any claim which it may receive jointly and severally, subsidiarily or through the exercise of any direct or indirect action, in relation to the employees of the Supplier, including but not limited to payments to the Social Security, severance payments, amounts paid in out-of-court settlements or any other payment of money, penalty, tax or otherwise which may be required of BT as a result of the failure of the Supplier to comply with the obligations set out in this section or the following section. For these purposes, and without prejudice to the termination of the contract pursuant to the provisions of section 10.1.B) of this agreement, BT may withhold all payments to the Supplier which are for any reason outstanding in an amount sufficient to cover such liabilities.

4 DELIVERY

4.1 The Supplier undertakes to deliver the goods and/or services included in a Purchase Order on the delivery dates indicated in the Purchase Order and to the address stated therein. The price of the goods and/or services shall include all costs directly or indirectly related to the goods, merchandise or service up to that point of delivery. The goods will be delivered at the risk and peril of the Supplier. The transfer of risk will take place upon acceptance of the goods or services. Each package in which the goods are sent, must clearly indicate the delivery address, as well as the Purchase Order number.

4.2 The verification and reception of the goods will be carried out after the delivery. The initial receipt by BT is to be understood as a provisional receipt. The Supplier shall not therefore treat BT's acknowledgement of receipt, or BT's signature, as final acceptance. Final acceptance (including any quality control tests or other tests carried out by BT), if any, shall be made within 30 days of the date of provisional acceptance. The date of final receipt shall be the date taken into account for the purposes of commencing the warranty period applicable to the goods or services.

4.3 The transfer of ownership of the goods shall take place once they have been delivered and definitively accepted at the place of delivery mentioned in condition 4.1 above.

5 WARRANTY PERIOD

5.1 The Supplier warrants to BT that the materials, equipment or services of any kind supplied under a Purchase Order have no defects, comply with applicable specifications, drawings, samples or established descriptions, are fit for purpose, are new and of first quality.

5.2 The Supplier is responsible for any apparent or hidden defects in any of the goods and services delivered, including any part whose manufacture or performance has been wholly or partly commissioned to a third party. The Supplier shall indemnify BT in full against all damages, injuries and claims or actions of any kind whatsoever suffered by BT without any exclusion or limitation of liability in this respect.

5.3 The Supplier grants a guarantee on the goods delivered of twenty-four (24) months from the date of final acceptance by BT. In case of fault on the goods, BT may directly or through third parties carry out the necessary work to remedy any faults or defects, and it can deduct from any outstanding payments any expenses it has incurred to, when the Supplier does pay said expenses on time.

5.4 The Supplier shall guarantee the Software for a period of one (1) year from the time that it is first used.

5.5 The Supplier shall take all necessary steps to inform and keep BT informed without delay of all actual or suspected manufacturing defects of which it becomes aware, so as to prevent possible damage.

5.6 Any parts, materials or services found to be defective during the warranty period shall be replaced immediately at the Supplier's expense in the same condition as the original. The Supplier may, however, recover defective parts and materials. The replaced parts and materials will have the same guarantee period as the ones initially supplied, starting the guarantee at the moment of the replacement.

5.7 Without prejudice to any other rights or remedies which BT may have, the Supplier undertakes to hold BT harmless and to indemnify it against any liability arising from or in connection with any claim brought under labour or social security law by Personnel of the Supplier in connection with the Services or the termination of this Agreement or any order or the cessation of the provision of the Services (or any part thereof), including, without limitation, any claim, demand for employment or related rights, or any claim for discrimination of any kind.

6 AUDIT RIGHTS

6.1 The Supplier will, and will ensure that any Subcontractors will, grant to BT (and to its representatives) the right of access to any records, documents, Supplier Sites, Supplier Personnel, Systems, facilities, equipment, information and software and any other relevant information:

1. at any time for the duration of the Contract and for a period of twelve (12) months following its termination or expiry, to audit the Supplier's performance of its obligations under the Contract

(and accuracy of information provided under the Contract), the Charges and taxes charged to BT; and

2. at any time for the duration of the Contract and for a period of six (6) years following their termination or expiry, to comply with any request by, requirement of, or duty to, any Authority in the course of carrying out its regulatory functions or the requirements of Applicable Law.

6.2 Each Party will bear its own costs of participation in any of such audits.

7 COMPLIANCE REQUIREMENTS

7.1 The Supplier shall comply with all Applicable Law and provisions applicable to the Purchase Order from the time it is placed, as well as to the material, elements and/or services that constitute its object.

7.2 The Supplier will procure and guarantee that its Supplier Personnel comply with all Applicable Law in the performance of the Supplier's obligations under the Contract.

7.3 The Supplier will, and will procure that all Supplier Personnel will, comply with the relevant Policies currently available at URL https://groupextranet.bt.com/selling2bt/articles/side/our_privacy_policy.html, provided that:

1. where any such Policy is expressed to apply to BT, the Supplier will comply and procure that all Supplier Personnel comply with such Policy as though such Policy applied to and had been adopted by the Supplier;

2. the Supplier will be granted a reasonable period from notification (or such other period as specified in the Policy) in which to implement any changes required to comply with any new or amended Policy; and

3. the Supplier will not be deemed to be in breach of this section 7 where it can demonstrate that its performance in connection with the Contract is compliant with its own policies provided that such policies are no less stringent than the relevant Policies.

8 SUPPLIER PERSONNEL HEALTH AND SAFETY

8.1 When the Service is provided at BT's own premises, both the Supplier and the personnel under its authority assigned to provide the Services undertake to comply with the internal rules of organisation, safety and operation of BT's offices and facilities. To that end, BT will keep the Supplier informed at all times of the internal organisational, safety and operating rules applicable to its offices and facilities, and the Supplier undertakes to keep its staff informed of those rules at all times.

8.2 During the term of the Contract, the Supplier undertakes to comply with Spanish Act 31/1995, of November 8th, on occupational Risk Prevention, and its development regulations, with respect to the Personnel assigned to the provision of the Service. For this reason it will present a preventive policy appropriate to the risks of the Personnel assigned to the provision of the Service, which will keep updated during the term of the Contract. Whenever the Supplier makes modifications it will notify BT. The Supplier also undertakes to provide information and

training to its employees before they occupy the positions for which they are hired. The parties agree to coordinate their health and safety measures.

8.3 During the term of this contract and to comply with the provisions of the law referred to in paragraph 8.2, the Supplier undertakes, prior to the signing of the Contract, to register in the web tool designated by BT for these purposes:

1. Its preventive policy according to the risks to which its employees are exposed. This policy shall include a health surveillance system, in accordance with Article 22 of Spanish Act 31/ 1995 on the Prevention of Occupational Risks and Article 37.3 of Spanish Royal Decree 39/1997, on Regulation of the Prevention Service.

2. The information and training given in writing to the employees of the Suppliers who provide their services in BT regarding the existence of the general risks and the position, its preventive policy and the obligation to know and comply with it.

3. The Mutual Insurer for work accidents and occupational hazards to which the Supplier is a member and must report to BT any changes that may occur on it during the term of the Contract or the Purchase Order.

4. Any documentation required for the performance of the Service to be rendered.

5. Any accident that may affect any worker of the Supplier during the rendering of the services scope of the Purchase Order.

8.4 If the services provided require the physical presence of Supplier's employees in any of BT's facilities or BT's customers, in compliance with the Occupational Risk Prevention Act, the Supplier shall be:

1. documented in the web tool designated by BT.

2. maintain the documentation required in the above tool updated at all times, including both company documentation and that of the workers who will provide the Service as well as any documentation required for the performance of the Service to be rendered.

3. report to BT through the service coordinator of any accident and/or occupational illness suffered by one of its workers during the performance of the Service and to record information regarding such accident and/or occupational disease, by sending the information by mail to servicio.de.prevencion@bt.com.

8.5 The application for registration in the Web tool will be made by sending an email to servicio.de.prevencion@bt.com. A user and password will then be sent to access it, and to manage the company and worker documentation requested.

8.6 BT undertakes to:

1. Notify the Supplier through the Web tool of the occupational risks and preventive measures to be taken regarding the Service.

2. Notify the Supplier through the Web tool of the results of risk assessments that are carried out and the changes that occur in the risks and preventive measures so that you can comply with their legal obligations regarding occupational risk prevention.

3. Report through the designated coordinator any health damage suffered by any worker of the Supplier during the Service.

4. To ensure the Supplier's workers providing the services of this Contract the same level of health and security protection as that of its employees.

8.7 During the term of this Contract, both parties undertake to coordinate their prevention of occupational risks policy if necessary and pursuant to the terms of current Spanish legislation on the prevention of occupational risks.

9 FORCE MAJEURE

9.1 "Force Majeure Event" means any circumstance beyond a Party's reasonable control that hinders, delays or prevents that Party from performing any of its obligations under the Contract including nuclear accident, acts of God, fire, flood, storm, drought, natural disaster, terrorist attack, civil commotion or armed conflict and pandemics or epidemics declared by the competent health authorities. For the avoidance of doubt, the mere shortage of labour, materials, equipment or supplies (unless caused by events or circumstances which are themselves Force Majeure Events), strikes, lock-outs or other industrial disputes involving the work force of the party so prevented or of any of its Subcontractors or suppliers will not constitute a Force Majeure Event;

9.2 If a Party is prevented from performing any of its obligations by the occurrence of a Force Majeure Event, that Party ("Affected Party") may, as soon as it becomes aware of the Force Majeure Event, claim relief from liability in respect of any delay in performance or any non-performance of any such obligation to the extent that the delay or non-performance is due to a Force Majeure Event, provided that the Affected Party promptly notifies the other Party in writing, in any case no later than one (1) day, after becoming aware that such delay was likely to occur, of the cause of the delay or non-performance and the likely duration of the delay or nonperformance.

10 RESOLUTION - TERMINATION - CANCELLATION OF THE ORDER

10.1 Either Party will have the right at any time to terminate the Purchase Order or Contract by giving written notice to the other, if:

1. any event of force majeure prevents the performance of all or a substantial part of the obligations of the other party in relation to such Service for a continuous period of twenty (20) days from the date on which such obligation should have been performed; or

2. the other party fails to comply with any term or condition set out in the Order or these GTC.

10.2 BT will have the right to terminate, completely or partially, the contract or any part of it at any time on a one (1) month's prior written notice to the other party, paying the Supplier solely any pending charges already made up to the date of its early termination.

10.3 In cases of partial termination, only the rights and obligations corresponding to the services that continue to be provided will be required.

10.4 Notwithstanding the termination of the Order, the obligations of intellectual and industrial property rights (condition 12), protection of personal data (condition 13), and confidentiality (condition 14) shall remain in force.

10.5 In the event of any breach of these GTC, and in particular any delay in delivery, BT may cancel the Order, without prejudice to any claim for damages.

11 ASSIGNMENT, NOVATION AND SUBCONTRACTING

11.1 The Supplier will not assign or sub-contract the Purchase Order or the services which are the subject of the Purchase Order or the content of the obligations arising out of these GCC, in whole or in part, without the prior written consent of BT. Such permission, if given, shall not relieve the Supplier of any obligation or liability it has under the Purchase Order or these GCC. The Supplier shall provide BT with reasonable access to the Subcontractor to obtain adequate assurances as to the performance and quality of the Service.

11.2 BT reserves the right to assign the whole or part of the Purchase Order to any of the companies within the BT Group or to its subsidiary or parent companies or to any other company in which BT holds stock or any company that holds stock in BT, upon giving the Supplier at least thirty (30) days written notice of such assignment.

12 INTELLECTUAL PROPERTY RIGHTS

12.1 BT's Intellectual and Industrial Property:

a. BT or its legitimate holder will remain the sole owner and proprietor of any title to and all Intellectual or Industrial Property Rights in the Goods of BT, materials, software, operating manuals and associated documentation, supplied or made available to the Supplier or otherwise generated by the Supplier in connection with these GTCS or the agreement and Purchase Orders. Nothing in these GTC shall be construed or interpreted as BT granting to the Supplier any licence or right on BT's intellectual or industrial property. The intellectual property rights in the works made by the Supplier under these GTC and the Purchase Orders or Agreements entered into among the Supplier and BT shall be the property of the latter. The Supplier hereby expressly and exclusively assigns to BT all rights to exploit such works, including the rights of reproduction, distribution, public communication, and adaptation, worldwide and for the entire duration of the intellectual property rights. This assignment is deemed to be included in the agreed price.

b. The Supplier will maintain, at all times, any software or other material containing BT's Intellectual Property Rights as confidential and will safeguard that they are not copied, disclosed or used by any third party without BT's prior written consent. The Supplier shall indemnify BT for all damages that it may cause BT as a result of Supplier's infringement of section 12.1.

12.2 Intellectual and Industrial Property Rights on the Products and Services of the GTCs:

1. In the event that the goods and services include software, the Supplier grants BT an irrevocable, non-exclusive, worldwide licence, with the right to sub-licence in the event that BT sells or rents the goods and services to a third party, to use the software or the goods supplied and for that sole purpose.

2. The Supplier guarantees to BT, and shall provide it with all documentary evidence, if required, that it owns the patents, trademarks or rights of use of the trademarks, licences and other intellectual and industrial property rights on the Software that the Supplier may provide BT. The Supplier shall keep BT harmless against any infringement of intellectual and/or industrial property that may occur from the Supplier's conduct. In addition, the Supplier, at its own expense, including the legal defence of BT against all claims and/or complaints received as a result of the supplier's, direct or indirect, infringements of third parties intellectual and industrial property rights, shall take all any necessary actions to keep BT harmless thereof.

13 DATA PROTECTION

13.1 For the purposes of this section, the following terms shall have the following meanings:

"BT" shall mean any company which provides personal data to the Supplier or from which the Supplier acquires Personal Data in connection with the Contract.

"**Data Protection Legislation**" means the European Union's General Data Protection Regulations 2016/679 on the protection of individuals with regard to the processing of personal data and the free movement of such data, such as Organic Law 3/2018 on Data Protection and Digital Rights Guarantees, and any subsequent amendments or regulations implementing it. The terms used in this section and defined in such regulations shall have the meaning attributed to them therein.

13.2 The Parties undertake to comply at all times with the provisions of the Data Protection Regulations in the development of their activity and in the execution of this Contract and to transfer and reflect the stipulations and obligations of this section 13 in the contracts with their subcontractors and agents, guaranteeing compliance with the provisions of the same.

13.3 For the exclusive purpose of maintaining and managing the contractual relationship and for the proper execution of the Contract, each party will receive personal data from the other (mainly commercial contact details of employees and, where applicable, of subcontractors and agents) and will undertake to:

1. guarantee that they have at all times the legal basis or legitimacy necessary for the processing of the personal data they provide to the other party;

2. process the personal data received from the other party for the sole purpose of maintaining and managing the contractual relationship between the parties, contacting the other party for the purposes of this Contract, as well as for the correct performance of the rights and obligations arising from it;

3. to inform the interested parties of the extremes and in the form and time periods foreseen in section 14 of the GDPR; and

4. in the event of a violation of the security of personal data, notify the other party at the time it becomes aware of it, indicating the relevant aspects that it should be aware of and guaranteeing, in any case, that the other party can comply with the obligations that, where appropriate, correspond to it in accordance with the provisions of the regulations on Data Protection

13.4 It is not within the scope of this Agreement that either party carries out any processing of personal data as processor on behalf of the other party. In the event that such processing is to be carried out for any reason, both parties will negotiate in good faith a new agreement setting out the arrangements necessary to carry out such processing in accordance with Data Protection legislation and including at least the security measures in Condition 16. In addition, in the event that the Supplier processes personal data on behalf of BT, the Supplier may be required to complete a questionnaire to establish which personal data it collects and how it processes such data, in accordance with the Generic Standard GS 12 Data Privacy available at https://groupextranet.bt.com/selling2bt/articles/side/policies_portal.html.

Any breach by the Supplier of this Clause 13 or of the Data Protection laws will be considered a major non-compliance with this Agreement.

