

**ACORDO ENTRE O GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL E O GOVERNO DO
GRÃO DUCADO DE LUXEMBURGO SOBRE TROCA E PROTEÇÃO
MÚTUA DE INFORMAÇÃO CLASSIFICADA**

O Governo da República Federativa do Brasil

e

O Governo do Grão Ducado de Luxemburgo

A seguir denominados conjuntamente "Partes" ou individualmente como "Parte",

No interesse da segurança nacional e com a finalidade de assegurar a proteção de informações classificadas trocadas no âmbito dos tratados de cooperação ou acordos celebrados entre si, seus indivíduos, órgãos, assim como entidades públicas ou privadas credenciadas;

Desejando estabelecer um conjunto de regras e procedimentos sobre a proteção de Informações classificadas de acordo com as leis e regulamentos nacionais das Partes;

Confirmando que este Acordo não afetará os compromissos de ambas as Partes decorrentes de outros acordos internacionais e que não deve ser usado contra os interesses, segurança e integridade territorial de outros Estados.

Acordam o seguinte:

Artigo 1

Objeto e âmbito de aplicação

O presente Acordo estabelece regras e procedimentos para a proteção de Informação classificada trocada e gerada no processo de cooperação, em relação aos seus interesses e segurança nacionais, entre as Partes mencionadas, seus indivíduos, agências e entidades credenciadas.

Artigo 2

Definições

Para os fins do presente Acordo, o termo:

- a) **Contrato classificado:** significa qualquer contrato ou subcontrato, incluindo as negociações pré-contratuais, entre dois ou mais Contratantes criando e definindo direitos e obrigações exigíveis entre eles, que contém ou fornece acesso a informação classificada;
- b) **Informação Classificada:** é a informação, independentemente da sua forma, natureza e meios de transmissão, definida de acordo com as respectivas leis e regulamentos de ambas as Partes, protegida contra acesso ou divulgação não autorizados, que foi classificada e for trocada ou gerada pelas Partes;
- c) **Autoridade de Segurança Competente (CSA):** significa uma entidade competente autorizada, de acordo com as leis e regulamentos nacionais das Partes, responsável pela implementação dos requisitos de segurança abrangidos pelo presente Acordo;
- d) **Comprometimento:** designa qualquer forma de uso indevido, danos ou acesso não autorizado, alteração, divulgação ou destruição de Informação Classificada, bem como qualquer outra ação ou inatividade, devido a uma violação de segurança, resultando em perda de sua confidencialidade, integridade, disponibilidade ou autenticidade;
- e) **Contratante:** significa um indivíduo, agência ou entidade com capacidade legal para celebrar contratos;
- f) **Habilitação de Segurança de Instalação (FSC):** significa uma habilitação fornecida por uma Autoridade de Segurança Competente de uma Parte, que uma entidade pública ou privada localizada no seu país está autorizada e possui medidas de segurança apropriadas dentro de uma instalação específica para o Tratamento de Informação Classificada, de acordo com as leis e regulamentos nacionais;
- g) **Autoridade Nacional de Segurança (NSA):** designa o órgão estatal especificado pela legislação nacional das Partes, especialmente autorizado no âmbito da proteção da Informação Classificada;
- h) **Necessidade de conhecer:** designa a condição pela qual o acesso à Informação Classificada pode ser concedido a um indivíduo que tenha a real necessidade de conhecimento ou posse de tais informações para poder desempenhar funções e tarefas oficiais;
- i) **Parte Originária:** significa a Parte, incluindo qualquer empresa pública ou privada sob sua jurisdição, a partir da qual a Informação Classificada é produzida;

- j) **Credencial de Segurança Pessoal (PSC):** significa a autorização fornecida pela Autoridade de Segurança Competente de uma Parte que um indivíduo recebeu a credencial de segurança para o tratamento da informação classificada, de acordo com as leis e regulamentos nacionais, baseado na condição de que esse indivíduo está autorizado a ter acesso e manipular informação classificada até o nível definido na respectiva credencial.
- k) **Parte Receptora:** significa a Parte, incluindo quaisquer entidades públicas ou privadas sob a sua jurisdição, para a qual Informação Classificada é transmitida;
- l) **Acreditação de Segurança:** designa a qualificação positiva de entidades e órgãos públicos ou privados, bem como de pessoas físicas que, em virtude de procedimento de fiscalização ou de investigação de segurança, em conformidade com a legislação nacional, tenham sido autorizadas para o tratamento de Informações Classificadas para um certo nível de sigilo;
- m) **Violação de Segurança:** significa a ação ou omissão, seja intencional ou acidental, que resulta no comprometimento real ou possível da Informação Classificada;
- n) **Grau de Sigilo da Informação Classificada:** significa categoria, de acordo com as leis e regulamentos nacionais das Partes, que caracteriza a importância da Informação Classificada, o nível de restrição de seu acesso e o nível de sua proteção pelas Partes, e também a categoria com base na qual as informações são identificadas;
- o) **Habilitação de segurança:** designa o processo de emissão de um FSC ou PSC por uma Autoridade de Segurança Competente, em conformidade com as leis e regulamentos nacionais das Partes;
- p) **Terceira Parte:** designa os Estados, qualquer organização internacional, governos ou indivíduos que representem organismos ou organizações estatais, incluindo quaisquer entidades públicas e privadas que não sejam Partes do presente Acordo;
- q) **Tratamento da Informação Classificada:** designa o conjunto de ações relativas à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivo, armazenamento, liberação, avaliação, destinação ou controle da Informação Classificada em qualquer Grau de Sigilo; e
- r) **Visita:** significa qualquer acesso a entidades públicas e privadas, para efeitos deste presente Acordo, que inclui o tratamento de Informação Classificada.

