Conteúdo

1. Introdução 2
2. Requisitos de acesso limitado 2
3. Segurança geral da informação 2
4. Segurança de funcionários do terceiro 3
5. Revisão de auditoria e segurança 4
6. Direito de inspeção 4
7. Certificações de segurança 4
8. Segurança física - Instalações da BT 5
9. Segurança física - Instalações do terceiro 5
10. Fornecimento de ambiente de hospedagem para equipamento da BT 5
11. Desenvolvimento de software seguro 5
12. CUSTÓDIA 5
13. Acesso aos sistemas da BT 5
14. Sistemas do terceiro com informações da BT 6
15. Sistemas do terceiro a hospedar informações da BT 6
16. Segurança de rede - Rede própria da BT 6
17. Segurança de rede do terceiro 6
18. Segurança na nuvem 7
19. Centro de atendimento 7
20. Informações classificadas como OFICIAIS ou superiores pela HMG 7
21. Termos definidos einterpretação 7
ANEXO 1 - Requisitos adicionais de segurança 9

1. Introdução

1.1 Este documento define os Requisitos de Segurança da BT e aplica-se a todos os terceiros que trabalham para o ou em nome do Grupo BT, incluindo Openreach, EE e PlusNet, doravante referidos como "BT" no resto do documento.

1.2 Estes requisitos de segurança são adicionais e sem prejuízo de quaisquer outras obrigações do terceiro incluído no contrato.

1.3 Todas as normas mencionadas neste documento poderão ser encontradas no seguinte local.Normas do terceiro

2. Requisitos de acesso limitado

2.1 Sem prejuízo de quaisquer obrigações de confidencialidade, quando os funcionários do terceiro tiverem acesso às informações da BT, o terceiro terá de:

2.2 Garantir que as informações da BT não sejam divulgadas ou consultadas por funcionários do terceiro, a menos que necessário para a prestação do Serviço; e

2.3 Estabelecer todos os sistemas e processos técnicos e organizacionais necessários para proteger as Informações da BT (i) contra destruição acidental ou ilegal e (ii) perda, alteração, divulgação não autorizada ou acesso às Informações da BT de acordo com as Boas Práticas de Segurança da Indústria.

3. Segurança geral da informação

3.1 Mediante solicitação razoável, o terceiro disponibilizará à BT cópias de certificações de segurança e de declarações de conformidade relevantes para o Serviço, a fim de ilustrar evidências de conformidade com tais Requisitos de Segurança.

3.2 Caso haja uma mudança significativa nas normas de segurança da tecnologia ou da indústria; ou se houver alterações significativas nos Serviços ou na forma como são fornecidos, a BT poderá emitir uma alteração ao Contrato durante o prazo, se houver necessidade de uma alteração aos Requisitos de Segurança aplicáveis. O terceiro deverá respeitar a emenda do Contrato acordada dentro de um prazo razoável considerando a natureza da mudança e o risco para a BT.

3.3 O terceiro terá de, no mínimo, anualmente ou quando houver alterações significativas nos Serviços ou na forma como são fornecidos, rever estes requisitos de segurança e as normas associadas para garantir que estão em conformidade com todos os controlos de segurança aplicáveis.

3.4 Se o terceiro subcontratar obrigações nos termos do Contrato, o terceiro garantirá que todos os Contratos com os Subcontratantes relevantes e os seus Subcontratantes incluem termos escritos exigindo que o Subcontratante respeite as partes aplicáveis de tais Requisitos de Segurança ou requisitos de segurança equivalentes do terceiro.

3.5 As informações da BT poderão ser retidas durante o tempo necessário para a execução do Contrato, após o qual deverá ser retido por um máximo de dois anos, a menos que tenha sido acordado um período de retenção diferente entre a BT e o terceiro ou qualquer lei aplicável tenha uma exigência diferente.

3.6 Se os Serviços prestarem suporte direto a um Contrato do Governo do Reino Unido, o terceiro terá de estar em conformidade com a versão mais atual do Cyber Essentials Plus.

3.7 O terceiro terá de garantir que as Informações da BT serão tratadas de acordo com os controlos nas seguintes normas:

- Classificação de informações do terceiro e norma de manipulação de dados V4.0
- A nossa norma sobre controlos de terceiros V1.1 - Secções

  Secção 1 Funções e responsabilidades.