14 CONFIDENTIALITY

14.1 The Supplier expressly undertakes to keep confidential any information supplied to it by BT as a result of the business relationship between the parties. Thus, during the term of these GTC, or of the Orders and upon completion thereof, each of the parties shall ensure that any documentation, information, technical data, design, manufacture, installation or operation that may have been exchanged does not come to the knowledge of competitors of either party or of third parties that may prejudice the industrial or commercial research position of BT.

14.2 Each Party will keep in strict confidence all Confidential Information disclosed to it and will:

1. only disclose Confidential Information to those of its employees, agents, Group Companies, officers, directors, advisers, insurers, Subcontractors and suppliers, who need to know it for the purpose of that Party discharging its obligations or receiving a benefit under the Contract, and will ensure that those receiving Confidential Information under this Section 14.2.a)comply with the obligations set out in this Section 14 as though they were a party to the Contract;

2. only disclose Confidential Information as required by Applicable Law, to any Authority or to a Court; or

3. not use or exploit the Confidential Information in any way different to what it is agreed in this Contract.

14.3 Section 14.2 will not apply to Confidential Information that:

1. is or becomes available to the public other than as a result of a breach of the Contract;

2. was lawfully available to a Party on a non-confidential basis prior to disclosure by the disclosing Party;

3. the Parties agree in writing it is not Confidential Information; or

4. was developed by or known by the receiving Party independently of the information disclosed by the disclosing Party.

14.4 Upon written request from a Party, the other Party will return or destroy, as its own cost, any Confidential Information received from the requesting Party within a reasonable time period and will provide written confirmation on request by the requesting party.

14.5 The Parties agree that if either of them breaches this Section 14, damages may not be an adequate remedy for the disclosing party and it will have the right to apply for injunctive relief or specific performance of the recipient's obligations.

15 SUPPLIER PERSONNEL

15.1 For the provision of the Services, the Supplier will use its own personnel, which will always be under its dependence, supervision and professional control, and over which the Supplier will exercise the direction, control, selection, training, replacement, assurance, compensation, discipline and such other employer authorities provided by employment law. The Supplier should provide its Personnel with the necessary equipment, tools and materials so that they can properly perform the tasks object of this Contract.

15.2 The relationship between the parties is exclusively of a commercial nature, and there is no labor relationship between BT and the Supplier Personnel. Therefore, the Supplier Personnel may not be considered in fact or by law, as BT employees. At no time may it be understood that the signing of this Contract means the establishment of any employment relationship between BT or its main client and the Supplier Personnel. To this extent, the Supplier undertakes the following:

1. To assign the necessary human resources, both in quality and quantity, to carry out all its obligations under the terms of this Contract, performing and managing the service under its control and coordination, applying the appropriate standards and methodologies and providing BT, periodically, sufficient information to facilitate supervision and decision making throughout the performance of the service, all regardless of whether the work subject to this service is carried out at the facilities of the Supplier, BT or its main customer, according to its needs.

2. To comply with all employment law obligations - including those related to workers' health and safety -, Social Security in relation to Supplier Personnel, as well as any additional expenses or costs incurred by their employees in providing the services collected in this contract, exempting, in this respect, from any responsibility to BT, other than expressly provided in this contract. Breach of any Supplier obligation with respect to Supplier Personnel shall entitle BT to terminate this Contract with immediate effect.

3. The training of Supplier Personnel rendering services at BT facilities is Supplier's exclusive obligation and responsibility, and will conform to each employee's responsibilities for the Services. The training material and content shall be previously agreed upon with BT or with the latter's training agency, if applicable. The training of Supplier Personnel is included in the price of the Service.

4. The Supplier Personnel rendering Services at BT facilities should be clearly identified as Supplier employees and they should carry some kind of distinctive sign to ease their identification as Supplier Personnel. BT will make available to the Supplier Personnel working at BT facilities an area that allows clearly separation from BT employees, adding or including, if necessary, for this purpose, sign in the furniture or at the area used by Supplier Personnel.

5. Where Supplier Personnel is to render services at Supplier premises, both the Supplier and BT will each designate their relevant Service coordinators or project managers, as contacts and liaison persons between both companies for the purposes of the Service. BT coordinators or BT main client's coordinators shall not give direct work instructions to the Supplier Personnel; rather they should provide indications to the Supplier project manager, who shall be the only one giving instructions to the Supplier Personnel.

6. The Supplier shall designate among the Supplier Personnel assigned to the rendering of the Services a coordinator or project manager who will be the only contact person and liaison with BT and its employees within its facilities. Likewise, BT will designate its own part Coordinator or project manager, who will be the only person at BT keeping contact and liaising with the Supplier Personnel at BT facilities.

7. The Supplier Personnel assigned to the Services will not interact with both BT or BT employees for the purposes of this contract. Any communication and / or request required between Supplier Personnel at BT must necessarily be channeled through the Supplier coordinator or project manager, who will properly send communications to the BT coordinator or project manager.

8. Upon BT's request the Supplier shall make available to BT the documents proving the Supplier employment relationship and evidencing compliance with employment, tax and Social Security obligations, including.

15.3 BT or its main client shall comply with the following obligations:

1. To refrain from applying or communicating to Supplier Personnel any measure that may affect their working conditions.

2. To hold communications regarding the Services or that might affect Supplier Personnel work conditions with Supplier coordinators, and to refrain from taking any measure before there is evidence that this has been communicated to the Supplier coordinator or project manager.

15.4 The Supplier Supervisors or project managers will review from time to time Supplier Personnel, individually dealing with the achievement of targets, productivity and career plan, designed by the Supplier for each of its workers.

15.5 The Supplier undertakes to ensure Supplier Personnel have the necessary qualification and experience, guaranteeing at all times that the Services are of high standard, in accordance with the requirements of expertise , skill and knowledge that can generally be expected in the rendering of the Services by reputable service companies, and undertakes that the Personnel shall act, in the exercise of their commitments, obligations and work, with the due diligence and in accordance with the generally accepted and acceptable standards of urbanity in the professional work environment. BT and the Supplier will carry out quality controls on the

development of the Service, according to the policy and quality parameters previously established by BT and agreed by the Parties.

15.6 BT and the Supplier shall carry out quality controls on the performance of the Service, in accordance with the policy and quality parameters previously established by BT and agreed by the Parties.

15.7 The Supplier undertakes to ensure Supplier Personnel have the necessary qualification and experience, guaranteeing at all times that the Services are of high standard, in accordance with the requirements of expertise , skill and knowledge that can generally be expected in the rendering of the Services by reputable service companies, and undertakes that the Personnel shall act, in the exercise of their commitments, obligations and work, with the due diligence and in accordance with the generally accepted and acceptable standards of urbanity in the professional work environment. BT and the Supplier will carry out quality controls on the development of the Service, according to the policy and quality parameters previously established by BT and agreed by the Parties.

15.8 BT and the Supplier Coordinators or project managers shall meet from time to time to discuss the execution and development of the Service, in accordance with the this Agreement and its Annexes.

15.9 BT shall not be liable for any loss or damage to the property of the Supplier or the Supplier's Personnel while they are on a BT premises.

15.10 The Supplier shall indemnify BT for any claim for damages or losses of any other kind, and / or for any complaint that may be received jointly and severally, subsidiarily or through the exercise of any direct or indirect action, in relation to the Supplier Personnel, including and without constituting a limitation, payments to Social Security, severance payments, amounts paid in out-of-court labor agreements or any other payment of amount, sanction, tax or any other concept that may be required of BT, as a consequence of non-compliance by the Supplier of the obligations provided.

16 ADDITIONAL SECURITY MEASURES APPLICABLE TO DATA ACCESS/PROCESSING

16.1 This section sets out the security obligations to be complied with by the Supplier in the provision of services to BT, where the provision involves access to BT's or third party's data relating to it, which are either personal or non-confidential, and are additional and complementary to those set out in the Data Protection condition.

16.2 Unless BT requests that it be provided, the Supplier shall delete the data processed or generated after the end of the contract or the legal period in which the data must be retained by the Seller by operation of law.

16.3 The Supplier assumes responsibility for making public and disclosing to all persons directly or indirectly involved in the processing of the data the security measures, rules and procedures adopted to ensure the security of the data, preventing their alteration, loss, processing or unauthorised access. Likewise, it will inform about the Duty of Secrecy to which it is obliged by Law. The Supplier thus assumes the responsibility of ensuring that all those persons involved in the processing of the data during the provision of the service are aware of the objectives and

scope of their functions, as well as the obligations arising therefrom, the rules they must comply with and the consequences of non-compliance.

16.4 Incident Registration System:

1. The Supplier will establish an Incident Registration System in which it must be recorded:
   i. Date and time when the incident occurred.
   ii. Type of incident.
   iii. Data identifying the person making the notification.
   iv. Data identifying the person to whom the notification is made.
   v. Effects arising from the occurrence.
   vi. Corrective measure applied.

2. Any anomaly or malfunction that occurs and that affects or could affect the security of the personal data will be notified immediately to BT, indicating all the points included in point a) above.

3. The Supplier will take the necessary preventive and/or corrective measures to ensure that the incident is resolved and that the effects on data security and the likelihood of the incident being repeated are eliminated or minimised. BT shall be informed of the characteristics of the measures taken and may dismiss them if they are not considered appropriate.

16.5 Access to data:

1. Only those persons whose intervention is necessary in any of the phases of the processing that makes up the service shall have access to the personal or confidential data, files and resources affected. The Supplier may request from BT a complete list of persons with access to the protected resources (any component part of the information system).

2. The Supplier will maintain a user map specifying which users have access to which protected resources and the type of access permitted. Access permissions shall be established exclusively on the basis of the needs arising from the functions assigned to the user in such a way as to ensure that access to data and resources is restricted. BT may request a description of the assignments made from the Supplier.

3. The Supplier will implement user authentication mechanisms with access to the systems that will enable the identity of the user to be checked securely in order to prevent impersonation and unauthorised access.

4. The Supplier will adopt the necessary security measures to ensure that the authentication processes are secure. Specific security and control standards will be adopted to preserve the quality of user passwords and to control their assignment, distribution and storage in a secure manner. BT may override the security measures adopted by the Supplier if it believes that such measures are insufficient in relation to the security policy implemented by BT. The Supplier must change its passwords at least every year and in any event should be documented in the Security Document.

5. The Supplier shall implement a mechanism for controlling access to resources that ensures that users' access is restricted exclusively to authorised resources and with the established

permissions. It will identify those responsible for the administration of logical access control and only the designated persons will be able to grant, alter or cancel access to the data and resources and always in accordance with the security criteria established by the Data Controller.

16.6 Data carriers and backups

1. Only those people whose intervention is necessary in any of the phases of the treatment that configures the service will have access to the personal or confidential data, files and resources affected. The Supplier may request from BT a complete list of the persons with access to the protected resources (any component part of the information system).

2. The Supplier will maintain a user map specifying which users have access to which protected resources and the type of access permitted. Access permissions shall be established exclusively on the basis of the needs arising from the functions assigned to the user in such a way as to ensure that access to data and resources is restricted. BT may request a description of the assignments made from the Supplier.

3. The Supplier will implement user authentication mechanisms with access to the systems that will enable the identity of the user to be checked securely in order to prevent impersonation and unauthorised access.

4. The Supplier will adopt the necessary security measures to ensure that the authentication processes are secure. Specific security and control standards will be adopted to preserve the quality of user passwords and to control their assignment, distribution and storage in a secure manner. BT may override the security measures adopted by the Supplier if it believes that such measures are insufficient in relation to the security policy implemented by BT. The Supplier must change its passwords at least every year and in any event should be documented in the Security Document.

5. The Supplier shall implement a mechanism for controlling access to resources that ensures that users' access is restricted exclusively to authorised resources and with the established permissions. It will identify those responsible for the administration of logical access control and only the designated persons will be able to grant, alter or cancel access to the data and resources and always in accordance with the security criteria established by the Data Controller.

16.7 Data carriers and backups

1. All the media containing personal data (both the base data and the data resulting from the processes that make up the treatment object of the service contracted) shall be inventoried and physically identified so that it can always be known:

    i. Their physical location.
    ii. Its content.
    iii. The degree of sensitivity and confidentiality of the information it contains.

2. The exchange of media containing personal data between the BT and the Supplier will be carried out by adopting the necessary security measures to protect the integrity of the media

and the information they contain, as well as the confidentiality of the data, during the transfers that are planned. The Supplier will specify in each case the conditions under which the transfer will be carried out.

3. The Supplier is responsible for ensuring that the media under its control are not transferred under any circumstances outside the facilities designated for their processing or storage without the knowledge and authorisation of BT. The removal of media and documents containing personal data, including those included in and/or attached to an e-mail, must always be authorised by the Data Controller.

4. The Supplier shall establish procedures for making backup copies, at least once a week. Likewise, the Supplier will establish procedures for the recovery of the data that guarantee at all times their reconstruction in the state in which they were at the time of the loss or destruction.

5. The Supplier will be responsible for verifying every six months the correct definition, operation and application of the procedures for making backup copies and recovering data.

17 ANTI-BRIBERY OBLIGATIONS

17.1 In this Condition "Affiliate" means in relation to the Supplier, (i) any person or entity under its control; and (ii) any person or entity that controls it and (iii) any other person or entity under the control of a person or entity supervising it under (ii).

17.2 The Supplier undertakes that

1. ensure that it and its Subsidiaries engage only in legitimate business and ethical practices and abide by and comply with all applicable laws, including, but not limited to, the anti-corruption laws of any country in which the Contract is executed, in the United Kingdom and the United States

2. not give, offer, agree or promise, and cause its Affiliates not to provide, directly or indirectly, any money or anything else of value to anyone or seek or receive any money or anything else of value from anyone, as an inducement or reward for favorable action or forbearance from any action or exercise of influence This applies to any gift, offer, agreement or promise to do so to any official government, national or regional, to any director or head of any corporate body or to any other person;

3. neither he, nor his Affiliates, contractors, officers, directors, employees, shareholders (whose shares are not listed), members or agents are a "Politically Exposed Person". This is defined as: a person who in the last twelve (12) months held a significant public office in any state and his family members and close associates. A significant public function includes: heads of state, heads of government and ministers; members of parliament; members of high-level judicial bodies; ambassadors, chargé d'affaires and high-ranking military officers; as well as members of administrative, managerial or supervisory bodies of state-owned enterprises;

4. all information provided by the Supplier to BT and its representatives in connection with its obligations under this Condition is current, accurate and complete. If there are any material changes to this information, the Supplier will notify BT of such changes as soon as practicable. BT may terminate the Agreement if it does not agree to such changes;

5. prior to engaging a subagent to perform the services on behalf of BT under the Agreement, the Supplier will obtain BT's written approval and will procure that each subagent agrees in writing to the provisions set out in this Term (mutatis mutandis);

6. at BT's request, the Supplier will provide documents and information to BT confirming the compliance of the Supplier and its Affiliates with this Term and will permit BT (or its agents) to review, at any time, the books and records of the Affiliates, in relation to work carried out on behalf of BT;

7. if there are any changes in its ownership, the Supplier will inform BT of such changes as soon as practicable. BT may terminate the Contract if BT does not agree to such changes. In respect of listed companies, this paragraph 2(g) applies only if a new owner or group of owners acquires 5% or more of the Supplier's voting share capital; and

8. maintain a separate account for all amounts received by it under the Contract and for all payments made by it in connection with its role of providing services to BT under the Contract, maintain such account in sufficient detail to enable the transactions and the destination of any payments to be verified to the satisfaction of BT and make such account available to BT or its agents, from time to time, on request, for such verification.

17.3 Notwithstanding anything in the Agreement to the contrary, where it is admitted or found that the Supplier or any of its Affiliates has breached paragraph 2 of this Condition or that any representation or statement made by the Supplier or any of its Affiliates in relation to this Condition is materially incorrect:

1. BT will have the option to terminate the Contract immediately;
2. the Supplier shall lose the right to any commission due from BT; and
3. the Supplier shall indemnify BT against any liability arising therefrom.