Artigo 3

Graus de Sigilo da Informação Classificada

1. De acordo com as leis e regulamentos nacionais, as Partes concordam que os Graus de Sigilo da Informação Classificada devem corresponder uns aos outros e serem considerados equivalentes da seguinte forma:

No Grão Ducado de Luxemburgo (Francês)	Equivalente em Inglês	Na República Federativa do Brasil (Português)
TRES SECRET LUX	Top Secret	ULTRASSECRETO
SECRET LUX	Secret	SECRETO
CONFIDENTIEL LUX	Confidential	
RESTREINT LUX	Restricted	RESERVADO

2. Qualquer Informação Classificada fornecida sob este Acordo deve ser identificada com o Grau de Sigilo apropriado às leis e regulamentos nacionais da Parte Originária e, quando apropriado, ser prefixado com o nome do país de origem que fornecer a Informação Classificada.

3. As Partes devem marcar toda a Informação Classificada recebida da outra Parte com o Grau de Sigilo equivalente, de acordo com o parágrafo 1 deste Artigo.

4. As Partes devem notificar uma a outra sobre quaisquer alterações nos Graus de Sigilo da Informação Classificada, conforme especificado no parágrafo 1, e sobre todas as alterações de classificação subsequentes relativas à Informação Classificada transmitida.

5. A Parte Originária deve:

- a) sem demora, notificar a Parte Receptora de quaisquer alterações no Grau de Sigilo da Informação Classificada transmitida;
- b) informar à Parte Receptora quaisquer condições de divulgação ou limitações no uso de Informação Classificada.

Artigo 4

Proteção da Informação Classificada

1. As Partes tomarão todas as medidas adequadas, de acordo com as respectivas leis e regulamentos nacionais, para garantir que o nível de proteção concedido à Informação Classificada recebida, esteja em conformidade com o Grau de Sigilo equivalente, conforme estabelecido no Artigo 3 deste Acordo.

2. Nada neste Acordo prejudicará as leis ou regulamentos nacionais das Partes em relação aos direitos das pessoas físicas para obter acesso a documentos públicos ou acesso a informações de caráter público, proteção de dados pessoais ou proteção da Informação Classificada.

3. De acordo com suas leis e regulamentos nacionais, cada Parte deve assegurar que sejam implementadas medidas adequadas para a proteção da Informação Classificada que seja processada, armazenada ou transmitida em sistemas de comunicação e informação, até onde forem necessárias. Tais medidas devem assegurar a confidencialidade, a integridade, a disponibilidade e, quando aplicável, o não repúdio e a autenticidade da Informação Classificada, bem como um nível apropriado de responsabilização e rastreabilidade de ações em relação a essa informação.

Artigo 5

Divulgação e uso da Informação Classificada

1. Cada Parte deve garantir que a Informação Classificada fornecida ou trocada sob este Acordo não seja:

- a) Desclassificada ou reclassificada para um Grau de Sigilo da Informação Classificada inferior sem o prévio consentimento por escrito da Parte Originária;
- b) usada para propósitos diferentes dos estabelecidos pela Parte Originária;
- c) divulgada a qualquer Terceira Parte sem o prévio consentimento por escrito da Parte Originária e sem um apropriado acordo ou contrato para proteção de Informação Classificada esteja em vigor com a referida Terceira Parte.

2. Cada Parte, de acordo com seus requisitos constitucionais e legislação nacional, deve respeitar o princípio do consentimento do originador.

Artigo 6

Acesso a Informação Classificada

1. Cada Parte deve garantir que o acesso à Informação Classificada seja concedido com base no princípio da "Necessidade de Conhecer".