  Secção 2 Governação.

  Secção 3 Gestão de incidentes.

  Secção 4 Gestão de mudanças.

  Secção 5 Gestão de riscos e ameaças cibernéticos

  Secção 6 Controlo de acesso e gestão de identidade.

  Secção 10 Classificação e proteção de dados.

  Secção 12 Prevenção de fuga de dados.

  Secção 13 PCI-DSS (se estiver no âmbito do Serviço).

  Secção 19 Gestão de vulnerabilidades.

  Secção 22 Registo e monitorização contínuos.

4. Segurança de funcionários do terceiro

4.1 O terceiro garantirá que todos os funcionários do terceiro têm acordos de confidencialidade antes de quaisquer funcionários do terceiro começarem a trabalhar nos edifícios da BT ou nos sistemas da BT ou terem acesso às informações da BT. Estes acordos de confidencialidade terão de ser mantidos por terceiros e as evidências terão de ser disponibilizadas para auditoria pela BT.

4.2 O terceiro deverá lidar com violações do terceiro e dos controlos e normas aplicáveis da BT Security através de processos formais, incluindo ações disciplinares que poderão incluir o impedimento de o indivíduo:

4.2.1 ter acesso aos sistemas ou a informações da BT; ou

4.2.2 realizar trabalhos relacionados com a prestação do Serviço.

Além disso, o terceiro deverá garantir que têm processos relevantes em vigor para garantir que qualquer funcionário do terceiro que tenha sido removido não receba acesso aos sistemas da BT, às informações da BT ou permissão para trabalhar em conexão com a prestação do Serviço.

4.3 O terceiro, na medida do permitido pela lei, deverá manter uma instalação confidencial a usar pelos funcionários do terceiro para relatar anonimamente se for instruído a agir de forma inconsistente ou de forma que viole estes Requisitos de Segurança. Relatórios relevantes a mencionar à BT.

- Quando os funcionários do terceiro já não estiverem designados para o Serviço, a critério da BT, quaisquer ativos físicos ou informações da BT na posse de funcionários do terceiro deverão ser: devolvidos à equipa operacional relevante da BT;
- destruídos de acordo com a classificação de informações do terceiro e a norma de manipulação de dados V4.0

4.4 O terceiro terá de garantir a existência de processos apropriados em relação aos funcionários do terceiro para executar os controlos nas seguintes normas:

- A nossa norma sobre controlos de terceiros V1.1 - Secções

  Secção 15 Redes sociais

  Secção 23 Formação e sensibilização

5. Revisão de auditoria e segurança

5.1 Sem prejuízo de qualquer outro direito de auditoria que a BT possa ter, a fim de avaliar a conformidade do terceiro com tais Requisitos de Segurança e normas associadas, o terceiro facultará à BT, ou aos seus representantes, acesso e assistência conforme necessário e apropriado para permitir a realização de análises de segurança com base em documentos ou auditorias no local. O terceiro será avisado no mínimo com 30 dias úteis de antecedência antes de uma auditoria de rotina a efetuar no local.

O âmbito da auditoria será rever qualquer um ou todos os aspetos das políticas, processos e sistemas do terceiro (desde que o terceiro proteja a confidencialidade de quaisquer informações não relacionadas com a prestação do Serviço à BT) que sejam relevantes para o serviço que está a ser fornecido.

5.2 O terceiro trabalhará com a BT para implementar as recomendações acordadas e realizará as ações corretivas identificadas como necessárias, resultantes de uma revisão de segurança baseada em documentos ou de uma auditoria no local no prazo de 30 dias após a notificação da BT ou do período acordado entre as partes às custas do terceiro.

5.3 Caso a BT precise de efetuar uma auditoria independente do terceiro e o terceiro não esteja em conformidade com os princípios e práticas da ISO / CEI 27001: 2013, o terceiro deverá, às suas próprias custas, realizar as ações necessárias para alcançar a conformidade necessária e reembolsará integralmente quaisquer custos incorridos pela BT na obtenção de tal auditoria.