17.4 The provisions of paragraphs 2 and 3 of this Term shall survive any termination or expiry of the Agreement.

18 LAW AND DISPUTE RESOLUTION

18.1 The Agreement is governed by and construed in accordance with the laws of Spain. The Parties irrevocably agree that the Courts of Madrid will have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with the Agreement.

18.2 DISPUTE RESOLUTION.

18.2.1 Intention for Extrajudicial Resolution. The Parties agree to resolve any dispute or claim arising out of or related to this Agreement through direct negotiation between them, without resorting to the courts, unless an agreement is not reached through such negotiation

18.2.2 Dispute Resolution Procedure.

18.2.2.1 The dispute resolution procedure will be initiated by notifying the other Party, detailing the nature and full particulars of the dispute, the relevant supporting documents, and a proposal for resolving the dispute.

18.2.2.2 The Parties agree to negotiate in good faith and use their reasonable efforts to resolve the dispute within 14 business days following the notification. During this period, the Parties must maintain confidentiality regarding all matters discussed in the negotiation, except for the act of initiating and concluding the negotiation process.

18.2.2.3 Final Offer: Upon the expiration of the 14-day period, both Parties will present an offer to resolve the dispute. If no agreement is reached within the following 7 business days after the offers are made, the negotiation process will be considered concluded. The failure to reach an agreement will allow either Party to file a claim in court.

18.2.3 Documentation of the Attempted Resolution. The Parties shall sign a joint document that records the start date of the negotiation, the issues discussed, the offers made, and the failure to reach an agreement at the conclusion of the negotiation process. This document will serve as evidence of the attempt to resolve the dispute. The initial act and the final act of the negotiation process are not confidential and may be attached to the court claim to prove the extrajudicial dispute resolution attempt.

18.2.4 Exceptions. Nothing in this clause prevents either Party from:

18.2.4.1 Seeking interim or other immediate relief where there is an imminent risk to the Party, which cannot be adequately resolved through negotiation.

18.2.4.2 Exercising any legal rights or remedies available in case of a breach of the terms of this Agreement, after attempting to resolve the conflict through negotiation.

18.2.5 Suspension of Prescription Deadlines. During the negotiation process, the statute of limitations or expiry deadlines for any legal action will be suspended, and will begin anew once the negotiation has ended without agreement or the Parties have communicated the termination of the process in writing. The Parties will have 30 business days from the conclusion of the negotiation process to file a claim in court.

18.3 The Supplier and BT irrevocably agree that the courts of Madrid will have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with the Agreement or its subject matter or formation (including non-contractual disputes or claims) which is not resolved in accordance with the procedure set out in 18.2

19 DEFINED TERMS AND INTERPRETATION

19.1 The following terms and expressions will have the following meanings:

"**Applicable Law**" means laws, regulations, regulatory guidance, obligations, enactments, statutory duties, or rules (including mandatory and legally required industry codes, binding codes of conduct and binding statements of principle incorporated and contained in such rules) applicable to the existence or operation of the Contract or the supply of the Goods, Software or Services from time to time, including (a) as modified, re-enacted or consolidated from time to time; and (b) any applicable subordinate legislation made from time to time;

"**Authority**" means any regulatory, governmental and/or judicial authority (including any public prosecution service) or any self-regulatory organisation, securities exchange, securities association or agency charged with enforcing the Applicable Laws and/or any Regulatory Matters from time to time. For the avoidance of doubt, the term Authority includes any replacement or successor of an Authority; "**BT Customer**" means an existing or potential BT customer;

"**BT Group**" means BT Global ICT Business Spain, S.L.U. with address at C/ María Tubau, 3; 28050 and any of its Affiliates or companies within the BT Group.

"**Charges**" mean the fees and charges payable by BT to the Supplier in relation to the relevant Goods, Software or Services as set out in the Contract;
"**Confidential Information**" means any and all Information, however it is conveyed and whether or not it is designated as "confidential", disclosed by one Party or its employees, agents, Group Companies, officers or advisers, to the other Party under or in connection with the Contract and whether disclosed before, on or after the date of any such agreement including whether in tangible or other form (a) the terms of the Contract; (b) all technical or commercial know-how, Intellectual Property Rights, pricing, specifications, reports, data, notes, documentation, drawings, computer programs, computer outputs, designs, circuit diagrams, models, patterns, samples, inventions (whether capable of being patented or not), developments, trade secrets, processes or initiatives that are of a confidential nature; (c) any information that ought to be reasonably regarded as confidential and relating to the business, affairs, customers, personnel, clients, suppliers, plans or strategy of the disclosing Party or its Group Companies; (d) the operations, product information, designs, trade secrets or software of the disclosing Party or its Group Companies; and (e) any Information disclosed by a BT Customer to the Supplier;
"Controller", "Personal Data", "Personal Data Breach" "Process/Processing" and **"Processor"** will have the meanings ascribed to them in the Directive, and/or in the GDPR;
"**Data Protection Legislation**" means collectively (i) the GDPR; (ii) Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights; (iii) any other applicable national privacy laws; (iv) any successor or replacement laws; and (v) any binding guidance or code of practice issued by a Supervisory Authority;
"**Defect**" means (a) the failure of any of the Goods or Software or, in BT's reasonable opinion, the likely failure of any of the Goods or Software to conform or operate in accordance with the Contract; or (b) where the quality of any of the Goods or Software (including its development, performance or output) (i) is such that they are not as a person may be generally and/or reasonably entitled to expect; (ii) is not satisfactory for any purposes for which such Goods or Software are usually purchased or used; (iii) does not meet the BT Requirements; or (iv) is not otherwise in accordance with the Contract, and "**Defective**" will be construed accordingly;
"Deliverable" means Materials which are to be prepared or created by or on behalf of the Supplier, a Supplier Group Company or any Subcontractor in the course of fulfilling the obligations under the Contract;
"**Directive**" means Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995;
"**GDPR**" means General Data Protection Regulation (EU) 2016/679 repealing the Directive, and any amendment or replacement to it (including any corresponding or equivalent national law or regulation which implements the GDPR);
"**General Conditions**", "**Contract**" or "**Agreement**" mean this document comprising Sections 1 to 19 and its Schedules;
"**Goods**" means the goods (including any firmware and associated software) as set out in the Contract (but excludes any Software to the extent it is licensed separately);
"**Information"** means information whether in tangible or any other form, including, without limitation, specifications, reports, data, notes, documentation, drawings, software, computer outputs, designs, circuit diagrams, models, patterns, samples, inventions, (whether capable of being patented or not) and know-how, and the media (if any) upon which such information is supplied;
"Intellectual Property Rights" means any trade mark, service mark, trade and business name, internet domain names, patent, petty patent, copyright and related rights, database right, rights in designs, semiconductor topography right, rights to use and protect the confidentiality of confidential information (including know-how and trade secrets), or any similar intellectual

property rights in any part of the world, whether registered or unregistered, including any applications and rights to apply for and be granted, renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights which subsist or will subsist now or in the future in any part of the world;
"Minimum security measures to be implemented by Suppliers" means the security measures available at Selling to BT that Suppliers or their subcontractors must implement as a minimum;
"**Policy**" and "**Policies**" means the policies and generic standards of BT and the BT Group accessible on the Policies Portal (as each policy or generic standard is amended by BT and notified to the Supplier from time to time through the Policies Portal);
"**Policies Portal**" means the online repository for the Policies accessible at https://groupextranet.bt.com/selling2bt/PoliciesPortal/index.html or any other URL that may be notified to the Supplier from time to time;
"**Services**" means any or all of the services as set out in the Contract including the provision of Supplier Materials and/or Deliverables;
"**Supplier**" means the supplier of the Goods, Software or Services named in the Purchase Order.

The Supplier acknowledges and agrees to this General Purchasing Terms.

SUPPLIER: _____
Tax ID _____

Signer Name: _____
Position: _____

ANNEX 1: BT SECURITY REQUIREMENTS

The Supplier shall (and ensure that any Subcontractor and Contract Personnel shall) comply with the version 5.3 of the BT Supplier Security Requirements available at BT Supplier Security Requirements or such other website as notified by BT from time to time.

For the current scope of this engagement **Sections --------** are applicable, additional sections may become applicable if the scope, method of working or location of work changes throughout the term. Scope of work should be reviewed annually for security impacted changes and significant changes reported to the BT Security Contact.

Any breach of this Condition by the Supplier shall be deemed to be a material breach of the Contract.

This Condition shall survive the Contract.

BT Security Requirements for Suppliers v 5.3

Contents

1. Introduction

1.1 BT's customers have an expectation that BT and its 3rd Party supply chain provide their services using industry standard information security management systems (ISMS). The 3rd Party's ISMS should cover infrastructure, networks, equipment and IT systems in order to protect services being provided and BT/BT customer information in scope of the services. This document sets out BT's Security Requirements and applies to all 3rd parties working for or on behalf of BT Group, including Openreach, EE and Plusnet, here on referred to as 'BT' for the rest of the document. 3rd Party will be advised which security control sets are applicable to the service it is providing to BT.

1.2 These Security Requirements are in addition to and without prejudice to any other obligations of the 3rd Party in the Contract. They are designed to ensure that BT retains control and oversight of its network and user data.

2. Limited Access Requirements

2.1 Without prejudice to any obligations of confidentiality it may have, where 3rd Party Personnel have Access to BT Information, the 3rd Party must:

2.2 Ensure BT Information is not disclosed to or Accessed by 3rd Party Personnel unless necessary for the provision of the Service; and

2.3 Put in place all systems and processes both technical and organisational as are required to protect BT Information (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or Access to BT Information in accordance with Good Industry Security Practices.

3. General Information Security

3.1 On reasonable request the 3rd Party shall make available to BT copies of security certifications and statement of compliance relevant to the Service to illustrate evidence of compliance with these Security Requirements.

3.2 Should there be a significant change to technology or industry security standards; or there are any material changes to the Services or how they are provided, BT may issue a Contract amendment during the term, if there is a need for a change to the applicable security control sets. The 3rd Party shall comply with the agreed Contract amendment within a reasonable time considering the nature of change and the risk to BT.

3.3 When there are any material changes to the Services or how they are provided, 3rd Party must review this Security Requirements policy to ensure they are still compliant to all applicable security controls.

3.4 If the 3rd Party subcontracts obligations under the Contract, then the 3rd Party shall provide a list of relevant Subcontractors and their locations to BT and shall ensure all Contracts with relevant Subcontractors and their Subcontractors, include written terms requiring the Subcontractor to comply with the applicable parts of either these Security Requirements or to equivalent 3rd Party security requirements, including rights of audit for BT equivalent to those in section 5 below.

3.5 If a 4th party will be used to provide the service, where they will hold or process BT Information, the 3rd Party must obtain agreement from BT. The 3rd Party must ensure they have a contractual relationship with the 4th party and must ensure the 4th party operates an industry standard security framework.

3.6 BT Information may be retained for as long as necessary to perform the Contract, after which it should be retained no longer than a maximum of two years, unless a different retention period has been agreed between BT and 3rd Party or is required by any applicable laws.

3.7 If the Services are in direct support of a UK Government Contract, the 3rd Party must comply with the most current version of the Cyber Essentials Plus - https://www.cyberessentials.ncsc.gov.uk/

3.8 Where BT Information will be processed or stored offshore 3rd Party must advise BT of the geographical locations, BT reserves the right to reject locations that are deemed high risk.

Handling BT Information

3.9 Unless advised otherwise by the BT stakeholder all BT Information is classified as "Confidential". Where personal data or sensitive personal data is in scope advice should be sought from 3rd Party's Data Protection and Privacy Team in case additional controls are required.

The following security controls are "voice handling requirements" which have a scope limited to verbal communications.

3.10 If there is a need to discuss, show or exchange BT Information using a collaboration platform (e.g., Teams)

- Ensure only individuals who have a need to know the information are present.
- If there is an external contractor involved, they must have either a signed contract with the 3rd Party or have an NDA in place prior to discussions starting.
- 3rd Party must verify who is on the conference before starting.

3.11 If there is a need to discuss BT Information with someone face to face, on a mobile phone or standard telephone line.

- Conversations must not be held or overheard by anyone who does not have a need to know.
- If the conversation is required with an external contractor, they must have a signed contract with 3rd Party, or an NDA must be in place prior to discussions starting.
- Confidential or Highly Confidential information must not be left on voice mail services.

The following security controls are "written handling requirements" and have a scope covering material kept in paper format. This includes but is not limited to handwritten letters, minutes, notes, and memos. It also includes printed electronic material such as work documents and reports once they are in a paper format.

3.12 If storing paper copies of BT Information at 3rd Party premises, when not in use these must be secured in a lockable facility, with access restricted to only those with a need to view the material. Documents must not be left unattended.

3.13 If there is a need to print, photocopy or duplicate BT Information, the following security controls apply:

- Only use the printing or copying facilities at 3rd Party's own premises.

- Photocopies or printouts must not be left unattended at the print location and must be collected at the time of creation.
- Where the printer or photocopier has memory capability where copied material can be recalled and re-printed this should be restarted to clear memory as soon as practicable.

3.14 If there is a need to remove copies of BT Information from 3rd Party premises:

- Unless already agreed as part of the scope of work 3rd Party must obtain evidenced consent from the BT stakeholder.
- If approved, the information must not be identifiable whilst in transit and must held in an anonymised or plain folder, bag, or case.
- The material must not be left unattended and must remain in the direct control of the person transporting the material, especially on public transport.

3.15 When no longer required paper copies of BT Information must be disposed of as follows:

- Paper copies must not be disposed of in the general waste bins.
- If using a shredder, it must be a minimum standard of P4 DIN66399.
- If approved shredders are not available information must be disposed of in confidential waste bins.

For "Highly Confidential information" the following additionally applies:

- Information must only be disposed of in confidential waste bins after being shredded.
- Information that is required to be shredded on site by the supplier, must gain a certificate of destruction from the supplier.

The following security controls relate to BT Information in electronic format.

3.16 When storing BT Information on 3rd Party PC or Laptop the following controls apply:

- Only allowed on devices with hard disk encryption (e.g. Bitlocker).
- All documents must be individually encrypted.
- Information Rights Management (IRM) must be applied to the document.
- If supplied, information must retain the BT classification label.

3.17 When saving a BT document to an internal file sharing location for general storage, collaboration or file sharing; the following security controls apply:

- The location the material is being stored to must have access permissions applied to only allow those with a need to see or use the document.
- If supplied, information must retain the BT classification label.
- All documents must be individually encrypted.
- Information Rights Management (IRM) must be applied to the document.
- If in scope of the service being provided PCI and Payment card material must not be saved to file storage sites at any time.
- If guest accounts are required to provide access to an external contractor they must have a signed contract with 3rd Party or an NDA must be in place prior to access being granted.

3.18 If there is a need to save BT Information on 3rd Party removable media (e.g. a USB memory stick) the following security controls apply:

- The device must be encrypted to the same level as the hard drive.
- If lost or stolen 3rd Party must raise a security incident.
- 3rd Party must have the evidences of prior approval from the BT Stakeholder to transfer "highly confidential" material to removable media.
- If in scope of the service, PCI material or personal data must not be stored on removable media.
- Devices intended for support and maintenance shall not be used for any other purpose.

3.19 BT Information must not be stored on personal PC's, laptops, removable media or mobile devices

3.20 BT Information must not be sent or auto-forwarded from a 3rd Party corporate email address to a personal e-mail or external email account unless they are an external contractor that has a signed contract with 3rd Party or an NDA in place and is used to provide the service.

3.21 To minimise the attack surface and the opportunities for attackers to manipulate human behaviour though their interaction with web browsers and email systems, implement processes to ensure that only fully supported web browsers and email clients are allowed and uninstall or disable any unauthorised browser or email client plugins or add-on applications.

3.22 3rd Party must have back-up measures in place in order to restore BT Information within 3 working days, in the event of corruption, loss or degradation.