2. Cada Parte deve garantir que todos os indivíduos que tenham acesso à Informação Classificada sejam informados sobre suas responsabilidades para proteger essa informação de acordo com os regulamentos de segurança apropriados.

3. As Partes assegurarão que o acesso às Informação Classificada seja concedido apenas a indivíduos que possuam um PSC apropriado ou que estejam devidamente autorizados em virtude de suas funções de acordo com a legislação nacional.

4. De acordo com suas leis e regulamentos nacionais, cada Parte deverá garantir que qualquer entidade sob sua jurisdição que possa receber ou gerar Informação Classificada seja devidamente habilitada e seja capaz de fornecer proteção adequada, conforme previsto no parágrafo 1 do Artigo 4 deste Acordo, no nível de segurança apropriado.

Artigo 7

Tradução, reprodução e destruição de Informação Classificada

1. Todas as traduções e reproduções de Informação Classificada devem conter os Graus de Sigilo equivalente e serem protegidas e controladas adequadamente pelas Partes assim como o original.
2. Todas as traduções de Informação Classificada devem conter uma anotação adequada, na língua para a qual foi traduzida, indicando que elas contêm Informação Classificada da Parte Originária.
3. De acordo com o parágrafo 3 do Artigo 6 deste Acordo, os tradutores devem ter PSC apropriada ao Grau de Sigilo da Informação Classificada a ser traduzida.
4. A Informação Classificada como TOP SECRET/TRES SECRET LUX/ULTRASSECRETO deve ser traduzida ou reproduzida apenas mediante autorização prévia por escrito da Parte Originária.
5. A Informação Classificada recebida sob este Acordo não deverá ser destruída. A informação deverá ser devolvida à Parte Originária quando não for mais necessária à Parte Receptora.
6. A Informação Classificada não será reproduzida pela Parte Receptora sem a aprovação prévia por escrito da Parte Originária.

Artigo 8

Transmissão entre as Partes

1. A Informação Classificada deverá ser transmitida entre as Partes pela via diplomática ou conforme acordado entre as Partes.
2. A informação Classificada deve ser transmitida por meio de sistemas de comunicação protegidos, redes ou outros meios eletromagnéticos aprovados por ambas as Partes. Tais transmissões devem ser protegidas por meios criptográficos mutuamente aceitos pelas Autoridades Nacionais de Segurança, de acordo com as leis e regulamentos nacionais.
3. Informação Classificada como TOP SECRET/TRES SECRET LUX/ULTRASSECRETO deve ser enviada apenas pela via diplomática.
4. Informação classificada como RESTRICTED/RESTREINT LUX/RESERVADO também poderá ser postada ou utilizado outro serviço de entrega, de acordo com as leis e regulamentos nacionais.
5. Em caso de transmissão de grandes remessas contendo Informação Classificada, os procedimentos de transporte devem ser acordados e avaliados conjuntamente, caso a caso, pelas Autoridades Nacionais de Segurança das Partes.

Artigo 9 Visitas

1. As visitas às instalações onde a Informação Classificada é tratada ou armazenada devem estar sujeitas a aprovação prévia pela Autoridade Nacional de Segurança da Parte anfitriã, a menos que, de outra forma, seja aprovada mutuamente.
2. O pedido de visita deverá ser submetido à Autoridade Nacional de Segurança da Parte anfitriã e deve incluir os seguintes dados, os quais deverão ser usados unicamente para o propósito da visita:
 - a) nome do visitante, data e local de nascimento, nacionalidade e número do cartão de identificação/passaporte;
 - b) posição e função do visitante, bem como o nome e endereço da instalação onde ele é empregado;
 - c) especificação do projeto em que o visitante está participando;
 - d) a validade e o nível do PSC do visitante;
 - e) o nome, endereço, número de telefone, e-mail e ponto de contato da instalação a ser visitada;
 - f) o objetivo da Visita, incluindo a entidade que pretendem visitar e o mais alto Grau de Sigilo da Informação Classificada envolvida;
 - g) a data e a duração da visita. Para visitas recorrentes, o período total coberto pelas visitas deve ser indicado;
 - h) outros dados, se acordados pelas Autoridades Nacionais de Segurança; e
 - i) data e assinatura.
3. O pedido de Visita deverá ser submetido pelo menos 30 (trinta) dias antes da data prevista da visita, a menos que seja previamente aprovado mutuamente pelas Autoridades de Segurança Competentes.
4. Qualquer Informação Classificada divulgada a um visitante deve ser considerada como Informação Classificada recebida segundo as regras deste Acordo. Todo visitante deve cumprir com os regulamentos de segurança da Parte anfitriã.
5. As visitas somente poderão ser autorizadas por uma Parte aos visitantes da outra Parte se estes:
 - a) possuírem a PSC válida emitida pelo país de origem; e

b) estiverem autorizados a receber ou ter acesso a Informação Classificada sob o princípio da necessidade de conhecer.