6. Direito de inspeção

6.1 O terceiro terá de conceder à BT o direito de inspeção de acordo com:

- A nossa norma sobre controlos de terceiros V1.1 - Secções

  Secção 24 Direito de inspeção.

7. Certificações de segurança

7.1 Os sistemas, Serviços, Serviços associados, processos e locais físicos do terceiro terão de estar em conformidade, e estar continuamente em conformidade, com a(s) norma(s) ISO / CEI 27001: 2013 (ou certificações que demonstrem controlos equivalentes, com o suporte de um relatório de auditor independente) bem como com qualquer versão alterada ou futura da norma emitida. Esta conformidade terá de ser garantida através de:

7.1.1 certificação do SGSI do terceiro por um Serviço de Acreditação do Reino Unido ou por um organismo de certificação aprovado equivalente internacional, em que o âmbito e a declaração de aplicabilidade tenham sido validados pela BT; ou

7.1.2 um processo bilateral de auditoria e um teste especificado pela BT.

7.2 O terceiro terá de enviar um certificado válido no início do Contrato e em futuras recertificações.

7.3 Caso o âmbito do certificado ou da declaração de aplicabilidade seja alterado a qualquer momento, o terceiro terá de enviar estas alterações para revalidação usando o procedimento de controlo de alterações (ou, na ausência de um procedimento de controlo de alterações, através do processo de variação). O terceiro terá de informar a BT no prazo de 2 dias úteis de qualquer não-conformidade importante identificada pelo organismo de certificação ou pelo terceiro.

8. Segurança física - Instalações da BT

8.1 Nos casos em que o terceiro estiver a trabalhar nas instalações da BT, serão aplicados os controlos na seguinte norma:

- A nossa norma sobre controlos de terceiros V1.1 - Secções

Secção 25. Segurança física - Instalações da BT

9. Segurança física - Instalações do terceiro

9.1 Quando forem usadas instalações do terceiro para fornecer o Serviço, serão aplicados os controlos na norma abaixo.

- A nossa norma sobre controlos de terceiros V1.1 - Secções

Secção 9. Segurança física em instalações do terceiro, **excluindo** os controlos 9.10 e 9.11 para fornecimento de ambiente de hospedagem para equipamentos da BT.

10. Fornecimento de ambiente de hospedagem para equipamento da BT

10.1 Quando forem usadas instalações do terceiro para fornecer um ambiente de hospedagem de equipamento, serão aplicados os controlos na norma abaixo.

- A nossa norma sobre controlos de terceiros V1.1 - Secções

Secção 9. Segurança física em instalações do terceiro - controlos 9.10 e 9.11 para fornecimento de ambiente de hospedagem para equipamentos da BT.

11. Desenvolvimento de software seguro

11.1 Quando o terceiro estiver a fornecer software ou sistemas, serão aplicados os controlos na norma abaixo.

- A nossa norma sobre controlos de terceiros V1.1 - Secções

Secção 17. (17.1 e 17.2) Desenvolvimento de software seguro

12. CUSTÓDIA

12.1 Quando uma CUSTÓDIA for necessária para proteger todas as partes, serão aplicados os controlos na norma abaixo.

- A nossa norma sobre controlos de terceiros V1.1 - Secções

Secção 17. (Apenas 17.3) Desenvolvimento de software seguro

13. Acesso aos sistemas da BT

13.1 Quando sistemas do terceiro ou funcionários do terceiro exigirem acesso / ligação aos sistemas da BT, serão aplicados os controlos na norma abaixo.

- A nossa norma sobre controlos de terceiros V1.1 - Secções

Secção 8. Acesso aos sistemas da BT

14. Sistemas do terceiro com informações da BT

14.1 Quando sistemas do terceiro forem usados para armazenar informações da BT, serão aplicados os controlos nas seguintes normas:

Classificação de informações do terceiro e norma de tratamento de dados V4.0

- A nossa norma sobre controlos de terceiros V1.1 - Secções

Secção 7 Gestão de ativos de informação.

Secção 11. Criptografia.

Secção 16 Configuração do sistema.

Secção 18 Proteção antimalware**.**

Secção 21. Mitigações de negação de serviço.