3.23 When disposing of BT data/Information, full records of data retention and disposal must be kept, providing audit trail, evidence and tracking. This must include:

- Proof of destruction and/or disposal (including date undertaken and method used).
- System audit logs for deletion.
- Data disposal certificates.
- Who undertook the disposal (including any disposal partners / 3rd parties or contractors).
- A destruction and verification report must be generated to confirm the success or failure of any destruction / deletion process. (i.e. an overwriting process must provide a report that details any sectors that couldn't be erased).

3.24 When disposing of equipment where BT data/information was present, an audit trail must be provided for the following equipment types:

- Removable media.
- Disk Drives.
- Back-up tapes.
- Computer components.

3.25 Full records must exist to provide an audit trail to include as a minimum:

- The name of the application or service that utilised this piece of equipment.
- Equipment type e.g. desktop, laptop, server, tape, router etc.
- Number of hard drives the equipment contains (if applicable).
- Equipment identified by serial number.
- Component parts of equipment identified by serial number.

- Full asset tracking of all equipment and component parts through the entire equipment disposal lifecycle.
- Proof of destruction and/or disposal (including date undertaken and method used).
- Details of who undertook the disposal (including any disposal partners / 3rd parties / waste disposal contractors).
- A destruction and verification report must be generated that confirms the success or failure of any recycling/sanitisation or destruction process. For example, an overwriting process must provide a report that details any sectors that couldn't be erased. These reports should include the capacity, make, model and serial number of the media.

Roles & Responsibilities

3.26 Every 3rd Party must be aware and understand the requirements of these security controls and are responsible for making sure that all individuals who are involved in providing a service to BT are familiar and comply with the relevant requirements of this standard.

Governance

3.27 The 3rd Party must have an established and consistent industry standard security framework for information and cyber security governance which covers the following components:

- Appropriate Information and Cyber Security policies and procedures which are approved and communicated.
- An information security strategy.
- Relevant legal and regulatory requirements regarding Information and Cyber Security (including privacy) which are understood and managed.
- Governance and risk management processes which address information and cyber security risks.

3.28 The 3rd Party must ensure that appropriate roles and responsibilities for Information and Cyber Security defined and implemented which includes the following:

- A full-time Chief Information Security Officer (or equivalent) who is sufficiently senior and has responsibility for information security programme.
- A high-level working group, committee or equivalent body which coordinates information security activity across the 3rd Party which is chaired by a suitably senior member of staff and meets on a regular basis.
- A specialist information security function with suitable and defined roles and responsibilities.

3.29 The 3rd Party must ensure that there is individual accountability for information and systems by ensuring that there is appropriate ownership of critical business environments, information, and systems and that this is assigned to capable individuals.

3.30 The 3rd Party must ensure that BT is notified (in writing) as soon as they are legally able to do so if the 3rd Party is subject to a merger, acquisition, or any other change of ownership.

Incident Management

3.31 The 3rd Party must have an established and consistent incident management framework to ensure that incidents are appropriately managed, contained and mitigated and covers the following components:

- Ensuring that personnel know their roles and order of operations when a response is needed.
- Ensuring incidents reported consistent with established criteria.
- Ensuring that the impact of the incident is understood.
- Ensuring that forensics are performed where necessary either internally or by a specialist function.
- Ensuring that lessons learned from incidents are incorporated into best practice.
- Ensuring information related to an incident impacting BT is treated as "Confidential".

3.32 The 3rd Party will take all reasonable steps to ensure appropriate individual(s) are appointed and made responsible as Point of Contact for security risk, incident management and compliance management. 3rd Party shall notify BT Stakeholder of the individual(s) contact details and any change to them.

3.33 The 3rd Party will inform BT via email security@bt.com or by telephone 0800 321 999, within a reasonable timeframe upon becoming aware of any incident that impacts the service to BT or BT Information, and in any event, no later than twenty four (24) hours from the time the Incident comes to 3rd Party's attention.

3.34 The 3rd Party without unreasonable delay, will take appropriate and timely corrective action to mitigate any risks and effects related to the incident to reduce the severity and duration of the incident.

3.35 The 3rd Party will provide within 30 days of an incident a report to the BT Stakeholder in respect of any incident that impacts the service to BT or BT Information, it should include as a minimum:

date and time, location, type of incident, impact, status, and outcome (including the resolution recommendations or actions taken).

3.36 The 3rd Party must perform a root-cause analysis of all security incidents. Outcomes of this analysis should be escalated to the appropriate management level within the 3rd Party's organisation.

Change Management

3.37 The 3rd Party must ensure that all IT changes are approved, logged, and tested, including backing out of failed changes, prior to implementation to prevent service disruption or security breaches and that there is a process for undertaking emergency updates in a controlled manner.

3.38 The 3rd Party must ensure that changes are reflected in both Production and DR environments.

3.39 The 3rd Party must ensure that maintenance and repair of organisational assets is performed and logged, with approved and controlled tools.

3.40 The 3rd Party must ensure that remote maintenance of organisational assets is approved, logged, and performed in a manner that prevents unauthorised access.

Cyber Risk and Threat Management

3.41 The 3rd Party must ensure that there is an ongoing Cyber Security risk and threat assessment framework to ensure that the Cyber Security risk profile to the organisation's operations, assets, premises, and individuals is understood and managed by:

- Assessing asset vulnerabilities.
- Identifying both internal and external threats.
- Sensitivity of information / data in scope.
- Assessing potential business impacts.
- Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
- Ensuring that the Cyber risk and threat management framework is agreed at a suitable level in the organisation.

3.42 The 3rd Party must ensure that all risks and threats identified as part of the Cyber Security Risk and threat assessment are prioritised and action taken accordingly to mitigate the risks in a suitable timescale.

3.43 The 3rd Party must notify BT Stakeholder if they are unable to remediate or reduce any material areas of risk that could impact the service being provided.

Identity Management and Access Control

3.44 The 3rd Party must have an established and consistent framework to ensure that identities and credentials are managed securely by authorised personnel:

- Only granting, re-enabling, changing, and disabling of access rights based on documented and authorised approvals.
- Ensuring that dormant accounts are disabled.
- Disabling accounts of personnel who are no longer in employment.
- Implement processes and tools to track, control, prevent and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
- Periodic reviews of access are in place to ensure that access is fit for purpose.
- User accounts have access recertified on at least an annual basis and privileged accounts have access recertified quarterly.
- Ensure persistent credentials and secrets (e.g., for break glass access) are protected within hardware-protected storage and are only made available to the responsible person(s) in an emergency.
- Ensure non-persistent credentials (e.g., username and password authentication) are stored in a centralised service with appropriate role-based access control which shall be updated in line with any relevant changes to roles and responsibilities within the organisation.

3.45 Central storage for persistent credentials shall be protected by hardware means. For example, on a physical host the drive could be encrypted with the use of a Trusted Platform Module

(TPM). Where a virtual machine (VM) is used to provide a central storage service, that VM and the data included in it shall also be encrypted, use secure boot and be configured to ensure that it can only be booted within an appropriate environment. The 3rd Party must ensure that remote access is managed so that only approved individuals can connect remotely to the 3rd Party's Systems and that connections are secure and prevent data leakage and appropriate access control is in place such as multi-factor authentication.

Two factor authentication should be achieved with a User ID, Password and one of the following methods:

- A one-time password generator: that requires a user specific PIN/password to view the one-time password.
- A smart card with an ISO 7816-compliant chip and associated card reader and software. Contactless smart cards are not permitted.
- Certificate based authentication issued in accordance with the 3rd Party's Infosec certificate policy.

For avoidance of doubt if privileged access for support is provided via remote access, then this must be via a secure connection and use two factor authentication.

3.46 The 3rd Party must ensure that access permissions and authorisations for all systems (including tools, applications, databases, operating systems, hardware etc.) are managed incorporating the principles of least privilege and separation of duties.

3.47 The 3rd Party must ensure that each transaction can be attributed to a unique identifiable individual and that if there are any shared credentials that there are appropriate compensating controls (including break glass procedures). Shared credentials for privileged access are not permitted.

3.48 The 3rd Party must ensure that all authentication is managed commensurate with the risk of the transaction, i.e., appropriate password length and complexity, frequency of changes of passwords, multi-factor authentication, secure management of password credentials or other controls. Privileged access must be via accounts secured with multi-factor authentication. 'Break-glass' privileged user accounts must have strong credentials unique to each network equipment point of access.

3.49 Appropriate controls must be in place to handle failed authentications, including screen notifications, logging of failure and user lockout.

3.50 Processes and controls must be in place to manage and authorise guest and service accounts.

Data Classification and Protection

3.51 The 3rd Party must have an established and consistent information classification, labelling and handling framework / scheme (aligned to Good Industry Practice / BT requirements) which contains the following components:

- Information handling guidelines.
- Information is protected in line with its assigned level of classification.
- Ensuring that all staff aware that BT Information shall not be used for any purpose other than that for which it was provided.

Data Leakage Prevention

3.52 The 3rd Party must have an established and consistent framework to ensure that protection against inappropriate data leakage is in place ensuring protection includes (but not limited to) the following vectors:

- Email, Internet / Web Gateway (including online storage and webmail), USB, Optical and other forms of ports / portable storage etc, Mobile Computing and BYOD, Remote Access Services, file sharing mechanisms and social media.
- Unauthorised devices must not be connected to the network (either the vendor's corporate network or BT's systems / network) or used to access non-public information.

Vulnerability Management.

3.53 The 3rd Party must have an established and consistent vulnerability management framework which includes the following components:

- Processes policies and procedures.
- Defined roles and responsibilities.
- Appropriate tools such as Intrusion Detection Systems and vulnerability scanning systems.

3.54 The 3rd Party's vulnerability management framework must ensure that the following are routinely monitored to detect potential cyber security events:

- Key systems and assets.
- Unauthorised connections.
- Unauthorised software / applications.
- Network activity.

3.55 The 3rd Party's vulnerability management framework must ensure that:

- There are processes established to receive, analyse, and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g., internal testing, security bulletins, or security researchers).
- Only authorised tools, technologies, users are permitted.
- Identified vulnerabilities are mitigated or documented as accepted risks.

Security Continuous Logging and Monitoring.

3.56 The 3rd Party must ensure that there is an established and consistent audit and log management framework which ensures that key systems including applications are set to log key events (including those of privileged access and personnel activity) with such logs being retained for a minimum period of 13 months. Logs for network equipment in Security Critical Functions must be fully recorded and made available for audit for 13 months.

As a minimum the 3rd Party must ensure that logs address the following events:

- System start-up and shutdown.
- Successful and unsuccessful authentication
- System log-on log-off
- Creation, modification, and deletion to/of accounts
- Credential change
- Privilege escalation
- Account lockout
- Hardware attachments and removals
- System and network management alerts and error messages
- Security event admin changes; including group management and security policy changes
- Start and stop points of the logged process
- Log activation or deactivation events
- Changes to the type of logged events as required by the audit trail (for example the start-up parameters and any changes to them).
- Log modification (or attempted modification)
- Any form of access to the management plane of systems used in connection with a UK public electronic communications network or service

As a minimum the 3rd Party must ensure that the following log parameters are captured for each event:

- Identity of asset to which the event relates
- Type of event
- Date and time of event
- An indication of success/failure of event
- Account user ID
- Identification of the source of event such as user/systems location, IP addresses terminal ID, terminal ID or other means of identification

3.57 The 3rd Party auditing, logging and monitoring framework must include the following components:

- Event logs generate alerts in real or near-real time to identify unauthorised activity
- Events and alerts are monitored by an independent function on a continuous basis and are investigated, triaged and assigned a level of severity
- Triaged alerts invoke Security Incident Management processes based on established protective monitoring use cases and playbooks in accordance with service level agreements and severity
- Logs are treated as having an information classification of “Confidential” as a minimum and protected against tampering, unauthorised access and loss
- Logging and monitoring activity is synchronised to an approved NTP time source

- Processes are established to identify and configure additional protective monitoring use cases and associated event logs, correlations and alerts necessary to address existing or emerging significant threats and risks

4. 3rd Party Personnel Security

4.1 The 3rd Party shall ensure that all 3rd Party Personnel have confidentiality agreements in place before any 3rd Party Personnel start working in BT buildings or on BT Systems or have Access to BT Information. These confidentiality agreements must be retained by 3rd Party and evidence be made available for audit by BT.

4.2 The 3rd Party shall deal with breaches of 3rd Party and applicable BT security controls and standards, through formal processes including disciplinary action which may include removal of the individual from:

- having Access to BT Systems or BT Information; or
- carrying out work connected with the provision of the Service.

In addition, the 3rd Party shall ensure they have relevant processes in place to ensure any 3rd Party Personnel who have been so removed are not subsequently given Access to BT Systems, BT Information or allowed to work in connection with the provision of the Service.

4.3 The 3rd Party shall, to the extent permissible by the law, maintain a confidential facility, to be used by the 3rd Party Personnel to anonymously report if they are instructed to act in a manner inconsistent or in violation of these Security Requirements. Relevant reports are to be notified to BT.

4.4 When 3rd Party Personnel are no longer assigned to the Service, at BT's option, any BT physical assets or BT Information in the possession of 3rd Party Personnel shall be either: handed back to the relevant BT operational team or securely destroyed as per security controls 3.22 and 3.23.

4.5 The 3rd Party must have an established and consistent framework on acceptable use of personal and corporate social media including ensuring personnel:

- do not post anything libellous, obscene, or abusive about the organisation, its clients or customers.
- do not use organisation or client logos without prior permission.
- do not expose organisation or client non-public information without prior consent.
- do not post opinions about the organisation its clients or customers which could reasonably be construed as official comment of the organisation or its clients.
- do not release any BT Information that is marked as 'General', 'Confidential' or 'Highly Confidential'.

4.6 The 3rd Party must ensure that all 3rd Party Personnel under their control undertake mandatory security of information training, which includes Cyber Security best practice and protection of personal data within one month of joining and refreshed at least on an annual basis including where appropriate:

- Privileged users
- 3rd Party stakeholders (e.g., Sub-contractors, customers, partners)

- Senior executives
- Physical and Cyber Security personnel

4.7 The 3rd Party must ensure that there is a testing component to verify that the user understands the training and awareness.

4.8 The 3rd Party must ensure that an up-to-date register is maintained listing the 3rd Party Personnel who have received the training referred to in paragraph 4.6 above, the related contents, and, where applicable, the list of assessments carried out.

5. Audit & Security Review

5.1 Without prejudice to any other right of audit that BT may have, to assess the 3rd Party's compliance to the security controls in this Security Requirements policy, the 3rd Party will provide BT, or its representatives, access, and assistance as necessary and appropriate to allow document-based security reviews or on-site audits to be undertaken. A minimum of 30 working days' notice will be provided to 3rd Party prior to a routine onsite audit.

The scope of the audit will be to review any or all aspects of the 3rd Party's policies, processes, and system(s) (subject to the 3rd Party protecting the confidentiality of any information not related to the provision of the Service to BT), that are relevant to the Service being provided.

5.2 The 3rd Party will work with BT to implement agreed recommendations and carry out any corrective actions identified as necessary resulting from a document-based security review or on-site audit within 30 days of being notified by BT of a major non-compliance, 90 days of being notified by BT of a minor non-compliance, or such period as agreed between the parties at the 3rd Party's expense.

6. Right of Inspection

6.1 The 3rd Party must permit BT to undertake an inspection of the control environment where the services are developed, manufactured, or provided to perform security compliance testing and/or assessments on reasonable request (or immediately following an incident).

6.2 The 3rd Party is responsible for the costs of remediating any security weaknesses identified by BT within a timescale as agreed by both Parties.

6.3 In the event of a serious incident the 3rd Party shall fully cooperate with BT in any ensuing investigation by BT, a regulatory authority and/or any law enforcement agency by providing access and assistance as necessary and appropriate to investigate the incident. BT may have need to request the 3rd Party quarantine for evaluation any relevant asset belonging to 3rd Party to aid the investigation and 3rd Party shall not unreasonably withhold or delay such request.

7. Security Certifications

7.1 The 3rd Party Systems, Service, associated Services, processes, and physical locations must be compliant with and shall continuously comply with the ISO/IEC 27001 standard (or certification(s) that demonstrate equivalent controls, supported by an independent auditor report) and any amended or future version of the standard issued. This compliance must be assured by certification of the 3rd Party's ISMS by a UK Accreditation Service (UKAS) or an international equivalent approved certification body where the scope and statement of applicability encompasses the services being provided at the locations they will be provided from.