6. Uma vez autorizada a Visita, a Autoridade Nacional de Segurança do país anfitrião deve notificar a Autoridade Nacional de Segurança do país do visitante sobre sua autorização, com um aviso mínimo de 10 (dez) dias, até a data prevista da Visita, e fornecer uma cópia do pedido para a entidade a ser visitada.

7. As Autoridades de Segurança Competentes podem concordar com uma lista de visitantes com direito a visitas recorrentes. A lista deve ser válida por um período inicial não superior a 12 (doze) meses e pode ser prorrogada por mais um período não superior a 12 (doze) meses. Um pedido de Visitas recorrentes deve ser apresentado de acordo com o parágrafo 3º deste Artigo. Assim que a lista for aprovada, as visitas podem ser organizadas diretamente entre as instalações envolvidas.

Artigo 10

Contratos Classificados relacionados a este Acordo

1. No caso de Contratos Classificados firmados e implementados no território de uma das Partes, a NSA ou CSA da outra Parte deve obter uma garantia escrita prévia de que o contratado proposto possui FSC e PSCs necessárias no Grau de Sigilo apropriado.

2. O Contratante compromete-se a:

- a) assegurar que suas instalações tenham condições adequadas para o Tratamento de Informação Classificada;
- b) possuir Habilitação de Segurança;
- c) assegurar que todas as pessoas com acesso a Informação Classificada tenham PSC apropriada e sejam informadas sobre suas responsabilidades em relação à sua proteção, de acordo com leis e regulamentos;
- d) permitir inspeções de segurança de suas instalações.

3. Para cada Contrato adjudicado, a Parte Originária informará a Parte Receptora o Grau de Sigilo da Informação Classificada transferida.

4. Os Contratos Classificados também devem fornecer os seguintes termos adicionais:

- a) responsabilidade pelo descumprimento dos procedimentos e medidas de segurança aplicáveis à Informação Classificada;
- b) obrigação de informar qualquer Violação de Segurança ou comprometimento de informação classificada para sua CSA;

- c) responsabilidade pelos danos resultantes de Violações de Segurança.
5. Qualquer subcontratado deve cumprir as mesmas obrigações de segurança que o Contratado.

Artigo 11

Autoridades Nacionais de Segurança e Cooperação de Segurança

1. As Autoridades Nacionais de Segurança responsáveis pela implementação e supervisão do presente Acordo serão:

Na República Federativa do Brasil

Gabinete de Segurança Institucional da Presidência da República – GSI/PR
Autoridade Nacional de Segurança
(National Security Authority)

No Grão Ducado de Luxemburgo:

Service de Renseignement de l'Etat
Autorité nationale de Sécurité
(National Security Authority)

2. Cada Parte deve fornecer à outra os dados de contato de sua respectiva Autoridade Nacional de Segurança por escrito.
3. As Autoridades Nacionais de Segurança devem informar-se mutuamente sobre suas respectivas leis e regulamentos nacionais vigentes que regulam a segurança da Informação Classificada.
4. As Autoridades Nacionais de Segurança devem informar-se mutuamente sobre quaisquer modificações a respeito delas mesmas ou sobre modificações das Credenciais ou Habilitações de Segurança de indivíduos, agências e entidades.
5. Com o objetivo de assegurar uma cooperação estreita na aplicação do presente Acordo, as Autoridades Nacionais de Segurança podem ser consultadas sempre que solicitado por uma delas.
6. Os representantes da Autoridade Nacional de Segurança de uma Parte podem visitar os estabelecimentos da Autoridade Nacional de Segurança da outra Parte com a intenção de adquirir conhecimento de procedimentos de segurança e medidas aplicáveis à Informação Classificada.
7. As Partes, por intermédio das suas Autoridades Nacionais de Segurança, devem informar-se mutuamente, a qualquer momento, sobre quaisquer alterações no título de tais órgãos ou transferência de suas competências para outros órgãos.
8. Se solicitado, as Partes, por meio das suas Autoridades Nacionais de Segurança, tendo em conta as respectivas leis e regulamentos nacionais, devem colaborar entre si no

decorrer dos procedimentos necessários para a emissão da Credencial de Segurança Pessoal de seus indivíduos que viveram ou vivem no território da outra Parte.

9. As Partes reconhecem mutuamente as PSC e as FSC, e devem informar à outra Parte prontamente sobre quaisquer mudanças nas mesmas.

