BT Security Ethical Hacking
Schedule to the General Terms

Contents

A note on 'you'

'You' and 'your' mean the Customer.

Words defined in the General Terms

Words that are capitalised but have not been defined in this Schedule have the meanings given to them in the General Terms.

Part A – The BT Security Ethical Hacking Service

1   Service Summary

BT will provide you with an ethical hacking service that will assess the vulnerability of your applications, network, people, procedures and policies comprising:

1.1   the Standard Service Components; and

1.2   any of the Service Options as set out in any applicable SoW,

up to the point of the Service Management Boundary as set out in Paragraph 4 ("**BT Security Ethical Hacking Service**").

2   Standard Service Components

BT will provide you with all the following standard service components ("**Standard Service Components**") in accordance with the details as set out in any applicable SoW:

2.1   **Vulnerabilities Testing**: BT will conduct a testing for Vulnerabilities.

2.2   **Testing Plan**: BT will provide a plan for carrying out the testing that BT will conduct.

2.3   Status Reports: BT will provide you with regular status reports containing any critical and high risk Vulnerabilities identified during the assessment and any steps that may be required to remediate the Vulnerabilities.

2.4   **Preliminary Report**: BT will provide you with a Preliminary Report on the date that BT completes the testing activities or as soon reasonably practicable after the date that BT completes the testing activities.

2.5   **Final Report**: BT will provide you with a Final Report that will contain all the Vulnerabilities that BT identified during the testing within 10 Business Days after the date we complete the testing.

3   Service Options

3.1   BT will provide you with any of the following options ("**Service Options**") as set out in any applicable SoW and in accordance with the details as set out in that SoW:

    3.1.1   Web Application Vulnerability Assessment;

    3.1.2   Network Vulnerability Assessment;

    3.1.3   Host Configuration Review;

    3.1.4   Mobile Application Vulnerability Assessment;

    3.1.5   Wireless Vulnerability Assessment;

    3.1.6   Source Code Review;

    3.1.7   Penetration Testing;

    3.1.8   Retesting;

    3.1.9   Firewall Policy Review;

    3.1.10   Social Engineering;

    3.1.11   Vehicle Vulnerability Assessment;

    3.1.12   Denial of Service Vulnerability Assessment;

    3.1.13   Assume Breach;

    3.1.14   Red Teaming;

    3.1.15   OSINT Assessment; and

    3.1.16   Hardware Vulnerability Assessment.

3.2   Service Options may not be available in all countries.

4   Service Management Boundary

4.1 BT will provide the BT Security Ethical Hacking Service in accordance with Part B of this Schedule and as set out in any applicable SoW, performing the BT Security Ethical Hacking Service either on your premises or remotely ("**Service Management Boundary**").

4.2 BT will have no responsibility for the BT Security Ethical Hacking Service outside the Service Management Boundary.

4.3 BT does not make any representations, whether express or implied, about whether the BT Security Ethical Hacking Service will operate in combination with any Customer Equipment or other equipment and software.

5 Associated Services and Third Parties

5.1 If BT provides you with any services other than the BT Security Ethical Hacking Service, this Schedule will not apply to those services and those services will be governed by their separate terms.

6 Specific Terms

6.1 **Amendments to the General Terms**

6.1.1 Clauses 3.2 and 3.3 of the General Terms are deleted.

6.1.2 The definition of Effective Date given in the General Terms is deleted and replaced with the following:

"**Effective Date**" means the date BT accepts your Order or SoW either expressly in writing or, in the absence of express acceptance, impliedly by BT's provision of the Service including the making of a commitment on any third party supplier by BT in anticipation of providing the Service.

6.2 **Termination for Convenience**

For the purposes of Clause 17 of the General Terms, either of us may, at any time after the Service Start Date and without cause, terminate the BT Security Ethical Hacking Service or any applicable SoW by giving 10 Business Days' Notice to the other.

6.3 **Customer Committed Date**

6.3.1 If you request a change to the BT Security Ethical Hacking Service or any part of the BT Security Ethical Hacking Service, then BT may revise the Customer Committed Date to accommodate that change.

6.3.2 BT may expedite delivery of the BT Security Ethical Hacking Service for operational reasons or in response to a request from you, but this will not revise the Customer Committed Date.

6.3.3 If BT discovers a Virus in your software, system, network, data or Application, BT may revise the Customer Committed Date.