15. Sistemas do terceiro a hospedar informações da BT

15.1 Quando o terceiro hospeda as informações da BT, as instalações terão de possuir um certificado ISO / CEI 27001 válido para gestão de segurança (ou certificações que demonstrem controlos equivalentes, com o suporte de um relatório de auditor independente).

15.2 Aplicar-se-ão os controlos nas seguintes normas:

- Classificação de Informações do terceiro e Norma de Tratamento de Dados V4.0
- A nossa norma sobre controlos de terceiros V1.1 - Secções

Secção 7 Gestão de ativos de informação.

Secção 11. Criptografia.

Secção 16 Configuração do sistema.

Secção 18 Proteção antimalware**.**

Secção 21. Mitigações de negação de serviço.

16. Segurança de rede - Rede própria da BT

16.1 Quando o terceiro estiver a instalar o equipamento e a configurar, manter, reparar ou monitorizar a própria rede da BT, aplicar-se-ão os controlos da seguinte norma:

- A nossa norma sobre controlos de terceiros V1.1 - Secções

Secção 26. Segurança de rede - Rede própria da BT.

17. Segurança de rede do terceiro

17.1 Quando a rede do terceiro for usada para aceder a informações da BT ou fornecer o Serviço, serão aplicados os controlos na seguinte norma:

- A nossa norma sobre controlos de terceiros V1.1 - Secções

Secção 16 Configuração do sistema.

Secção 20 Integridade da rede

18. Segurança na nuvem

18.1 Nos casos em que o terceiro forneça à BT Serviços na nuvem, serão aplicados os controlos n seguinte norma:

- A nossa norma sobre controlos de terceiros V1.1 - Secções

  Secção 14. Computação online / cloud.

19. Centro de atendimento

19.1 Nos casos em que terceiros forneçam à BT Serviços de centro de atendimento, serão aplicados os controlos na seguinte norma:

- Norma do terceiro do centro de atendimento V1.0

20. Informações classificadas como OFICIAIS ou superiores pela HMG

20.1 Quando o Fornecedor precisar acessar, armazenar, processar ou transmitir informações classificadas como HMG OFFICIAL ou um Fornecedor superior, para realizar uma Avaliação de Risco de Segurança do Pessoal em todas as funções identificadas na Declaração Sensitiva Oficial nº 2, de acordo com os requisitos estabelecidos no documento CPNI National Security Clearance - A guide (4th Edition - June 2013 or later).

20.2 Os Requisitos de Segurança adicionais estabelecidos no Anexo 1 destes Requisitos de Segurança aplicar-se-ão a cado terceiro que armazenará, tratará ou transmitirá informações classificadas como "Sensíveis Oficiais", de acordo com o Esquema de Classificação de Segurança Governamental de Sua Majestade, atualizado periodicamente.

20.3 O terceiro garantirá que os sistemas e a infraestrutura usados para fornecer os Serviços estão contidos numa rede lógica dedicada. Esta rede só poderá ser composta pelos sistemas dedicados à entrega de instalações seguras de tratamento de dados dos clientes.

21. Termos definidos einterpretação

21.1 A menos que definido de outra forma abaixo, as palavras e expressões usadas nesses Requisitos de Segurança terão o mesmo significado que no Contrato:

"**Acesso**" significa o tratamento, a manipulação ou o armazenamento de informações da BT através de um ou mais dos seguintes métodos:

a. por interligação com os sistemas da BT;

b. com fornecimento em papel ou em formato não eletrónico;

c. informações da BT sobre sistemas de fornecedores; ou

d. por suportes móveis

e/ou acesso às instalações da BT para fornecimento dos Suprimentos, excluindo a entrega de hardware e a participação em reuniões.

"**Informações da BT**" significa todas as informações relacionadas com a BT ou um Cliente da BT dadas ao Fornecedor e todas as Informações que processadas ou tratadas pelo Fornecedor em nome da BT ou de um Cliente da BT nos termos do Contrato.

"**Sistemas da BT**" significa os Serviços e componentes, produtos, redes, servidores, processos, sistemas baseados em papel ou sistemas de TI dos Serviços (no todo ou em parte) pertencentes à e/ou operados pela BT ou outros sistemas que possam ser hospedados nas instalações da BT.