7.2 The 3rd Party must submit a valid certificate at the start of the contract and on future re-certifications.

7.3 Should the scope of the certificate or statement of applicability be changed during the term of the contract to the extent it no longer covers all the services being provided at the locations they are provided from, the 3rd Party must advise BT within a reasonable time frame. The 3rd Party must inform BT within 2 working days of any major non-conformance identified by the certification body or the 3rd Party, which poses a risk to the services being provided.

8. Physical Security – BT Premises

8.1 The 3rd Party shall adhere to all relevant instructions provided to them with regards to access to BT premises and building entry systems. All 3rd Party Personnel working on BT premises shall be in possession of, and display prominently, a 3rd Party or BT provided identification card which must include a photographic image displayed on the card that is a clear and true likeness of the 3rd Party Personnel.

8.2 BT may also provide 3rd Party Personnel with an electronic access card and/or limited duration visitor card which shall be used in accordance with local issuance and revocation instructions

8.3 The 3rd Party is responsible for advising BT with 24 hours when a 3rd Party individual no longer requires BT building access and/or access to BT entry systems.

8.4 Only approved BT build servers, BT Webtop PCs and Trusted End Devices can directly connect (plug into LAN port or Wireless connection) to BT domains. The 3rd Party must not without the prior written authorisation from BT connect any equipment not approved by BT to any BT Domain.

8.5 Physical protection and guidelines for working in BT premises shall be adhered to, and shall include but not be limited to, the escorting of 3rd Party Personnel and the adoption of appropriate working practices within secure areas.

8.6 Where the 3rd Party is authorised to provide its 3rd Party Personnel with un-hosted access to areas within the BT estate; the 3rd Party authorised signatory and 3rd Party Personnel must adhere to the guidance document Supplier Access to BT's sites - Mandatory Security Guide Selling to BT.

9. Physical Security – 3rd Party Premises

9.1 The 3rd Party must have a physical access process that covers access methods and authorisation to 3rd Party premises (sites, buildings, or internal areas) where services are provided, or where BT Information is stored or processed. Access method shall include 1 or more of the following:

- An authorised 3rd Party identification card with a photographic image displayed on the card that is a clear and be a true likeness of the individual.
- An authorised electronic access card to access the applicable areas of the premises.
- Keypad security access, which must have processes for: authorisation, the dissemination of code changes (which must occur monthly, as a minimum); and ad-hoc code changes.
- Biometric recognition.

9.2 The 3rd Party must have processes and procedures for the control and monitoring of visitors and other external persons, including personnel with physical access to secure areas or for the purpose of environmental control maintenance, alarm maintenance and cleaning.

9.3 Secure areas in 3rd Party premises used to provide the service (e.g., network communications rooms) shall be segregated from general access areas and protected by appropriate entry controls to ensure that only authorised individuals are allowed access. Access made to these areas must be audited regularly and an assessment of re-authorisation of access rights to these areas must be carried out annually as a minimum.

9.4 The 3rd Party shall have CCTV security systems in locations where BT Information is stored or handled. Recordings and recorders must be securely located to prevent modification, deletion or the 'casual' viewing of any associated CCTV screens and access to the recordings must be controlled and restricted to authorised individuals only. CCTV recordings must be retained for a minimum of 20 days.

9.5 The 3rd Party must have implemented appropriate measures to ensure physical security with respect to the following:

- Fire prevention measures including but not limited to alarms, detection, and suppression equipment.
- Climatic conditions, with consideration given to temperature, humidity and static electricity and the associated management, monitoring, and response to extreme conditions (such as automatic shutdown, alarms).
- Control equipment including, but not limited to air conditioning and water detection.
- Prevention of water damage, location of water tanks, pipes etc. within the premises.

9.6 The 3rd Party must ensure that physical access to areas that are hosting BT Information is with smart or proximity cards (or equivalent or better security systems) and 3rd Party must conduct monthly checks to ensure only relevant individuals are provided with this access.

9.7 The 3rd Party must ensure that photography and/or the image capture of any BT Information is prohibited. Where there is a business need to capture such images, confirmation must be obtained in writing from the BT Stakeholder.

10. Provision of Hosting Environment for BT Equipment

10.1 The 3rd Party must, where the 3rd Party is providing a secure access area on their premises for hosting BT or BT customer equipment:

- Provide BT with a floor plan of allocated space in the secure area of the premises.
- Ensure that BT and BT customer cabinets at the premises are kept locked and only accessed by authorised BT personnel, BT approved representatives and relevant 3rd Party Personnel.
- Implement a secure key management process.

10.2 BT shall provide the 3rd Party with:

- A record of BT and/or BT customer's physical assets held at the 3rd Party premises.
- Details of BT's employees, subcontractors and agents that need access to the 3rd Party premises (on an on-going basis).

11. Secure Software Development

11.1 The 3rd Party must ensure that production and non-production environments are appropriately controlled by ensuring the following components are in place:

- Segregation of production and non-production environments with segregation of duty.
- No live data to be used in test unless prior agreement from the data owners and controls commensurate with the production environment.
- Segregation of duties between production and non-production development.

11.2 The 3rd Party must have an established and consistent Systems Development framework to prevent security vulnerabilities and Cyber Security breaches which contains the following components:

- Systems are developed in line with Secure Development best practice (e.g., OWASP).
- Code is securely stored and subject to Quality Assurance.
- Code is adequately protected from unauthorised modification once testing has been signed off and delivered into production.

12. Escrow

12.1 Where Escrow is required to protect all parties for either 1st party or 3rd Party Escrow (i.e., for Intellectual Property / Source code etc.) the 3rd Party must have a consistent and established framework which includes the following components:

- Execution of escrow agreement with independent, neutral, and reputable Escrow agent.
- Delivery and ongoing updates of source code and other materials to the Escrow agent to ensure the required information is up to date.
- Secure storage of source code and other materials until release conditions are met.
- Appropriate release conditions.
- Ongoing updates, appropriate payments, and reviews to the Escrow agreement.

13. Access to BT Systems

13.1 The 3rd Party shall adhere to all relevant instructions provided to them with regards to access and use of BT Systems.

13.2 3rd Party is responsible for advising BT with 24 hours when a 3rd Party individual no longer requires access.

13.3 The 3rd Party shall ensure user identification, passwords, PINs, tokens, and conferencing access are for individual 3rd Party Personnel and not shared. Details must be stored securely and separately from the device that is used to access. If a password is known by another person, it must be changed immediately.

System to System connectivity

13.4 Inter domain linking to BT Systems is not permissible unless specifically approved and authorised by BT.

13.5 The 3rd Party must use all reasonable endeavours to ensure no malware (as the expression is generally understood in the computing industry) is introduced to BT Systems.

13.6 Where there is connectivity between the 3rd Party and BT systems the connectivity will be via secure links with data protected by encryption conforming to the cryptography controls in 14.9, 14.10, 14.11, 14.12 and 14.13.

13.7 The 3rd Party will ensure that the systems and infrastructure used are contained within a dedicated logical network. This network must consist only of the systems dedicated to delivery of a secure customer data processing facility.

14. 3rd Party Systems holding BT Information

14.1 3rd Party must ensure that the latest security patches are applied to systems/assets/Networks/applications ensuring that:

- 3rd Party deploys patches as soon as reasonably practicable and uses best endeavours to deploy within the following timescales following patch release:

	Actively exploited in the wild	**High EPSS** Vulnerability CVSS: > 8.0 (High + Critical) EPSS: >= 70% (Network Attack Vector – see definitions section)	**Lower EPSS** Vulnerability CVSS: > 8.0 (High + Critical) EPSS: < 70% (Network Attack Vector – see definitions section)	**Other** (non-Network Attack Vector)
Externally exposed interface	7 days	14 days	30 days	90 days
Internally exposed interface	7 days	14 days	30 days	90 days/BAU

- 3rd Party uses patches obtained from: vendors directly for proprietary systems and patches that are either (i) digitally signed or (ii) verified via the use of a vendor hash (MD5 hashes must not be used) for the update package such that the patch can be identified as coming from a reputable support community for open-source software.
- 3rd Party tests all patches on systems that accurately represent the configuration of the target production systems before deployment of the patch to production systems and that the correct operation of the patched service is verified after any patching activity.
- Monitoring all applicable vendors and other relevant information sources for vulnerability alerts.
- If a system cannot be patched deploy appropriate countermeasures.
- 3rd Party will install critical security patches separately to feature releases to maximise the speed at which the patch can be deployed and will prioritise critical security patches over functionality upgrades wherever possible.

14.2 The 3rd Party must ensure that at least on an annual basis, an independent IT security assessment / penetration test approved by BT Security is commissioned on the 3rd Party IT

infrastructure and applications used to provide services, including Disaster Recovery sites to identify vulnerabilities that could be exploited to breach data / services and to prevent against any security breaches through Cyber Attacks. The 3rd Party must on reasonable request permit BT access to penetration test reports relevant to the services being provided.

14.3 The 3rd Party must ensure that access to diagnostic and management ports as well as diagnostic tools are securely controlled.

14.4 The 3rd Party must ensure that access to audit tools is restricted to relevant supplier personnel and their use is monitored.

14.5 The 3rd Party must ensure that any servers used to provide the service are not deployed on untrusted networks (networks outside the 3rd Party security perimeter, that are beyond its administrative control e.g., internet-facing) without appropriate security controls.

Asset Management

14.6 The 3rd Party must maintain an accurate and up-to-date information asset inventory of all technology assets with the potential to store or process information, so that only authorised devices are given access, and unauthorised and unmanaged devices are found and prevented from gaining access. This inventory shall include all hardware assets, whether connected to the organisation's network or not. If applicable, any BT equipment hosted in 3rd Party premises shall be included in the inventory.

14.7 The 3rd Party must ensure that the information asset inventory has the following components inventoried or catalogued:

- Physical devices and systems, software platforms and applications, external information systems.
- Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value.
- Organisational and Communication Data Flows including external / 3rd Party flows.
- Manual processes that handle BT or BT Customer data.

14.8 The 3rd Party must maintain an accurate and up-to-date software asset inventory for all software on the network so that only authorised software is installed and can execute, and that unauthorised and unmanaged software is found and prevented from installing or executing.

Cryptography

14.9 The 3rd Party must ensure that BT Information classified as Confidential or higher, is appropriately encrypted (in transit and at rest). All encryptions shall be accomplished with strong, modern cryptographic algorithms and ciphers employing robust integrity protection mechanisms and in accordance with industry standards for secure key and protocol negotiation and key management. For data in transit the following TLS options are not allowed: TLS v1.0, TLS v1.1 and SSL (any version). The following SSH (SFTP) options are not allowed: SSH v1. The following IPsec options are not allowed: IKE Version 1.

14.10 Cryptographic keys must meet or exceed the following minimum lengths:

- Symmetric keys (e.g., AES) must have a key length of at least 256 bits.

- Asymmetric keys (e.g., RSA) must have a key length of at least 3072 bits.
- Elliptic Curve keys must have a key length of at least 384 bits.

14.11 If NIST announces a crypto algorithm is no longer secure, it must not be used for new deployments. Existing deployments must review the continued use of deprecated crypto algorithms and deliver a migration plan to move away from deprecated crypto algorithms to a more secure alternative.

14.12 For symmetric encryption the following algorithms are not allowed; 3DES-168 (unless mandated by an international standard), 3DES-112, Blowfish, Twofish, RC4, IDEA, Camellia, Seed and ARIA.

14.13 Salted hashes must be used to protect data in storage i.e., passwords. Hashing may also be used to anonymise data before processing, for example MSISDNs or payment. The following hashing algorithms are not allowed MD2, MD4, MD5 and SHA-1.

System Configuration

14.14 The 3rd Party must have an established and consistent framework to ensure that systems are appropriately configured including the following components:

- Systems, network devices are configured to function in accordance with security principles (e.g., concept of least functionality and no unauthorised software).
- Ensuring that devices have the correct and consistent time.
- Systems are free from any malicious software.
- Appropriate checks and monitoring are in place to ensure the integrity of the builds / devices are maintained.

Malware protection

14.15 The 3rd Party must ensure that the most up to date malware protection is applied to all applicable IT assets to prevent service disruption or security breaches and ensure that appropriate user awareness procedures are implemented.

Anti-malware shall include detection for (but not limited to) ransomware, unauthorised mobile code, viruses, spyware, key logger software, botnets, worms, trojans etc.

Denial of Service Mitigations.

14.16 The 3rd Party must ensure that key systems are protected against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

15. 3rd Party Hosting BT Information

15.1 In addition to the controls in Section 14. 3rd Party Systems holding BT Information, where 3rd Party is hosting BT's Information in a datacentre or cloud solution the premises must hold a valid ISO/IEC 27001 certificate for security management (or certification(s) that demonstrate equivalent controls, supported by an independent auditor report).

16. Network Security – BT's own Network

Where 3rd Party will be installing equipment into, configuring, maintaining, managing, repairing, or monitoring BT's own network the following controls will apply:

16.1 Upon request, the 3rd Party shall provide BT with the names, addresses and such other details as BT shall reasonably require of all individual 3rd Party Personnel who:

- shall from time to time be directly involved in the deployment, maintenance and/or management of the Service(s) before they are respectively engaged.
- shall liaise with BT in relation to discussion around BT- and/or 3rd Party-identified vulnerabilities in the Service(s).

16.2 In relation to its UK-based support activities, the 3rd Party shall retain a skilled security team comprised of at least one UK national who shall be available for liaison with BT and the team shall attend such meetings as BT shall from time to time reasonably require.

16.3 The 3rd Party shall provide BT with a schedule (updated as necessary from time to time) of all active components comprised in the Service(s) and their respective sources.

16.4 The 3rd Party shall ensure that installation of new systems, equipment or software on BT's own network utilises the most recent software version and patch.

16.5 The 3rd Party shall ensure that all security-relevant logging is enabled on all network equipment installed by the 3rd Party and sent to the BT network logging systems.

16.6 The 3rd Party shall provide BT with timely (i.e., as soon as practicable to allow remediation before publicly publishing) information in relation to any vulnerabilities in the Service(s) and comply (at the 3rd Party's cost) with such reasonable requirements in relation to vulnerabilities as may be notified by BT.

16.7 The 3rd Party shall ensure that any security-related components comprised in the Service(s) as are identified by or to BT from time to time are, at the 3rd Party's cost, externally evaluated to BT's reasonable satisfaction.

16.8 The 3rd Party shall promptly, and in any event within 7 Working Days, provide to BT full details of any features and/or functionality in the Service(s) or that are planned in the Roadmap for the Service(s) that from time to time:

- the 3rd Party knows; or
- BT reasonably believes and so informs the 3rd Party are designed for, or could be used for, lawful interception or any other interception of telecommunication's traffic. Such details shall include all Information that is reasonably necessary to enable BT to fully understand the nature, composition, and extent of such features and/or functionality.

16.9 The 3rd Party must not use any network monitoring tools that can view application information.

16.10 The 3rd Party Personnel building, developing, and/or supporting BT's own network shall have as a minimum L2 pre-employment check. L3 pre-employment checks will be required for roles identified by BT.

16.11 3rd Party shall permit BT to install security software to BT's specification, on any 3rd Party virtual infrastructure (including but not limited to virtual machines and containers) or 3rd Party-installed operating system running on BT Networks.