6.4 **Invoicing**

6.4.1 Unless set out otherwise in any applicable SoW, BT will invoice you for the following Charges in the amounts set out in any applicable SoW:

(a) Professional Services Charges; and

(b) any Termination Charges incurred in accordance with Paragraph 6.5 upon termination of the relevant Service.

6.4.2 BT may invoice you for any of the following Charges in addition to those set out in any applicable SoW:

(a) Charges for commissioning the BT Security Ethical Hacking Service in accordance with Paragraph 7.2 outside of Business Hours;

(b) Charges for expediting provision of the BT Security Ethical Hacking Service at your request after BT has informed you of the Customer Committed Date;

(c) Charges for Abortive Visits; and

(d) any other Charges as set out in any applicable SoW or the BT Price List or as otherwise agreed between both of us.

6.5 **Cancellation and Termination Charges**

6.5.1 **Cancellation Charges**

For the purposes of Clause 16 of the General Terms, if you cancel a SoW, or part of it, any time before the Service Start Date you will pay BT the Cancellation Charges as set out below:

(a) any costs reasonably incurred by BT in preparing to deliver the BT Security Ethical Hacking Service; and

(b) any charges reasonably incurred by BT from a supplier as a result of your cancellation of the BT Security Ethical Hacking Service.

6.5.2 **Termination Charges**

If you terminate the Contract or the BT Security Ethical Hacking Service for convenience in accordance with Clause 17 of the General Terms you will pay BT:

(a)   all outstanding Charges for Services rendered;

(b)   any additional amounts due under the Contract;

(c)   any other Charges as set out in any applicable SoW; and

(d)   any charges reasonably incurred by BT from a supplier as a result of the early termination.

6.5.3   BT will refund to you any money you have paid in advance after deducting any Charges or other payments due to BT under the Contract.

6.6   **Service Amendment**

6.6.1   You may request, by giving BT Notice, a change to:

(a)   an SoW for the BT Security Ethical Hacking Service (or part of an SoW) at any time before the applicable Service Start Date; or

(b)   the BT Security Ethical Hacking Service at any time after the Service Start Date.

6.6.2   If you request a change in accordance with Paragraph 6.6.1, except where a change results from BT's failure to comply with its obligations under the Contract, BT will, within a reasonable time, provide you with a written estimate, including:

(a)   the likely time required to deliver the changed BT Security Ethical Hacking Service; and

(b)   any changes to the Charges due to the changed BT Security Ethical Hacking Service.

6.6.3   BT has no obligation to proceed with any change that you request in accordance with Paragraph 6.6.1, unless and until the necessary changes to the Charges, implementation timetable and any other relevant terms of the Contract to take account of the change are agreed between both of us in writing.

6.6.4   If BT changes a BT Security Ethical Hacking Service prior to the Service Start Date because you have not fulfilled your obligations under the Contract or you have given BT incomplete or inaccurate information or less than 10 Business Days' Notice to delay the vulnerability assessments, BT may, acting reasonably, apply additional Charges.

6.7   **Limitation of Liability**

In addition to the wording in Clause 22 of the General Terms, the following will apply:

6.7.1   You authorise BT and BT Personnel to perform the ethical hacking acts as part of the BT Security Ethical Hacking Service as legal acts that are not committed with any criminal, malicious, damaging or other detrimental intent or purpose.

6.7.2   You will not file or permit any person to file any criminal or civil complaints or initiate any criminal or civil procedures against BT or BT Personnel for the performance of the BT Security Ethical Hacking Service.

6.7.3   BT will not be liable for any financial or reputational damage, government or regulatory action and any other detrimental consequence that you suffer as a result of any criminal or civil proceedings, or BT's delivery and/or your use of the BT Security Ethical Hacking Service.

6.7.4   Nothing in Paragraphs 6.7.2 and 6.7.3 excludes BT's liability for its failure to deliver the BT Security Ethical Hacking Service as set out in the Schedule.

6.7.5   You are liable for and will fully indemnify, keep indemnified and hold harmless BT against all Claims, losses, costs and liabilities brought by any third parties (including your employees, workers or contractors) against BT arising out of BT's delivery and/or your use of the BT Security Ethical Hacking Service.

6.7.6   BT will not be liable for any losses or damages that result from a Transmitted Virus that is present on the Customer Equipment, Application, your software, system, data and network or for any other failure of the Customer Equipment Application, your software, system, data or network that is not caused by the performance of the Service.