"**Contrato**" significa o Contrato assinado pelas Partes para o fornecimento de bens, software ou Serviços que faz referência a estes Requisitos de Segurança.

"**Cyber Essentials Plus**" significa um esquema apoiado pelo governo do Reino Unido para ajudar as organizações a protegerem-se contra ataques cibernéticos comuns.

"**Custódia**" significa o contrato de depósito do código-fonte assinado em conformidade com o Contrato para usar, copiar, manter e modificar tal código-fonte para fins comerciais da BT (incluindo o direito de compilar tal código-fonte).

"**Boas práticas de segurança do setor**" significa, em relação a qualquer empresa e a qualquer circunstância, a implementação das práticas, políticas, normas e ferramentas de segurança que seria razoável e normal esperar de uma pessoa qualificada e experiente envolvida no mesmo tipo de atividade em circunstâncias iguais ou semelhantes.

"**Segurança de rede**" significa a segurança dos caminhos e nós de comunicação interligados que ligam de forma lógica as tecnologias do utilizador final e os sistemas de gestão associados.

"**Declaração Sensível Oficial**" significa a declaração escrita a fornecer pelo Fornecedor relacionada com as funções identificadas pelo Fornecedor como tendo acesso a informações classificadas como "Sensíveis Oficiais" ou com privilégios elevados na infraestrutura que armazena, trata ou transmite informações classificadas como "Oficiais Sensíveis", cujo modelo consta do Anexo 1.

"**Requisitos de segurança**" significa este documento conforme atualizado periodicamente.

"**Subcontratante**" significa um Subcontratante do Fornecedor que realiza ou está envolvido no fornecimento dos Suprimentos ou que emprega ou envolve pessoas envolvidas no fornecimento dos Suprimentos.

"**Funcionários do terceiro**" significa qualquer pessoa envolvida pelo Fornecedor ou seus Subcontratantes no desempenho das obrigações do Fornecedor nos termos do Contrato.

"**Serviço**" significa todo e qualquer "**Bens**", "**Software**" ou "**Serviços**", conforme definido no Contrato.

"**Sistemas do terceiro**" significa qualquer computador, aplicação ou sistema de rede propriedade do Fornecedor usado para aceder, armazenar ou tratar as Informações da BT ou envolvido no fornecimento dos Suprimentos.

Interpretação

21.2 Quaisquer palavras após os termos "incluindo", "incluir", "em particular", "por exemplo" ou qualquer expressão semelhante serão interpretadas como ilustrativas e não limitarão o sentido das palavras, da descrição, da definição, da expressão ou do termo anterior a tais termos.

21.3 Sempre que um direito ou obrigação de uma Parte for expresso como um que "**poderá**" exercer ou executar, a opção de exercer ou executar tal direito ou obrigação ficará a critério exclusivo da Parte.

21.4 Quando qualquer hiperligação ("**URL**") for referenciada, tal referência será ao recurso online acessível através de tal URL ou de outra URL substituta, conforme notificado periodicamente à Parte aplicável.

ANEXO 1 - Requisitos adicionais de segurança

Quando o terceiro for obrigado a aceder, armazenar, tratar ou transmitir informações "Sensíveis Oficiais HMG", o terceiro respeitará estes Requisitos de Segurança e ainda os requisitos estabelecidos neste Anexo 1 e fornecerá à BT a Declaração Sensível Oficial preenchida antes da assinatura do contrato. Em todos os casos, o controlo de nível mais alto substituirá os requisitos documentados noutras partes destes Requisitos de Segurança para os Serviços e sistemas estabelecidos na Declaração Sensível Oficial.

1. FUNCIONÁRIOS

1.1. Todas as funções identificadas pelo Terceiro como tendo acesso a informações classificadas como "Oficiais Sensíveis" ou com privilégios elevados na infraestrutura que armazena, trata ou transmite informações classificadas como "Oficiais Sensíveis" serão documentadas na Declaração Sensível Oficial.

1.2. Os funcionários do terceiro empregados em funções identificadas na Declaração Sensível Oficial:

1.2.1. terão de estar sujeitos a uma verificação pré-emprego, de acordo com a norma BPSS (Baseline Personnel Security Standard, Norma de Base Relativa à Segurança dos Funcionários);

1.2.2. terão de assinar uma declaração da Lei de Segredos Oficiais; e

1.2.3. incapazes de obter as autorizações de segurança necessárias terão de ser impedidos de aceder às informações ou aos sistemas.