10. Para alcançar e manter padrões de segurança compatíveis, as Autoridades de Segurança Competentes devem, sob demanda, fornecer uma à outra informações sobre os seus padrões nacionais de segurança, procedimentos e práticas para a proteção de Informação Classificada. Se necessário, as Autoridades Nacionais Competentes podem realizar reuniões regulares.

11. Sob demanda, as Partes devem prestar assistência mútua à concessão de PSCs.

Artigo 12

Assistência para Procedimentos de Habilitação e Credenciamento de Segurança

1. A pedido, as Autoridades Nacionais de Segurança das Partes, levando em consideração suas respectivas leis e regulamentos nacionais, devem auxiliar-se mutuamente durante os procedimentos de Habilitação e Credenciamento de Segurança.

2. As Partes devem reconhecer as Habilitações e Credenciais de Segurança emitidas de acordo com as leis e regulamentos da outra Parte.

Artigo 13

Violação de Segurança

1. No caso de uma violação de segurança relacionada a Informação Classificada que envolva as Partes deste Acordo, a Autoridade Nacional de Segurança da Parte onde a Violação de Segurança ocorreu deverá informar imediatamente a Autoridade Nacional de Segurança da outra Parte.

2. Quando a violação de Segurança ocorrer em uma Terceira Parte, a Autoridade Nacional de Segurança da Parte Originária deverá informar à Autoridade Nacional de Segurança da outra Parte, o mais rápido possível, e assegurar a investigação apropriada.

3. A Parte competente deve tomar todas as medidas em conformidade com as leis e regulamentos nacionais, a fim de limitar as consequências da violação a que se refere o parágrafo 1 deste Artigo e evitar violações futuras. A pedido, a outra Parte deve prestar assistência adequada; devendo ser informada do resultado do processo e das medidas tomadas pela violação.

4. A Parte onde a Violação de Segurança ocorrer deve investigar ou acompanhar a investigação do incidente e, ao final, informar imediatamente a outra Parte sobre o resultado da investigação e as medidas corretivas aplicadas.

5. A outra Parte, se necessário, deverá cooperar na investigação.

Artigo 14

Custos

Cada Parte deve arcar com os custos das suas próprias despesas resultantes da implementação e supervisão de todos os aspectos do presente Acordo.

Artigo 15

Disputas

1. Qualquer disputa que surja entre as Partes sobre a interpretação ou aplicação do presente Acordo, ou qualquer assunto relacionado, deve ser resolvida mediante consultas e negociações entre as Partes, por meio da via diplomática.
2. Durante o período de resolução da disputa, ambas as Partes devem continuar a cumprir todas as suas obrigações nos termos do presente Acordo.

Artigo 16

Comunicações

Todas as comunicações entre as Partes relativas à implementação deste Acordo serão feitas por escrito, em inglês.

Artigo 17

Entrada em Vigor

O presente Acordo deve entrar em vigor no primeiro dia do segundo mês após a recepção da última notificação, mediante a qual as Partes se informaram, por meio da via diplomática, de que os seus requisitos legais internos necessários para sua entrada em vigor foram cumpridos.

Artigo 18

Alterações

1. O presente Acordo pode ser alterado em qualquer momento, por escrito, por consentimento mútuo das Partes.
2. As alterações entrarão em vigor nos termos estabelecidos no Artigo 17 do presente Acordo.

Artigo 19

Validade e Denúncia

1. O presente Acordo permanecerá em vigor indefinidamente.

2. Qualquer Parte poderá, em qualquer momento, denunciar o presente Acordo mediante notificação escrita à outra Parte.
3. A rescisão deve ser notificada pela via diplomática e entrará em vigor após 6 (seis) meses a partir da data em que a outra Parte tenha recebido a notificação de denúncia.
4. Em caso de denúncia, qualquer Informação Classificada trocada nos termos do presente Acordo deve continuar a ser protegida de acordo com as disposições aqui estabelecidas, a menos que a Parte Originária isente a Parte Receptora dessa obrigação.

Artigo 20
Disposições Finais

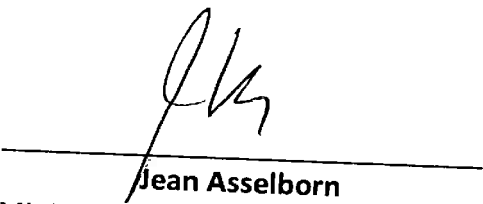
As Partes devem notificar-se prontamente sobre quaisquer alterações às respectivas leis ou aos regulamentos nacionais que afetem a proteção da Informação Classificada compartilhadas no âmbito deste Acordo. No caso de tais mudanças, as Partes consultarão para considerar possíveis mudanças neste Acordo. Enquanto isso, a Informação Classificada continuará a ser protegida conforme descrito neste documento, a menos que requisitado por escrito pela Parte Originária.