6.8   **BT Personnel**

6.8.1   BT will perform the Service using BT employees that BT considers to be suitably qualified ("**BT Personnel**").

6.8.2   BT may vary the BT Personnel to meet BT's business needs and the personal needs of the BT Personnel and will give you reasonable notice.

6.8.3   BT will direct, control and supervise the work performed by the BT Personnel in accordance with BT's conditions of employment that apply to the Personnel.

6.8.4   BT may replace BT Personnel that are not reasonably acceptable to you where:

(a)   you ask BT to; and

(b)   where alternative BT Personnel are available.

6.8.5   Nothing in this Contract will prevent BT from assigning any BT Personnel to provide similar services for third parties or in any way restrict BT's use of the BT Personnel.

6.8.6   You will not take any disciplinary action against, deal with any grievance raised by, or grant any absence or leave requests from, the BT Personnel, and will refer any such management issues to BT.

6.8.7 Where the BT Security Ethical Hacking Service is provided on your premises, you will:

(a) comply with all reasonable health and safety rules and regulations and reasonable security requirements relating to the health, safety and welfare of the Personnel;

(b) will not act in a way inconsistent with BT remaining the employer of the BT Personnel and comply with all relevant employment legislation as it applies between you and the BT Personnel;

(c) You will at BT's reasonable request, promptly at no charge to BT, provide adequate office accommodation, facilities and other office support that BT requires for the effective performance of the Service; and

6.9 **Service Exclusions**

6.9.1 BT does not make any representations, whether express or implied, about whether the BT Security Ethical Hacking Service will identify all Vulnerabilities or lead to specific result or outcome.

6.9.2 BT will have no responsibility for any disruption to Customer Equipment, network, system, Application and any data being tested, except to provide reasonable information about the tests performed.

Part B – Service Delivery and Management

7 BT's Obligations

7.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the BT Security Ethical Hacking Service, BT will:

7.1.1 will provide you with contact details for the BT Contact;

7.1.2 will comply with all reasonable health and safety rules and regulations and reasonable security requirements that apply at the Site(s) and that you have notified to BT in writing, but BT will not be liable if, as a result of any such compliance, BT is in breach of any of its obligations under this Contract;

7.1.3 will provide you with a Customer Committed Date and will use reasonable endeavours to meet any Customer Committed Date but all dates are estimates; and

7.1.4 use BT Personnel that BT reasonably considers to be suitably qualified to deliver the Service.

7.2 **Commissioning of the Service**

Before the Service Start Date, BT will:

7.2.1 BT will agree with you on the scope of work that BT will provide as part of the BT Security Hacking Service as set out in the relevant SoW;

7.2.2 BT will attend a kick off meeting with the Customer Contact to discuss and obtain information required to commission the BT Security Ethical Hacking Service; and

7.2.3 BT will confirm to you the Service Start Date.

7.3 **During Operation**

On and from the Service Start Date, BT will provide you with the BT Ethical Hacking Service as set out in this Schedule.

7.4 **The End of the Service**

On expiry or termination of the BT Security Ethical Hacking Service by either of us, BT:

7.4.1 may disconnect and remove any BT Equipment (including any testing tools) located at the Site(s);

7.4.2 may delete any Content; and

7.4.3 will terminate your access to the portal.

8 Your Obligations

8.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the BT Security Ethical Hacking Service, you will:

8.1.1 provide BT with the names and contact details of the Customer Contact, but BT may also accept instructions from a person who BT reasonably believes is acting with your authority;

8.1.2 provide BT with any information reasonably required without undue delay;

8.1.3 provide BT with physical and logical access to any Site(s), network, equipment, applications, policy, systems, information, people and facilities (as applicable) during Business Hours, or as otherwise agreed between the both of us in writing, to enable BT to set up and provide the BT Security Ethical Hacking Service;

8.1.4 complete any preparation activities that BT may request to enable you to receive the BT Security Ethical Hacking Service (such as for example providing BT with authorisation and access to Customer Equipment and facilities promptly and in accordance with any reasonable timescales;

8.1.5 provide BT with Notice of any health and safety rules and regulations and security requirements that apply at the Site(s);

8.1.6 in jurisdictions where an employer (or any other person who receives the BT Security Ethical Hacking Service) is legally required to make a disclosure to its employees or Users:

(a) inform your employees and Users that as part of the BT Security Ethical Hacking Service being delivered by BT, BT may monitor and report to you on the use of any targeted applications by them;

(b) ensure that your employees and Users have consented or are deemed to have consented to such monitoring and reporting (if such consent is legally required); and

(c) agree that BT will not be liable for any failure by you to comply with this Paragraph 8.1.6, you will be liable to BT for any Claims, losses, costs or liabilities incurred or suffered by BT due to your failure to comply with this Paragraph 8.1.6.