2. FORMAÇÃO EM SEGURANÇA

2.1. O terceiro exigirá formação de segurança após a contratação e pelo menos anualmente, cobrindo os requisitos de manuseamento de informações para informações classificadas como "Oficiais" ou "Oficiais Sensíveis", de acordo com os requisitos do Esquema de Classificação de Segurança Governamental de Sua Majestade, conforme indicado nas orientações de proteção de informações da HMG da BT para terceiros

2.2. O terceiro atualizará as descrições dos cargos para as funções documentadas na Declaração Sensível Oficial para exigir a participação na formação descrita no ponto 2.1 acima. O Terceiro manterá um registo de formação que terá de ser disponibilizado à BT mediante solicitação.

3. CONTROLO DE ACESSO

3.1. Quando os funcionários deixam determinada função, ou mudam de função, os seus direitos de Acesso terão de ser revogados dos Sistemas do terceiro relevantes no prazo de um (1) Dia Útil.

3.2. Nos casos em que os funcionários do terceiro, incluindo contratantes, funcionários temporários e funcionários de agências, têm privilégios elevados na infraestrutura da BT, o terceiro terá de notificar a BT por escrito no prazo de 1 dia útil a partir de quando um funcionário já não precisar de ter acesso aos sistemas da BT (por exemplo, baixa de funcionários ou mudança de cargos).

3.3. Quando os funcionários do terceiro, incluindo contratantes, funcionários temporários e agentes de agências, recebem cartões de acesso permanentes para as instalações da BT, o terceiro terá de notificar a BT por escrito no prazo de 1 dia útil quando um funcionário já não precisar de ter acesso às instalações da BT (por exemplo, baixa de funcionários ou mudança de cargos).

4. AVALIAÇÃO E CLASSIFICAÇÃO DE ATIVOS

4.1. O terceiro implementará procedimentos adicionais de manipulação de informações para atender aos requisitos de manipulação de informações "Oficiais" ou "Oficiais Sensíveis", de acordo com os requisitos do Esquema de Classificação de Segurança Governamental de Sua Majestade conforme atualização periódica

5. RESPOSTA A INCIDENTES E RELATÓRIOS - ACORDOS DE NÍVEL DE SERVIÇO

5.1. O terceiro será aconselhado relativamente a acordos específicos de Nível de Serviço para apoiar o processo de resposta a incidentes. Estes poderão substituir qualquer acordo anterior descrito nestes Requisitos de Segurança.

6. AUDITORIA, TESTES E MONITORIZAÇÃO

6.1. O terceiro implementará uma monitorização de segurança 24 horas por dia/7 dias por semana sempre que especificado pela BT

6.2. A infraestrutura do terceiro sujeita a monitorização de segurança 24 horas por dia, 7 dias por semana será documentada na Declaração Sensível Oficial.

7. CONTINUIDADE OPERACIONAL E RECUPERAÇÃO DE DESASTRES

7.1. O terceiro produzirá um plano de continuidade de negócio e recuperação de desastre de acordo com a BS ISO 22301 no prazo de 30 dias após a assinatura do Contrato.

8. LOCALIZAÇÃO

8.1. Salvo indicação em contrário da BT, o Serviço terá de estar fisicamente localizado dentro dos limites físicos do Reino Unido ou, se aplicável, do EEE.

ANEXO 1, EVIDÊNCIA 1 - MODELO DECLARAÇÃO SENSÍVEL OFICIAL

1. Sistemas / serviços no âmbito

Indique os sistemas e Serviços fornecidos no suporte ao cliente HMG.

Sistema	Serviço

2. Funções do terceiro que exigem um nível de habilitação de segurança.

Função	Nível de autorização de segurança necessário
** por exemplo, DBA*	*SC*

3. Gestão de vulnerabilidade

Sistema	Avaliação do tipo de vulnerabilidade	Frequência

4. Auditoria, testes e monitorização

Sistemas a monitorizar 24 horas por dia/7 dias por semana, conforme recomendado pela BT