Feito em Nova York em 25 de setembro de 2018, em dois originais, cada um na língua portuguesa, francesa e inglesa, sendo todos os textos igualmente autênticos. Em caso de divergências de interpretação, o texto em inglês deverá prevalecer.

PARA O GOVERNO DA REPÚBLICA
FEDERATIVA DO BRASIL


Aloysio Nunes Ferreira
Ministro de Estado das Relações Exteriores

PARA O GOVERNO DO GRÃO DUCADO DE
LUXEMBURGO


Jean Asselborn
Ministro dos Negócios Estrangeiros e
Europeus

**AGREEMENT BETWEEN THE GOVERNMENT OF THE FEDERATIVE REPUBLIC OF BRAZIL AND
THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG ON THE EXCHANGE AND
MUTUAL PROTECTION OF CLASSIFIED INFORMATION**

The Government of the Federative Republic of Brazil

and

The Government of the Grand Duchy of Luxembourg,

hereinafter referred to jointly as "Parties" or in singular as a "Party",

In the interest of national security and for the purpose of ensuring the protection of Classified Information exchanged within the sphere of cooperation treaties or contracts entered into between them, their accredited individuals, bodies, as well as public or private entities;

Wishing to establish a set of rules and procedures about the protection of Classified Information in accordance with the national legislation of the Parties;

Confirming that this Agreement shall not affect the commitments of both Parties which stem from other international agreements and that it shall not be used against the interests, security and territorial integrity of other states;

Have agreed as follows:

Article 1

Object and Scope of Application

The present Agreement establishes rules and procedures for the protection of Classified Information exchanged and generated in the process of cooperation, in respect of their national interests and security, among the aforementioned Parties, their accredited individuals, agencies and entities.

Article 2 Definitions

For the purpose of the present Agreement, the term:

- a) **Classified Contract:** means any contract or sub-contract including the pre-contractual negotiations, between two or more Contractors creating and defining enforceable rights and obligations between them, which contains or provides for access to Classified Information;
- b) **Classified Information:** means the information, regardless of its form, nature, and means of transmission, determined according to the respective laws and regulations of both Parties, protected against unauthorised access or disclosure, which has been classified and is exchanged between, or generated by the Parties;
- c) **Competent Security Authority (CSA):** means a competent entity authorized according to the national laws and regulations of the Parties which is responsible for implementing the security requirements covered by this Agreement;
- d) **Compromise:** designates any form of misuse, damage or unauthorized access, alteration, disclosure or destruction of Classified Information, as well as any other action or inaction, due to a Security Breach, resulting in loss of its confidentiality, integrity, availability or authenticity;
- e) **Contractor:** means an individual, agency or entity possessing the legal capacity to conclude contracts;
- f) **Facility Security Clearance (FSC):** means a determination by a Competent Security Authority of a Party that a public or private entity located in its country is security cleared and has in place appropriate security measures within a specific facility for the Treatment of Classified Information, in accordance with the national laws and regulations;
- g) **National Security Authority (NSA):** designates the state body specified by the national legislation of the Parties which is specially authorized in the sphere of protection of Classified Information;
- h) **Need to Know:** designates the condition by which access to Classified Information may be granted to an individual who has a verified requirement for knowledge of or possession of such information in order to be able to perform official duties and tasks;
- i) **Originating Party:** means the Party, including any public or private entities under its jurisdiction, from which Classified Information is released;
- j) **Personnel Security Clearance (PSC):** means a determination by a Competent

Security Authority of a Party that an individual has been security cleared for the Treatment of Classified Information, in accordance with its national laws and regulations; on the basis of which the individual is authorized to have the access and to handle Classified Information up to the level defined in the clearance;

- k) **Receiving Party:** means the Party, including any public or private entities under its jurisdiction, to which Classified Information is transmitted;
- l) **Security Accreditation:** designates the positive qualification of public or private entities and bodies, as well as of individuals, that, due to an inspection procedure or security investigation, in conformity with national laws and regulations, have been authorized for the treatment of Classified Information for a certain secrecy level;
- m) **Security Breach:** means the action or omission, whether intentional or accidental, which results in the actual or possible Compromise of Classified Information;
- n) **Security Classification Level:** means the category, according to the national laws and regulations of the Parties, which characterizes the importance of Classified Information, the level of restriction of access to it and the level of its protection by the Parties, and also the category on the basis of which information is marked;
- o) **Security Clearance:** designates the process for issuing a FSC or PSC by a Competent Security Authority, in conformity with the national laws and regulations of the Parties;
- p) **Third Party:** designates the states, any international organization, Governments or individual representing state bodies or organizations, including any public and private entities, which are not Parties to this Agreement;
- q) **Treatment of Classified Information:** designates a set of actions relating to production, reception, classification, use, access, reproduction, transportation, transmission, distribution, archiving, storage, disposal, evaluation, destination or control of Classified Information at any classification level;
- r) **Visit:** means any access to public and private entities, for the purpose of this Agreement which includes the handling of Classified Information.