8.1.7 ensure that you have the applicable service, Application, network, data or equipment available to be tested by BT;

8.1.8 attend and participate in a kick off meeting with BT to discuss and provide to BT information required to commission the BT Security Ethical Hacking Service;

8.1.9 undertake all appropriate backups (such as backup of your system data, programs, configuration files, security data, identification, authentication, access control, accounting and audit, source files and operating system configuration parameters as applicable);

8.1.10 inform your employees, subcontractors, and any other concerned parties about any planned testing activities and obtain any necessary prior consents;

8.1.11 ensure that you obtain all prior written authorisations required for BT to perform testing and assessments of any third party assets, equipment, people, applications, and systems, and, if requested by BT, provide a copy of such written authorisations to BT; and

8.1.12 fulfil any prerequisites as set out in the SoW.

8.2 **During Operation**

On and from the Service Start Date, you will:

8.2.1 ensure that the Customer Contact reports incidents relating to the BT Security Ethical Hacking Service to the BT Contact using the agreed reporting procedures, and ensure the Customer Contact is available for all subsequent Incident management communications;

8.2.2 monitor and maintain any Customer Equipment, Applications, network, systems or data connected to or used in connection with a BT Security Ethical Hacking Service;

8.2.3 ensure that any Customer Equipment, Application, data, system, network, and facilities (as applicable) that is connected to or used with the BT Security Ethical Hacking Service is:

(a) approved and used in accordance with relevant instructions, standards, and Applicable Law and any safety and security procedures applicable to the use of that Customer Equipment, Application, system, data, network or facilities; and

(b) is adequately separate from your production environment and managed to minimise impact to the production environment;

8.2.4 restore any back-ups required to return any of your applicable operational system, data, software, Application, network to its original state;

8.2.5 comply with any applicable business recovery regulatory guidelines (such as the SEC, SOX and CBFA guidelines);

8.2.6 duplicate and store Content you wish to keep on other devices not connected with the BT Security Ethical Hacking Service. BT will not be responsible if any Content is lost or deleted; and

8.2.7 ensure that you use any reasonable means to mitigate any disruption that may be caused by the testing undertaken as part of the BT Security Ethical Hacking Service.

8.3 **The End of the Service**

On expiry or termination of the BT Security Ethical Hacking Service by either of us, you will:

8.3.1 provide BT with all reasonable assistance necessary to remove BT Equipment from the Site(s);

8.3.2 disconnect any Customer Equipment from BT Equipment located at the Site(s);

8.3.3 not dispose of or use BT Equipment other than in accordance with BT's written instructions or authorisation;

8.3.4 arrange for any BT Equipment located at the Site(s) to be returned to BT; and

8.3.5 be liable for any reasonable costs of recovery that BT incurs in recovering the BT Equipment.

Part C – Service Levels

9   Service Care Levels

There are no Service Levels for this BT Security Ethical Hacking Service.

BT Security Ethical Hacking Schedule

Part D – Defined Terms

10   Defined Terms

In addition to the defined terms in the General Terms, capitalised terms in this Schedule will have the below meanings (and in the case of conflict between these defined terms and the defined terms in the General Terms, these defined terms will take precedence for the purposes of this Schedule). BT has repeated some definitions in this Schedule that are already defined in the General Terms. This is to make it easier for you to find the definitions when reading this Schedule.

"**Abortive Visit**" means a visit (on premise or remotely) where BT is not able to access the Site, system, network, data, information, policy, Application or software due to failure or delay by you.

"**Application**" or "**app**" means an application program or a computer program used by you or that you provide to BT in connection with a BT Security Ethical Hacking Service.

"**Assume Breach**" means the Service Option that verifies that protection, detection and response mechanisms are implemented properly by focusing to identify and addressing gaps in:

       (a)   detection of attack and penetration;

       (b)   response to attack and penetration;

       (c)   recovery from data leakage, tampering or compromise; and

       (d)   prevention of future attacks and penetration.

"**BT Contact**" means the BT representative that you will be able to contact to submit service requests, report Incidents and ask questions about the BT Security Ethical Hacking Service.

"**BT Price List**" means the document containing a list of BT's charges and terms that may be accessed at: www.bt.com/pricing (or any other online address that BT may advise you).