16.12 3rd Party must ensure that the latest security patches are applied to systems/assets/Networks/applications ensuring that:

- 3rd Party deploys patches as soon as reasonably practicable and uses best endeavours to deploy within the following timescales following patch release:

	Actively exploited in the wild	**High EPSS** Vulnerability CVSS: > 8.0 (High + Critical) EPSS: >= 70% (Network Attack Vector – see definitions section)	**Lower EPSS** Vulnerability CVSS: > 8.0 (High + Critical) EPSS: < 70% (Network Attack Vector – see definitions section)	**Other** (non-Network Attack Vector)
Externally exposed interface	7 days	14 days	30 days	90 days
Internally exposed interface	7 days	14 days	30 days	90 days/BAU

- 3rd Party uses patches obtained from: vendors directly for proprietary systems and patches that are either (i) digitally signed or (ii) verified via the use of a vendor hash (MD5 hashes must not be used) for the update package such that the patch can be identified as coming from a reputable support community for open-source software.
- 3rd Party tests all patches on systems that accurately represent the configuration of the target production systems before deployment of the patch to production systems and that the correct operation of the patched service is verified after any patching activity.
- Monitoring all applicable vendors and other relevant information sources for vulnerability alerts.
- If a system cannot be patched deploy appropriate countermeasures.
- 3rd Party will deliver critical security patches separately to feature releases to maximise the speed at which the patch can be deployed and will prioritise critical security patches over functionality upgrades wherever possible.

Where the 3rd Party is supplying or making available goods, services or facilities for use in connection with an ICT Product or ICT Service (including a public electronic communications network or service), the following security controls apply.

16.13 Where 3rd Party is supporting more than one operator, controls must be implemented to prevent one operator or their network from adversely affecting any other operator or their network.

16.14 Where 3rd Party is operating as a 3rd Party Administrator for more than one operator, the following controls apply:

- Implement logical separation within the 3rd Party network to segregate customer data and networks.

- Implement separation between 3rd Party management environments used for different operator networks.
- Implement and enforce security enforcing functions at the boundary between the 3rd Party network and the operator network.
- Implement technical controls to limit the potential for users or systems to negatively impact more than one operator.
- Implement physically and logically independent Privileged Access Workstations per operator.
- Implement independent administrative domains and accounts per operator.

16.15 When providing network equipment 3rd Parties must provide BT with a 'security declaration' on how secure equipment is produced and how the equipment's security is ensured throughout its lifetime. This security declaration shall be approved at an appropriate level of seniority agreed with BT.

16.16 Where the 3rd Party is providing network equipment the following controls are applicable:

- 3rd Party warrants that it will adhere to a standard no lower than its published 'security declaration'.
- 3rd Party will supply up-to-date guidance on how the equipment should be securely deployed.
- 3rd Party will support all equipment and all software and hardware subcomponents for the length of the contract.
- 3rd Party will provide details for all major 3rd party components and dependencies, including but not restricted to, product and version, open-source components and level of support and period.
- 3rd Party will remediate all security issues that pose a security risk to BT's network or service discovered within their products within a reasonable time of being notified, providing regular updates on progress in the interim – such time to be agreed between BT and the 3rd Party both acting reasonably. This shall include all products impacted by the vulnerability, not only the product for which the vulnerability was reported.
- 3rd Party will either remove or change default passwords and default or hardcoded accounts or ensure that the network equipment is configured to enable BT to do so.
- 3rd Party will wherever possible disable unencrypted management protocols, and where not possible identify the presence of such protocols to BT to enable their use to be mitigated.

16.17 If 3rd Party has obtained internationally recognised security assessments or certifications for equipment (e.g., Common Criteria or NESAS), they shall share with BT the full findings that evidence this assessment or certificate.

16.18 Where 3rd Party's own network has potential to impact BT's UK Networks, the 3rd Party will, as advised by BT, undergo the same level of testing as BT applies to BT's UK Networks and will remediate identified vulnerabilities as agreed by both parties.

16.19 3rd Party authorises BT to share details of security issues as appropriate where necessary for the purposes of network security.

16.20 Infrastructure and Systems used to maintain BT's UK Networks must be located within the UK.

16.21 Where 3rd Party is performing BT's UK Network Oversight Functions, equipment used for this function shall be both located within the UK and operated using UK-based staff.

16.22 Where 3rd Party is responsible for network security and audit logs, these shall be stored within the UK and protected subject to UK law.

16.23 Where 3rd Party is operating as a 3rd Party Administrator, BT retains the right to determine permissions of the accounts used by the 3rd Party to access its network, and to require all logs relating to the security of the 3rd Party network to the extent that such logs relate to access into BT's network. The 3rd Party shall monitor and audit the activities of its staff when accessing BT's network.

17. 3rd Party Network Security

17.1 The 3rd Party must ensure that network integrity is established and maintained by ensuring the following components are appropriately controlled, and notifying BT in any instances where this is not technically possible:

- External connections to the network are documented, routed through a firewall and verified and approved prior to the connections being established to prevent data security breaches.
- The network is appropriately designed using "defence in depth" principles to ensure Cyber security breaches are minimised by ensuring appropriate controls that prevent any purposeful attack, such as "network segmentation", are in place.
- The design and implementation of the network is reviewed at least annually.
- All wireless access to the network is subject to authorisation, authentication, segmentation, and encryption protocols to prevent security breaches.
- Using secure communications between devices and management stations.
- Using secure communications between devices as appropriate; including the encryption of all non-console administrator access.
- Using strong architectural design, which are tiered and zoned with effective identity management and operating system configuration which must be appropriately hardened and documented.
- By the disabling (where practical) of services, applications and ports that will not be used.
- By the disabling or removal of guest accounts.
- By the avoidance of trust relationships between servers.
- Use of the best practice security principle of "least privilege" to perform a function.
- Ensuring appropriate measures are in place for intrusion detection and/or protection.
- Where appropriate, file integrity monitoring to detect any additions, modifications or deletions of critical system files or data.
- Change all default and vendor supplied passwords before network components go live.

- Disable unencrypted management protocols wherever technically possible.

17.2 The 3rd Party Network shall meet all legal and regulatory requirements, and:

- Use best endeavours to prevent unauthorised individuals (e.g., hackers) from gaining access to the 3rd Party Network(s).
- Use best endeavours to reduce the risk of misuse of the 3rd Party Network(s) by those individuals authorised to access it.
- Use best endeavours to detect any Security Breaches and ensure quick rectification of any breaches, alongside the identification of the individuals who obtained access and determination of how they obtained it.

17.3 Where the 3rd Party is supplying or making available goods, services or facilities for use in connection with an ICT Product or an ICT Service (including a public electronic communications network or service), the following additional security controls apply:

- Externally facing systems, excluding Customer Premises Equipment (CPE), are security tested every two years or when there is a significant change.
- Sensitive datasets and sensitive or critical functions are not hosted on equipment at the Exposed Edge of the network.
- If not cryptographically protected, physical and logical separation shall be implemented between the Exposed Edge and sensitive or critical functions.
- Security separation using security enforcing functions shall be implemented between the Exposed Edge and sensitive or critical functions.

18. Cloud Security

18.1 The 3rd Party must be certified to the latest version of ISO27017 or have an established and consistent framework to ensure that all use of Cloud technology and non-public data stored in the Cloud is approved and subject to appropriate controls equivalent to the latest version of the Cloud Security Alliance, Cloud Controls Matrix (CCM).

18.2 Network and infrastructure service level agreements (in-house or outsourced) shall clearly document shared responsibilities, security controls, capacity and service levels, and business or customer requirements.

18.3 3rd Party must implement security measures across all aspects of the service being supplied, such that it safeguards the confidentiality, availability, quality, and integrity by minimizing the opportunity of unauthorised individuals (e.g., other cloud customers) from gaining access to BT Information and the services utilised by BT.

18.4 To the extent 3rd Party provides hosted applications or services to BT, whether single-tenant or multi-tenant, including software-as-a-service, platform-as-a-service, infrastructure-as-a-service, and similar offerings, to collect, transmit, store, or otherwise process Confidential Data, 3rd Party shall provide BT the ability:

- to isolate such Confidential Data logically from the data of 3rd Party's other customers.
- to restrict, log, and monitor access to such Confidential Data at any time including access by 3rd Party Personnel

- to create, enable, disable, and delete the uppermost encryption key (known as Customer Managed Key) used to encrypt and decrypt subsequent keys including the lowermost data encryption key.
- to restrict, log, and monitor access to the Customer Managed Key at any time; and at no time shall any subsequent encryption key, an encryption key in a key hierarchy lower than the Customer Managed Key, be stored in the same system as Confidential Data unless encrypted by the Customer Managed Key, also known as being wrapped by the Customer Managed Key.

19. SIM Cards

19.1 Where the 3rd Party is providing SIM Cards, the following controls are applicable:

- For fixed-profile SIM cards, 3rd Party shall ensure that sensitive SIM data is appropriately protected by the SIM card manufacturer.
- For fixed-profile SIM cards, 3rd Party shall ensure that, the confidentiality integrity and availability of the sensitive SIM card data shared with the SIM card manufacturer is protected at every stage of their lifecycle.

20. Information classified as OFFICIAL or higher by HMG

20.1 The additional Security Requirements set out in Annex 1 to these Security Requirements will apply to each 3rd Party that will store, process or transmit information classified as OFFICIAL in line with His Majesty's Government Security Classifications Scheme as updated from time to time.

21. Defined Terms and Interpretation

21.1 Unless otherwise defined below, words and expressions used in these Security Requirements will have the same meaning as in the Contract:

"**Access**" and **"Accessed"** means the Processing, handling or storing BT Information by one or more of the following methods:

a. by interconnection with BT Systems;

b. provided in paper or non-electronic format;

c. BT Information on Supplier Systems; or

d. by mobile media

and/or Access to BT premises for the provision of the Supplies excluding the delivery of hardware and meeting attendance.

"**BT Information**" means all Information relating to BT or a BT Customer provided to the Supplier and all Information which is processed or handled by the Supplier on behalf BT or a BT Customer under the Contract.

"BT Stakeholder" means the BT representative who has ownership of the scope of work 3rd Party is undertaking.

"**BT Systems**" means the Services and Service components, products, networks, servers, processes, paper-based system or IT systems (in whole or part) owned and/or operated by BT or such other systems that may be hosted on BT premises.

"BT's UK Networks" means any Public Electronic Communications Network operated by BT, as defined by section 32 of the UK Communications Act 2003.

"BYOD" means bring your own device.

"**Contract**" means the Contract entered into by the Parties for the supply of goods, software or Services which references these Security Requirements.

"Customer Premises Equipment" means equipment provided to customers by the provider, and managed by the provider, that is used, or intended to be used, as part of the network or service. This excludes consumer electronic devices such as mobile phones and tablets, but does include devices such as edge firewalls, SD-WAN equipment, and fixed wireless access kit. **""**

"**Cyber Essentials Plus**" means UK Government backed scheme to help organisations protect themselves against common cyber-attacks.

"Cyber Security" means how individuals and organisations reduce the risk of cyber-attack. Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access - both online and at work - from theft or damage.

"**Escrow**" means the source code deposit agreement entered into in accordance with the Contract, to use, copy, maintain and modify such source code for the business purposes of BT (including the right to compile such source code).

"**Exposed Edge**" means Equipment that is either within customer premises, directly addressable from customer/user equipment, or is physically vulnerable. Physically vulnerable equipment includes equipment in road-side cabinets or attached to street furniture. The Exposed Edge includes CPEs, base station equipment, OLT equipment and MSAN/DSLAM equipment.

"**Good Industry Security Practice**" means in relation to any undertaking and any circumstances, the implementation of the security practices, policies, standards and tooling which would reasonably and ordinarily be expected from a skilled and experienced person engaged in the same type of activity under the same or similar circumstances.

"ICT product" means an element or a group of elements of a network or information system.

"ICT service" means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems.

"NDA" means a non-disclosure agreement is a binding contract between two or more parties that prevents sensitive information from being shared with others.

"NESAS" means the GSM Association's Network Equipment Security Assurance Scheme.

"Network Asset" means an item that is part of a collection of interconnected components such as computers, routers, hubs, cabling, and telecommunications controllers that make up a network.

"Network Attack Vector" means that the vulnerable component is bound to the network stack and the set of possible attackers extends beyond the other options listed below, up to and including the entire Internet. Such a vulnerability is often termed "remotely exploitable" and can be thought of as an attack being exploitable at the protocol level one or more network hops away (e.g., across one or more routers). An example of a network attack is an attacker causing a denial of service (DoS) by sending a specially crafted TCP packet across a wide area network (e.g., CVE 2004 0230).

"Network Oversight Function" means the components of BT's UK Network that oversee and control the security critical functions, which make them vitally important in overall network security. They are essential for BT to understand the network, secure the network, or to recover the network.

"**Network Security**" means the security of the interconnecting communication paths and nodes that logically connect end user technologies together and associated management systems.

"NIST" means The National Institute of Standards and Technology - a unit of the U.S. Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.

"**Official Sensitive Declaration**" means the written declaration to be provided by the Supplier relating to roles identified by the Supplier as having Access to information classified as "Official Sensitive" or having elevated privileges to infrastructure that stores, processes or transmits information classified as "Official Sensitive", a template of which is set out in Annex 1.

"Privileged Access Workstation (PAW)" means workstations through which Privileged Access is possible.

"Security Critical Function" means any function of BT's UK Network or the Service whose operation is likely to have a material impact on the proper operation of the entire network or service or a material part of it.

"**Security Requirements**" means this document as updated from time to time.

"SIM" means a unique hardware component or token, and associated software, used to authenticate the subscriber's access to the network. As used in this document, the SIM encompasses the hardware UICC/eUICC, the SIM/USIM/ISIM applications, eSIM and RSP functionality and any SIM applets.

"**Subcontractor**" means a Subcontractor of the Supplier which performs or is involved in the provision of the Supplies, or which employs or engages persons engaged in the provision of the Supplies.

"**Service**" means any and all of the "**Goods**", "**Software**" or "**Services**" as defined in the Contract.

"Transaction" means transactional data/ information that is captured from transactions i.e., data generated by various applications while running or supporting everyday business processes.

"Trusted Platform Module" means technology designed to provide hardware-based, security-related functions. A TPM chip is a secure crypto processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper-resistant, and malicious software is unable to tamper with the security functions of the TPM. The most common TPM functions are used for system integrity measurements and for key creation and use. During the boot process of a system, the boot code that is loaded (including firmware and the operating system components) can be measured and recorded in the TPM. The integrity measurements can be used as evidence for how a system started and to make sure that a TPM-based key was used only when the correct software was used to boot the system.

"3rd Party" means a Supplier to BT.

"3rd Party Administrator" means a managed service provider, provider of group functions, or external support for third party supplier equipment (e.g., third-line support function)

"**3rd Party Personnel**" means any persons engaged by the Supplier or its Subcontractors in the performance of the Supplier's obligations under the Contract.

"3rd Party Network" means any Supplier network.

"**3rd Party System**" means any Supplier owned computer, application or network systems used for accessing, storing or processing BT Information or involved in the provision of the Supplies.

Interpretation

21.2 Any words following the terms "including", "include", "in particular", "for example" or any similar expression will be construed as illustrative and will not limit the sense of the words, description, definition, phrase or term preceding those terms.

21.3 Any time a Party's right or obligation is expressed as one that they "**may**" exercise or perform, the option to exercise or perform that right or obligation will be in that Party's sole discretion.

21.4 Where any hyperlink ("**URL**") is referenced, such reference will be to such online resource Accessible via that URL, or such other replacement URL as notified to the applicable Party from time to time.

Version	Description	Author	Date
5.0	Telecommunications (Security) Act 2021 (TSA) Legislation and BT's adoption of CIS	Jemma Turner	25/10/22
5.1	Amendment to 14.9 TLS	Jemma Turner	17/04/23
5.2	Alterations to various clauses to incorporate TSA and vulnerabilities	Jemma Turner	30/11/23
5.3	Expansion for NIS2 purposes	Jemma Turner	06/05/25

ANNEX 1 – Additional Security Requirements

Where the 3rd Party is required to Access, store, process or transmit information classified as OFFICIAL or above, the 3rd Party will comply with the BT Security Requirements and additionally the requirements set out in this Annex 1. In all cases, the highest-level control will supersede requirements documented elsewhere in these Security Requirements.