Article 3
Security Classification Levels

1. In accordance with the national laws and regulations, the Parties agree that the Security Classification Levels shall correspond to one another as follows and be considered as equivalent:

In the Grand Duchy of Luxembourg (Français)	Equivalent in English	In the Federative Republic of Brazil (Português)
TRES SECRET LUX	Top Secret	ULTRASSECRETO
SECRET LUX	Secret	SECRETO
CONFIDENTIEL LUX	Confidential	
RESTREINT LUX	Restricted	RESERVADO

2. Any Classified Information provided under this Agreement shall be marked with the appropriate Security Classification Level according to the national laws and regulations of the Originating Party and, where appropriate, be prefixed with the name of the country owning and providing the Classified Information.

3. The Parties shall mark all the Classified Information received from the other Party with an equivalent Security Classification Level according to paragraph 1 of this Article.

4. The Parties shall notify each other of any changes to the Security Classification Levels as specified in paragraph 1 and about all subsequent classification alterations to the transmitted Classified Information.

5. The Originating Party shall:

- a) without delay, notify the Receiving Party of any changes to the Security Classification Level of released Classified Information;
- b) inform the Receiving Party of any conditions of release or limitations on the use of Classified Information.

Article 4
Protection of Classified Information

1. The Parties shall take all appropriate measures in accordance with their respective national laws and regulations to ensure that the level of protection granted to Classified Information received shall be in accordance with their equivalent Security Classification Level as stated in Article 3 of this Agreement.

2. Nothing in this Agreement shall cause prejudice to the national laws or regulations of the Parties regarding the rights of individuals to obtain access to public documents or access to information of public character, the protection of personal data or the protection of Classified Information.

3. In accordance with its national laws and regulations, each Party shall ensure that appropriate measures are implemented for the protection of Classified Information processed, stored or transmitted in communication and information systems as long as it is deemed necessary. Such measures shall ensure the confidentiality, integrity, availability and, where applicable, non-repudiation and authenticity of Classified Information, as well as an appropriate level of accountability and traceability of actions in relation to that information.

Article 5

Disclosure and use of Classified Information

1. Each Party shall ensure that Classified Information provided or exchanged under this Agreement is not:

- a) declassified or downgraded without the prior written consent of the Originating Party;
- b) used for purposes other than those established by the Originating Party;
- c) disclosed to any Third Party without the prior written consent of the Originating Party, and an appropriate agreement or arrangement for the protection of Classified Information is in place with the Third Party concerned.

2. Each Party in accordance with its constitutional requirements and national legislation shall respect the principle of originator consent.

Article 6

Access to Classified Information

1. Each Party shall ensure that access to Classified Information is granted based on the principle of "Need to know".

2. Each Party shall ensure that all individuals granted access to Classified Information are informed of their responsibilities to protect such information in accordance with the appropriate security regulations.

3. The Parties shall ensure that access to Classified Information is granted only to individuals who hold an appropriate PSC or who are otherwise duly authorized by virtue of their functions in accordance with national legislation.

4. In accordance with its national laws and regulations, each Party shall ensure that any entity under its jurisdiction that may receive or generate Classified Information be appropriately security cleared and be capable of providing suitable protection, as provided for in paragraph 1 of Article 4 of this Agreement, at the appropriate security level.

Article 7

Translation, Reproduction and Destruction of Classified Information

1. All translations and reproductions of Classified Information shall bear the appropriate Security Classification Levels and shall be protected and controlled as the original by the Parties accordingly.
2. All translations of Classified Information shall contain a suitable annotation, in the language to which they were translated, indicating that they contain Classified Information of the Originating Party.
3. In accordance with paragraph 3 of Article 6 of this Agreement the translators must have an appropriate PSC in the level of secrecy of the Classified Information to be translated.
4. Classified Information marked as top secret (TRES SECRET LUX/ULTRASSECRETO) shall be translated or reproduced only upon prior written permission of the Originating Party.
5. Classified Information received under this Agreement shall not be destroyed. When it is no longer considered necessary by the Receiving Party it shall be returned to the Originating Party.
6. Classified Information shall not be reproduced by the Receiving Party without the prior written approval of the Originating Party.