"**BT Personnel**" has the meaning given in Paragraph 6.8.1.

"**BT Security Ethical Hacking Service**" has the meaning given in Paragraph 1.

"**Business Hours**" means between the hours of 0800 and 1700 in a Business Day.

"**Content**" means applications, data, information (including emails), video, graphics, sound, music, photographs, software or any other material.

"**Customer Committed Date**" means the date provided by BT on which delivery of the BT Security Ethical Hacking Service (or each part of the BT Security Ethical Hacking Service, including to each Site) is due to start.

"**Customer Contact**" means any individuals authorised to act on your behalf for BT Security Ethical Hacking Service management matters.

"**Customer Equipment**" means any equipment including any Purchased Equipment or any software, other than BT Equipment, used by you in connection with a BT Security Ethical Hacking Service.

"**Denial of Service Vulnerability Assessment**" means the testing to identify Vulnerabilities in Internet facing infrastructure and web application(s) which could lead to a denial of service condition.

"**Final Report**" means the report that BT provides to you within 10 Business Days after the date that BT completes the testing and contains all Vulnerabilities that BT identified during the testing.

"**ECU**" means electronic control unit.

"**Firewall Policy Review**" means the review of your firewall rules and configuration for conformance with your IT Requirements and BT identified best practice.

"**General Terms**" means the general terms that this Schedule is attached to, or where not attached to this Schedule, can be found at www.bt.com/terms, and form part of the Contract.

"**Hardware Vulnerability Assessment**" means the testing to identify Vulnerabilities in embedded devices like printers, scanners, multifunctional devices, IoT devices, set-up boxes and network connected appliances including ECUs.

"**Host Configuration Review**" means the host based diagnostics that BT performs against hosts within your network.

"**Incident**" means an unplanned interruption to, or a reduction in the quality of, the BT Security Ethical Hacking Service or particular element of the BT Security Ethical Hacking Service.

"**Internet**" means a global system of interconnected networks that use a standard Internet Protocol to link devices worldwide.

"**IoT**" means internet over things.

"**Mobile Application Vulnerability Assessment**" means the testing for Vulnerabilities in your mobile Applications.

"**Network Vulnerability Assessment**" means the testing for Vulnerabilities that BT performs in your fixed wired network.

"**OSINT**" means open source intelligence and refers to all unclassified information which includes anything freely available on the Internet.

"**OSINT Assessment**" means the gathering and analysis of OSINT data.

"**Penetration Testing**" means the exploitation of identified Vulnerabilities to address the consequences.

"**Preliminary Report**" means the preliminary report that BT provides to you on or after the date that BT completes the testing activities.

"**Professional Services**" means those services provided by BT which are labour related services.

"**Red Teaming**" means the Service Option that provides real-world attack simulations designed to assess and significantly improve the effectiveness of an entire information security programme and that may include aspects of other Service Options including Social Engineering, Wireless Vulnerability Assessment, Source Code Review and Web Application Vulnerability Assessment.

"**Report**" means any and all preliminary, status and final reports issued to you as part of the BT Security Ethical Hacking Service.

"**Retesting**" means the testing of identified Vulnerabilities by BT to verify that they have been remediated.

"**Service Management Boundary**" has the meaning given in Paragraph 4.1.

"**Service Options**" has the meaning given in Paragraph 3.

"**Site**" means a location at which the BT Security Ethical Hacking Service is provided.

"**Social Engineering**" means a variety of test scenarios to assess the resistance of your employees to attacks by email or telephone.

"**Source Code Review**" means the testing by BT for Vulnerabilities in the source code of any of your applications.

"**SoW**" means statement of work and is the defined scope of works to be provided by BT as part of the BT Security Ethical Hacking Service. The SoW may also be referred to as the Order.

"**Standard Service Components**" has the meaning given in Paragraph 2.

"**Vehicle Vulnerability Assessment**" means the testing by BT to identify Vulnerabilities present in your vehicle.

"**Virus**" means a piece of program code, including a self-replicating element, usually (but not necessarily) disguised as something else that causes some unexpected and, for the victim, usually undesirable event and which is designed so that it may infect other computer systems.

"**Vulnerabilities**" means a flaw, weakness, bug, possible shortcoming or faulty implementation.

"**Web Application Vulnerability Assessment**" means the testing for Vulnerabilities in your web Applications.

"**Wireless Vulnerability Assessment**" means the testing for Vulnerabilities in your wireless network or other wireless device.