1. EMPLOYEES

1.1 All 3rd Party Personnel employed having access to information classified as OFFICIAL or above or having elevated privileges to infrastructure that stores, processes or transmits information classified as OFFICIAL or above:

1.1.1 must be subject to pre-employment screening to Baseline Personnel Security Standard (BPSS) standard as a minimum;

1.1.2 must sign an Official Secrets Act declaration; and

1.1.3. must be prevented from accessing information or systems unless they have the required security clearances as specified in the relevant contract.

2. SECURITY TRAINING

2.1. The 3rd Party will mandate security training upon hire and at least annually for all employees having access to information classified as OFFICIAL or above or having elevated privileges to infrastructure that stores, processes or transmits information classified as OFFICIAL or above. This training shall cover the information handling requirements in line with the requirements of His Majesty's Government Security Classifications Scheme, as detailed in BT's Protecting HMG Information Guidance for 3rd Parties which shall be provided to the 3rd Party by BT.

2.2. The 3rd Party will update job descriptions for all employees having access to information classified as OFFICIAL or above or having elevated privileges to infrastructure that stores, processes or transmits information classified as OFFICIAL or above, to mandate participation in training described in paragraph 2.1 above. The 3rd Party will maintain a record of training which must be made available to BT upon request.

3. ACCESS CONTROL

3.1. When employees leave or move roles, their access rights must be revoked from relevant 3rd Party Systems within 1 Business Day.

3.2. Where the 3rd Party's employees, including contractors, temporary employees and agency workers, have elevated privileges to the BT infrastructure, the 3rd Party must notify BT in writing within 1 Business Day from when an employee no longer requires Access to BT Systems (e.g., employees leave or move roles).

3.3. Where the 3rd Party's employees, including contractors, temporary employees and agency workers, are issued with permanent Access cards to BT premises, the 3rd Party must notify BT in writing within 1 Business Day when an employee no longer requires Access to BT premises (e.g., employees leave or move roles).

4. VALUATION AND CLASSIFICATION OF ASSETS

4.1. The 3rd Party will implement additional information handling procedures to meet handling requirements in line with the requirements of His Majesty's Government Security Classification Scheme as updated from time to time.

5. INCIDENT RESPONSE AND REPORTING – SERVICE LEVEL AGREEMENTS

5.1. The 3rd Party will be advised on specific Service level agreements to support the incident response process. These may supersede any previous agreement outlined in these Security Requirements.

6. AUDIT, TESTING AND MONITORING

6.1. The 3rd Party will implement 24/7 security monitoring where specified by BT for the 3rd Party's infrastructure that supports the processing, storage or transmission of information classified as OFFICIAL or above.

7. BUSINESS CONTINUITY AND DISASTER RECOVERY

7.1. The 3rd Party will produce a business continuity and disaster recovery plan in accordance with BS ISO 22301 within 30 days of contract signature.

8. LOCATION

8.1. Unless specified otherwise by BT, the Service must be physically located within the physical boundaries of the UK or, if applicable, the EEA. Any remote support and/or management of the Service by the Supplier from an offshore location shall only be performed in accordance with the approvals process set out in the applicable contract between BT and the Government department concerned.

9. ADDITIONAL REQUIREMENTS FOR OFFICIAL-SENSITIVE OR ABOVE

9.1 All roles identified by the 3rd Party as having Access to information classified as OFFICIAL-SENSITIVE or above, or having elevated privileges to infrastructure that stores, processes or transmits information classified as OFFICIAL-SENSITIVE or above shall be documented in the OFFICIAL-SENSITIVE Declaration and provide BT with the completed OFFICIAL-SENSITIVE Declaration prior to Contract signature.

9.2 Where the Supplier is required to access, store, process or transmit information classified as HMG OFFICIAL-SENSITIVE or higher the Supplier to conduct a Personnel Security Risk Assessment on all roles identified in the OFFICIAL-SENSITIVE Declaration para 2 in line with the requirements set out in the document National Protective Security Authority (NPSA) Personnel Security Risk assessment - A guide (4th Edition - June 2013 or later).

ANNEX 1, EXHIBIT 1 – OFFICIAL SENSITIVE DECLARATION TEMPLATE

1. Systems/Services in Scope

Please list the systems and Services being provided in support of the HMG customer.

System	Service

2. 3rd Party roles requiring a security clearance level.

Role	Required Security Clearance Level
* e.g., DBA	SC

3. Vulnerability Management

System	Type of vulnerability Assessment	Frequency

4. Audit, Testing and Monitoring

Systems to be monitored 24/7 as advised by BT

ANNEX 2

Not used.

ANNEX 3, NIS 2 Implementing Regulation - Code of Practice to Contractual Security Requirements conversion

References below are to provisions of the Annex to the Commission Implementing Regulation laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures ("the NIS 2 Implementing Regulation")

Annex to the NIS 2 Implementing Regulation	Requirement	BT Security Requirement Clause
5.1.4	Based on the supply chain security policy and taking into account the results of the risk assessment carried out … the relevant entities shall ensure that their contracts with the suppliers and service providers specify, where appropriate through service level agreements, the following, where appropriate:	See below
5.1.4.a	cybersecurity requirements for the suppliers or service providers, including requirements as regards the security in acquisition of ICT services or ICT products set out in point 6.1. 6.1 requires: (a) security requirements to apply to the ICT services or ICT products to be acquired; (b) requirements regarding security updates throughout the entire lifetime of the ICT services or ICT products, or replacement after the end of the support period; (c) information describing the hardware and software components used in the ICT services or ICT products; (d) information describing the implemented cybersecurity functions of the ICT services or ICT products and the configuration required for their secure operation; (e) assurance that the ICT services or ICT products comply with the security requirements according to point (a); (f) appropriate methods for validating that the delivered ICT services or ICT products are compliant to the stated security requirements, as well as documentation of the results of the validation.	5, 16.15, 16.16
5.1.4.b	requirements regarding skills and training, and where appropriate certifications, required from the suppliers' or service providers' employees	4.6, 7
5.1.4.c	requirements regarding the verification of the background of the suppliers' and service providers' employees	16.10, Supplier Agreement and Policies Portal Selling to BT
5.1.4.d	an obligation on suppliers and service providers to notify, without undue delay, the relevant entities of incidents that present a risk to the security of the network and information systems of those entities	3.33

5.1.4.e	provisions on repair times	3.39, 14.1, 16.12
5.1.4.f	the right to audit or right to receive audit reports	5
5.1.4.g	an obligation on suppliers and service providers to handle vulnerabilities that present a risk to the security of the network and information systems of the relevant entities	14.1, 16.12
5.1.4.h	requirements regarding subcontracting and, where the relevant entities allow subcontracting, cybersecurity requirements for subcontractors in accordance with the cybersecurity requirements referred to in point (a)	3.4
5.1.4.i	obligations on the suppliers and service providers at the termination of the contract, such as retrieval and disposal of the information obtained by the suppliers and service providers in the exercise of their tasks	3.23, 3.24

ANNEX 2: SANTANDER CYBERSECURITY CLAUSE

The Supplier shall (and ensure that any Subcontractor and Contract Personnel shall) comply with this cybersecurity clause so long as it sells BT services and goods to be delivered to the Santander Group.

Any breach of this Condition by the Supplier shall be deemed to be a material breach of the Contract.

This Condition shall survive the Contract.

CYBERSECURITY CLAUSE

DEFINITIONS

For the purposes of this clause only, the following defined terms shall have the following meaning and all other defined terms in this Clause shall have the meaning given in the Agreement:

"Client's Information"	shall mean information provided by or on behalf of the Client, pursuant to the Agreement for the provision of the Services and/or development of the Project, including (without limitation) Confidential Information;
"ICT-related incident"	a single event or a series of linked events that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of information, or on the services provided by the financial entity.
"FIPS"	shall mean the Federal Information Processing Standard which specifies the security requirements that shall be satisfied by a cryptographic module;
"Identity and Access Management System"	shall mean the system which addresses an organizational need for a system-wide solution that manages user's access and authentication into external and internal applications, databases, or networks;
"Information and Communication Technology Risk"	means any reasonably identifiable circumstance in relation to the use of Network and Information Systems, - including a malfunction, capacity overrun, failure, disruption, impairment, misuse, loss or other type of malicious or non-malicious event - which, if materialised, may compromise the security of the Network and Information Systems, of any technology-dependant tool or process, of the operation and process' running, or of the provision of services, thereby compromising the integrity or availability of data, software or any other component of ICT services and infrastructures, or causing a breach of confidentiality, a damage to physical ICT infrastructure or other adverse effects;
"Information Asset"	means a collection of information, either tangible or intangible, that is worth protecting;
"Information Security Management System"	shall mean the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its Information Assets and its Network and Information Systems. It is a systematic approach to managing information so that it remains secure, by applying a risk management process, as defined by ISO/IEC 27001;

“Network and Information System’’	shall mean (a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC; (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;
“NIST”	shall mean the National Institute of Standards and Technology;
“Minimum Required Privilege”	shall mean the principle of least privilege which states that users and programs should only have the necessary privileges to complete their tasks;
“OWASP”	shall mean the Open Web Application Security Project;
“PCI—DSS”	shall mean the Payment Card Industry Data Security Standard approved by the PCI Security Standards Council and currently in effect;
“Penetration Testing”	shall mean a specialized type of assessment conducted on Information Systems or individual system components that attempts to simulate the actions of adversaries in carrying out hostile cyber-attacks to specific assets, with the aim of providing an in-depth analysis of the vulnerabilities of the asset which could be exploited by the attacker;
“Red Team”	shall mean a not-informed targeted exercise in order to emulate a potential adversary’s attack or exploitation capabilities with respect to a group of assets for the determination of the capabilities of an attacker overcoming the perimeter defences and compromising internal systems;
“Segregation of Duties”	refers to the principle that no user should be given enough privileges to misuse the system on their own;
“SOC 2 Type 2”	shall mean the report on management’s description of a service organization’s system and the suitability of the design and operating effectiveness of controls;
"Threat Led Penetration Testing".	framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the entity’s critical live production systems.”

"Vulnerability"	means a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited by a threat;
"Vulnerability Scanning"	shall mean a technique used to test systems for the occurrence of vulnerabilities published on public repositories which allows testing the security through automated techniques in a network through the analysis of open ports and running services with respect to one individual system component or network;

CYBERSECURITY MEASURES

The Provider shall develop, implement and maintain an Information Security Management System and distribute within its organization a set of procedures and policies that meet, as a minimum, the following requirements:

1. General

1.1. Provider shall ensure that an effective Information Security Management System is implemented, consistent with the applicable law and the highest international security standards such as ISO/IEC 27001 and NIST Cybersecurity Framework or any other that could be applicable. As part of the Information Security Management System, Provider shall implement a Network and Information Systems security policy, taking into account the principles of integral security, Information and Communication Technology Risk management, prevention, response and recovery, lines of defense, periodic reassessment and Segregation of Duties. The Information Security Management System shall include as a minimum: Information and Communication Technology Risk analysis and management, third party and Provider Information and Communication Technology Risk management, catalogue of measures (security, organizational, technological and physical), personnel management and professionalism, procurement of security products or services, incident detection and management, recovery plans and business continuity assurance, continuous improvement, interconnection of Network and Information Systems and a log of user activity.

Provider must reflect and specify all applicable regulations, industry standards (including but not limited to PCI—DSS) and legal requirements in the Information Security Management System.
Provider shall thoroughly review all these aspects periodically, but not less often than once a year as well as upon the occurrence of major ICT-related incidents or conclusions derived from relevant testing or audit processes. Provider agrees to remedy any discovered deficiencies promptly and continuously improve its Information Security Management Systems

1.2. Provider shall inform Client of any changes to its Information Security Management System and/or Network and Information System, including but not limited, to systems, security measures, processes or procedures that may affect, reduce or limit the level of security or the rights and obligations of this Clause, and shall provide Client an executive report analyzing the information security implications of said change, at least within thirty (30) days prior to the effective implementation of such change. The Client will be allowed to terminate this Agreement automatically without incurring in any penalty or cost (except for the payment of outstanding fees for Services already performed) if Client determines that the change could alter the effectiveness of the security measures agreed under this Clause or could represent an Information and/or Communication Technology Risk for Client's Information Assets and Network and Information Systems.

1.3. The Provider shall appoint the following person as an information security liaison to work with Client's Cybersecurity team to review and coordinate all matters, concerns or questions raised in connection with Client's Information and Cybersecurity requirements, standards and practices:

Mr/Ms ----------
C/ ----------
e-mail; ----------
Telephone: ----------

1.4. The Provider must notify the Client promptly :

a. Should there be any changes to the details stated above or in relation other security matters that are not related to cybersecurity incidents: *cybergrc.risk.continuity@gruposantander.com*
b. Any notification regarding cybersecurity incident should be notified to the following email address: *cybersecurityincidents@gruposantander.com.*

1.5. Provider shall at no additional cost provide full cooperation and assistance to the Client to allow the latter to comply with its regulatory obligations, including in relation to data security; audit, any potential Cybersecurity Incident notification, any enquiry or complaint received from an authority related to Client's Information or any request, notice or investigation by an authority.

1.6. In no case the implementation of the Cybersecurity measures established in this Clause may constitute a justification for the decrease of the levels established in the agreed service level agreements (SLA) by the Provider.

1.7. The Provider shall (if not already contracted) contract an insurance policy with cybersecurity coverage for the damages caused by a Cybersecurity Incident to Client's Information, Client's Network and Information Systems or third parties.

1.8. For the avoidance of doubt, when/where there is a conflict and/or inconsistency between the measures of this Cybersecurity Clause and measures contained elsewhere within the Agreement (including, in particular, the ones applicable to Personal Data or subcontracting), the provisions that impose more stringent obligations shall prevail.

2. <u>Identity management and access control</u>

2.1. Provider shall implement and document appropriate identity management and access control policies, procedures, and mechanisms for authorized users to ensure the confidentiality, integrity, and availability of unique identification and authentication of users and systems accessing (including for remote and emergency access) the Client's Information and Network and Information Systems, to enable assignment of user access rights, in accordance with the below. To that end, the Provider must identify, authenticate, and authorize the user's responsibilities for access to the Client's Information and Network and Information Systems, as well as to identify and implement key controls to these effects, including controls and tools to prevent unauthorized access, maintenance of records of all identity assignments and a lifecycle management process. The Provider shall ensure that access rights are provided on a "Minimum Required Privilege" and "Segregation of Duties" basis. Compliance with these policies and procedures should be subject to continuous monitoring and periodic reviews at least annually.

2.2. As a minimum, Provider shall implement appropriate controls to ensure the following:

a. All Networks and Information Systemsmust be integrated with an Identity and Access Management System.
b. Assignment of a unique identity, corresponding to a unique access account to each staff member with access to the Network and Information Systems and the implementation (avoiding generic accounts not assigned to a list of specific users) of controls and tools on access restrictions to Network and Information Systems to prevent unauthorized access.
c. For the performance of administrative tasks on the Network and Information systems, dedicated accounts shall be used.

d. Access rights must be provided, withdrawn or modified when appropriate and in accordance with the previously established approval flows. Provider shall implement the appropriate procedures in order to process the access rights of new incorporations, internal movements and withdrawals.
e. Periodic access rights should be certified and reviewed to ensure that users maintain the strictly necessary rights, at least every six months.

2.3. Provider may only implement different minimum identity management and access control requirements when expressly agreed by the Parties.

2.4. In addition to the security measures described under this Cybersecurity clause, where the Provider stores and/or manages Client's Information and/or Network and Information Systems, the Provider must implement and enforce, for every access by the Client, MFA and any other access and configuration controls that may be requested by the Client.

3. Segregation of information and storage

3.1. Provider shall implement and maintain appropriate security measures and procedures to ensure that Client's Information can be processed separately, including, but not limited to the following: (a) no production data shall be used for development testing without the explicit prior consent of Client, which reserves the right to request additional controls in such cases; (b) the development of new application or system software shall be kept separate from the production environment; (c) Client's Information shall be kept separate from the information of other clients and Provider's own information.

3.2. The Provider shall ensure the logical isolation of the storage of Client information from that of other Clients, as well as the deployment of all necessary technical measures to ensure the segregation of Client information.

4. Security development life cycle

4.1. In the event that the Project or Service implies software development, Provider shall ensure that software developed by the Provider which either forms part of the Service or Project, or could provide access to Client's Information and/or Network and Information Systems is developed using secure coding practices such as OWASP or equivalent. Such software will undergo security testing during the development process to identify vulnerabilities. Any identified vulnerabilities shall be remediated prior to deployment. The Provider shall have an independent third party audit or a certification (SOC 2 Type 2 or equivalent) that covers the software development procedure and Vulnerability management, guarantying that the product or service has no critical Vulnerability. The Provider shall deliver to the Client a copy of the report or the certification.

4.2. The Provider shall monitor the use of any licensed third-party libraries (including open source) and the existence of any versions or updates, keeping the Client informed at all times. In case of off-the-shelf assets or components acquired and used in the operation of the Services, the Provider shall also track the usage of third-party libraries, including open-source ones, keeping the Client informed at all times

5. Information transfer & Data Loss Prevention

5.1. Provider shall ensure that electronic transfers of Client's Information over public / non-secure network are undertaken securely using appropriate industry standard encryption methods such as FIPS or NIST. The Provider shall have appropriate technical controls to prevent unauthorized transfer of Client's Information to portable computing devices.

5.2. In the event that the Provider uses its own PCs, work stations or any other technological device for the provision of the service, the Provider shall have in place effective data loss prevention (DLP) measures, policies and procedures designed to prevent the unauthorized transfer of Client's Information. These measures must include, as minimum:

a) DLP in e-mail to block sending of Client's Information outside the organization.
b) DLP to prevent browsing on potentially harmful pages, or pages that facilitate data theft (filesharing) or other unauthorized data repositories.
c) DLP on PCs that disables writing accesses to removable disks.

5.3. In addition, if the service is based on a Provider's system/application, access to such system/application shall be restricted so that access by its employees is exclusively done from corporate managed devices that implement, as a minimum, the measures agreed in this clause. Where remote access to systems is required, connections implementing information encryption (e.g. via VPN or encrypted communication protocols), as well as security measures similar to those existing in the case of access via corporate PCs, shall always be used.

6. Antimalware

6.1. Provider shall implement antivirus and/or antimalware protection in its Networks and Information Systems by implementing the version in force at any time, which will be updated periodically in accordance with the manufacturer's recommendations.

7. Vulnerability identification and testing

7.1. Provider shall perform the following exercises and will deliver the reports to the Client, including confirmation that the Vulnerabilities have been corrected or, where appropriate, that there is a plan to correct them:

- Vulnerability Scanning at least on a weekly basis on live production systems.
- Penetration Tests and Red Team exercises on internet facing assets in connection with the Service or Project on live production systems, through a duly-qualified independent expert at least on an annual basis, and additionally whenever there are relevant changes in the Network and Information Systems infrastructure, processes, procedures, as well as when the changes made are due to security incidents, or due to significant changes of critical applications that are exposed to the internet on live production systems.
- Advanced testing at least every three (3) years, or as requested by the Client's competent authority, through Threat Led Penetration Testing through a duly qualified independent expert.

7.2. The Provider shall notify immediately and any event, within 24 hours, of any critical[1] Vulnerability with available patch or publicly available exploits on live production systems.

7.3. In addition, Client through a qualified third party appointed by the Client and agreed with the Provider (which consent shall not be unreasonably withheld), shall have the right to conduct Vulnerability Scanning, Penetration Tests and Red Team exercises on Provider's internet facing assets and/or Network and Information Systems solely in respect of the Client's or the Provider's dedicated products and services. In this sense, the Client through designated qualified third party by it will notify the Provider with reasonable advance notice of the performance of these activities, and shall establish in coordination with the Provider the action schedules, so that these exercises have the least possible impact on the Provider's activities. Due to the agreed planning between the Parties and Provider's control over the exercise, neither the Client nor its designated qualified third party will

[1] Criticality based on a CVSS Score > 7.

assume any responsibility or liability for the damages that the Provider may suffer derived from the performance of these activities.

7.4. Provider is responsible for the Vulnerability correction plans of all the assets under its responsibility, taking into account the criticality and exposure in accordance with the following requirements:

- Vulnerability correction must be done either directly by solving the Vulnerability, or by developing or applying adequate controls to mitigate the Information and Communication Technology Risk.
- High and Critical vulnerabilities shall be corrected within a maximum period of thirty (30 days), and Medium ones shall be corrected within a maximum period of ninety (90) days[2].

7.5. Provider shall implement and maintain appropriate security measures and procedures in order to ensure the regular update and patching of all computer hardware and software including testing prior to installation in production environments to eliminate vulnerabilities and remove flaws that could otherwise facilitate Cybersecurity Incidents. New security patches releases must be checked weekly.

7.6. Additionally, Provider must ensure that all technological assets (software and hardware) associated to the Service or Project have a contract in force with the manufacturer or, failing that, an extended support contract that includes the publication of the necessary security patches. In case this was not possible, the Provider shall ensure the migration of the asset before the end date of the software or the vulnerabilities support.

8. Subcontractors and third parties

8.1. Provided that a Subcontractor is authorized by the Client for the Service or Project under the Agreement, Provider shall: (a) identify the security measures of the Subcontractor and a description of the intended processing to be carried out by the Subcontractor, in order to enable the Client to evaluate any potential Information and Communication Technology Risk; and (b) impose legally binding contract terms on the Subcontractor which replicate to those contained in this Contract.

8.2. Provider shall routinely assess its subcontractors and any other third party appointed by it using audits, test results, or other forms of evaluations to validate and ensure that such third parties have the capability to meet the security requirements under this Clause. Audits, test results, or any other forms of evaluations undertaken by the Provider with respect to its Subcontractors shall be provided to the Client on an annual basis. Notwithstanding the foregoing, the Client reserves the right to request these results at any time for the fulfillment of its Cybersecurity legal, regulatory and contractual obligations. These rights shall be extended to any competent and/or resolution authorities.

8.3. Provider acknowledges and agrees that it shall remain liable to the Client for a breach of the terms of this Clause by a Subcontractor and any other third party appointed by it and will be fully liable vis-à-vis the Client for the effective performance of the corresponding obligations of any sub-contractor involved in the provision of the Services, whether designated directly by the Provider or indirectly through a subcontracting chain.

9. Incident management and reporting

9.1. Provider shall develop, document and implement an incident management process, which shall encompass the identification, qualification, quantification, classification and escalation of Cybersecurity Incidents, as well as their management, reporting and resolution. Said Cybersecurity Incident management process must be aligned with the applicable regulations and submitted to the Client for its evaluation. Provider shall thoroughly test all

[2] According to the CVSS (Common Vulnerability Scoring System).

aspects of the Cybersecurity Incident management process periodically, but not less often than once every twelve (12) months. Provider agrees to remedy any deficiencies in the Cybersecurity Incident management process discovered by such tests promptly.

9.2. Provider shall notify the Client immediately and in any event no later than four (4) hours after becoming aware of any Cybersecurity Incident. The obligation to notify shall extend to any circumstance giving rise to suspicion of the existence of an incident, not being necessary for the incident to have materialized or for there to have been an actual adverse effect. The notification shall be sent to the following e-mail address cybersecurityincidents@gruposantander.com.

9.3. At no additional cost, the Provider shall provide the Client, in the most expedient time possible, with including but not limited to (i) a detailed description of categories of ICT-related incident and its impact on the Provider; date and time of detection; information on the origin; Client's Information, and/or Network and Information Systems affected); information on whether the incident is recurrent or related to a previous one; an indication of whether there has been an impact or potential impact on other financial institutions and third-party providers, (ii) the mitigating measures implemented to revert the situation, and (iii) copy of all internal and forensic reports including, without limitation, preliminary forensic reports, audit reports or reports of any other nature that are produced which must contain, as a minimum, an inventory of indicators of compromise and confirmed facts, as well as logs and any other information and cooperation which the Client may reasonably request relating to the Incident ICT-related incident. If there are malicious artifacts that allow profiling the threat (evidence, samples, scripts, etc.), these shall be shared with the Client. The Provider will take the measures to investigate the Incident ICT-related incident immediately and identify, prevent and mitigate its effects, keeping the Client informed at all times. At the reasonable discretion of the Client, the Provider shall grant the Client with access to its premises. In addition, the Provider shall provide a report issued by an independent third party that describes the measures adopted for the resolution and mitigation of the relevant Incident ICT-related incident, confirms their implementation, and that the incident has been resolved and does not pose a risk to Client's Information and/or its Network and Information Systems.

9.4. Provider will notify the Client, in a completely anonymized form, of any relevant or critical Cybersecurity Incident where the Provider is directly involved affecting an entity of similar characteristics of the Client.

9.5. Provider may not make available to any third party any communication or press release concerning a Cybersecurity Incident that affects the Client without the its written approval unless legally required.

9.6. The Client will communicate cybersecurity incidents to the competent authorities (initial, intermediate and final notifications), as well as, where applicable, to the natural persons affected in accordance with the applicable regulations. Notwithstanding the foregoing, the Provider shall cooperate with the Client in the creation and management of such notifications. In this regard, both parties will manage the Cybersecurity Incident in a coordinated manner when a third party notification is required.

10. Confidentiality, recruiting and training

10.1. Provider shall ensure that all employees and contractors having access to Client's Information and/or Network and Information Systems: (i) are under an obligation of confidentiality no less stringent than the confidentially obligations imposed on the Provider under the Agreement; (ii) are adequately qualified and kept up-to-date in all relevant security obligations, maintain the relevant technical skills, and receive Cybersecurity training as a minimum on an annual basis; and (iii) are subject to background checks in accordance with relevant regulations and (iv) the Provider shall ensure that all employees, including contractors and temporary staff, receive appropriate awareness training on relevant policies and procedures, as well as on the latest threats that may

affect their job function.

11. Information deletion

11.1. Always in accordance with the Agreement's data protection and business continuity plan provisions, Provider shall ensure that any information held, whether original, reproduced or derived from Client's Information regardless of media shall be physically destroyed when no longer needed in any event no later than thirty (30) days after termination of the applicable services or seven (7) days of Client's request, in accordance with NIST hard drive destruction SP 800-88[3] or equivalent international standard. Records and certificates of destruction must be retained and made available to Client.

12. Detection and monitoring

12.1. Provider shall establish and implement policies and procedures to detect anomalous activities that may affect information security and respond to Cybersecurity events appropriately. As part of this continuous monitoring, the Provider must implement appropriate and effective capabilities to detect intrusions, as well as events that affect the confidentiality, integrity and availability of Client's Information and/or Information Asset that support it. Provider shall maintain sufficient solutions to detect and monitor events with respect to the activity of the user or system.

12.2. All Information Assets and Network and Information Systems that manage or process Client's Information must record all actual or attempted log-on attempts as well as access violations to the Confidential Information and systems containing the Confidential Information, including additions, deletions, alterations and copying of the Confidential Information for at least five (5) years without prejudice to the minimum retention periods established by applicable regulations, and shall provide reports, to the Client upon prior request.

12.3. The activities of services and users that affect Client's Information may be monitored by the Client Operations Security Center (SOC). For this purpose, at the request of the Client, Provider shall make available to the Client the security logs of the applications where Client's Information is processed.

13. Network and Information Systems protection and segmentation

13.1. The Provider shall implement, as a minimum, the following measures to protect the Network and Information Systems:

a) Network segmentation to isolate parts that share equivalent levels of importance and establish traffic control mechanisms to restrict transfer between segments; communication between areas with different critical levels should be segmented (e.g., by means of firewalls).

b) Separate and dedicated network for the administration of ICT assets.

c) Identification and implementation of network access controls to prevent and detect connections to the network by any unauthorized device or system, or any endpoint not meeting the security requirements contained herein.

d) Design of networks in accordance with security requirements and taking into account leading practices to ensure confidentiality, integrity, and availability of the network.

[3] NIST Special Publication 800-88 Guidelines for Media Sanitization

e) Securing of network traffic between internal networks and the internet and other external connections.

f) Identification of roles, responsibilities, and steps for the definition, implementation, approval, change, and review of firewall rules and connection filters. The Provider shall verify the adequacy of existing firewall rules and connection filters at least every six months.

g) Performance of reviews of the network architecture and of the network security design at least once a year to identify potential vulnerabilities. Implementation of secure configuration baseline of all network components and hardening of the network and network devices.

h) Procedures to limit, lock, and terminate system and remote sessions after a predefined period of inactivity. i) Measures to temporarily isolate, where necessary, subnetworks and network components and devices .

13.2. Provider will have secure web browsing and e-mail; as well as network access controls (NAC). Where the Service or Project is connected to the Internet, Provider must use resilient architectures to withstand denial-of-service attacks.

14. Information and Communication Technology Risk assessments

14.1. Provider shall perform no less frequently than annually, and additionally whenever there are relevant changes in the Network and Information Systems infrastructure, Information and Communication Technology Risk analysis and impact assessments in order to: (a) identify reasonably foreseeable threats that could result in unauthorized processing of Client's Information ; (b) assess the likelihood of these threats occurring, and the potential damage that might result, taking into consideration the nature and classification of Client's Information, with particular regard to Confidential Information; and (c) assess the sufficiency of the security measures, policies and procedures in order to protect Client's Information and the Network and Information Systems.

14.2. Risk assessments and treatment plans must consider the implications of Cybersecurity, and applicable industry standards and legal requirements. The Provider shall implement appropriate controls to manage the identified risks, and shall provide Client with evidence of the performance of the risk analysis and impact assessments and treatment plans.

15. Encryption

15.1. The Provider must ensure that Client Information (where in electronic form) is appropriately encrypted on any Network and Information System by implementing controls including, as a minimum, the following elements:

a) rules for the encryption of data at rest and in transit;
b) rules for the encryption of data in use. Where encryption of data in use is not possible, the Provider shall process data in use in a separate and protected environment or take equivalent measures that ensure the confidentiality, integrity, authenticity and availability of data;
c) rules for the encryption of internal network connections and traffic with external parties;
d) provisions for cryptographic key management establishing the correct use, protection and lifecycle of cryptographic keys
e) use cryptographic algorithms that have not been declared vulnerable or obsolete by international security standards such as FIPS or NIST.

15.2. Provider must allow encryption keys management via the Client infrastructure (BYOK Bring Your Own Key), so that the Client has absolute control over the encryption keys. If management is delegated to the Provider, the Provider

must use elements designed for the purpose such as Hardware Security Modules (HSMs) or any other mechanism providing similar safeguards.

16. Information Asset management & data flow diagram

16.1. Provider must maintain (a) an updated register of the IT resources used to provide the Services (hardware, software, and network), managed consistent with their relative importance to business objectives and the organization's risk strategy; and (b) a data flow diagram including Client's Information. Both the register of IT resources and the data flow diagram might be requested by the Client from time to time.

17. Certifications

17.1. The Provider shall deliver a copy of the certifications available and in force at any time. As a minimum, those certifications which have been presented or alleged before the Client during the certification process shall be in force during the term of its associated Service. In addition, if under the Client's consideration from a risk management perspective, it is required, the Client reserves the right to request the extension of the scope of certification to cover the services

18. Most Favourable Nation

18.1. Provider represents and warrants that all of the cybersecurity measures granted hereunder are equivalent to or better than the terms being offered by Provider to any of its existing customers for similar services. Should Provider enter into an agreement with another client providing such client with more favorable terms, Provider shall inform Client as soon as possible and shall enter into a written agreement to provide such terms to the Client.

19. Subsistence of the remaining stipulations

19.1. Except as provided herein, this Annex does not cancel or modify the remaining terms of the Contract or the Annexes thereto, which shall remain in full force and effect and shall simply be modified by this Annex in accordance with the provisions of this Annex. In the event of contradiction between the terms of this Annex and those of the Contract, the provisions of this Annex shall prevail.

19.2. And, in witness whereof, the Parties have signed the present document, in duplicate, one copy of which shall remain in the possession of each party and for a single purpose, at the place and on the date indicated in the heading.