Article 8

Transmission between the Parties

1. The Classified Information shall be transmitted between the Parties through diplomatic channels or as otherwise agreed by the Parties.
2. The Classified Information must be transmitted through protected communications systems, networks, or other electromagnetic media approved by both Parties. Such transmissions shall be protected by cryptographic means that are mutually accepted by the National Security Authorities in accordance with the national laws and regulations.
3. Classified Information marked as top secret (TRES SECRET LUX/ULTRASSECRETO) shall be sent only through diplomatic channels.
4. Information classified as restricted (Restreint Lux/Reservado) may be transmitted also by post or another delivery service in accordance with the national laws and regulations.

5. In case of transmitting a large consignment containing Classified Information, procedures for transport shall be jointly agreed and evaluated, on a case-by-case basis, by both National Security Authorities of the Parties.

Article 9

Visits

1. Visits to facilities where Classified Information is handled or stored shall be subject to prior approval by the National Security Authority of the host Party, unless otherwise mutually approved.

2. A request for a Visit shall be submitted to the National Security Authority of the host Party and shall include the following data that shall be used for the purpose of the visit only:

- a) the visitor's name, date and place of birth, nationality and identification card/passport number;
- b) position and function of the visitor as well as the name and address of the facility where he/she is employed;
- c) specification of the project in which the visitor is participating;
- d) the validity and level of the visitor's PSC;
- e) the name, address, phone number, e-mail and point of contact of the facility to be visited;
- f) the purpose of the Visit, including the entity that they intend to visit and the highest security classification level of Classified Information involved;
- g) the date and duration of the visit. For recurring visits, the total period covered by the visits shall be stated;
- h) other data, if agreed upon by the National Security Authorities; and
- i) date and signature.

3. A request for a Visit shall be submitted at least 30 (thirty) days prior to the expected date of the visit unless otherwise mutually approved by the Competent Security Authorities.

4. Any Classified Information released to a visitor shall be considered as Classified Information received under this Agreement. All visitors shall comply with the security regulations of the host Party.

5. The visits shall be authorized by one Party to the visitors of the other Party, only if those:

- a) have valid Personal Security Clearance granted by their country of origin; and
- b) are authorized to receive or have access to the Classified Information as per the Need to Know basis.

6. Once the Visit is authorized, the National Security Authority of the host country shall notify the National Security Authority of the visitor's country about its authorization with a minimum notice of 10 (ten) days to the expected date of the Visit and supply a copy of the request to the entity to be visited.

7. The Competent Security Authorities may agree on a list of visitors entitled to recurring Visits. The list shall be valid for an initial period not exceeding 12 (twelve) months and may be extended for a further period of time not exceeding 12 (twelve) months. A request for recurring Visits shall be submitted in accordance with paragraph 3 of this Article. Once the list has been approved, Visits may be arranged directly between the facilities involved.

Article 10

Classified Contracts related to this Agreement

1. In case of Classified Contracts concluded and implemented in the territory of one of the Parties, the NSA or CSA of the other Party shall obtain prior written assurance that the proposed Contractor holds a FSC and all PSCs necessary for the appropriate level.

2. The Contractor commits itself to:

- a) ensure that its premises have adequate conditions for the Treatment of Classified Information;
- b) have appropriate Facility Security Clearance;
- c) ensure that all persons with access to Classified Information have appropriate Personal Security Clearance and are informed of their responsibility towards their protection, according to laws and regulations;
- d) allow security inspections of their premises.

3. For each contract awarded the Originating Party shall inform the Receiving Party of the level of the Classified Information transferred.

4. The Classified Contracts must also provide these additional terms:

- a) liability for the non-compliance with the Security procedures and measures applicable to the Classified Information;

- b) obligation of informing any Security Breach or Compromise of Classified Information to its Competent Security Authority;
 - c) liability for the damages resulting from Security Breaches.
5. Any subcontractor must fulfill the same security obligations as the Contractor.

Article 11

National Security Authorities and Security Cooperation

1. The National Security Authorities responsible for the implementation and supervision of the present Agreement shall be:

In the Federative Republic of Brazil:

Gabinete de Segurança Institucional da Presidência da República – GSI/PR
Autoridade Nacional de Segurança
(National Security Authority)

In the Grand Duchy of Luxembourg:

Service de Renseignement de l'Etat
Autorité nationale de Sécurité
(National Security Authority)

2. Each Party shall provide the other with the necessary contact data of their respective National Security Authorities in writing.
3. The National Security Authorities shall inform each other about their respective national laws and regulations in effect that regulate the security of Classified Information.
4. The National Security Authorities shall inform each other about any modifications concerning them or regarding the Security Clearances of individuals, agencies and entities.
5. Aiming at ensuring a close cooperation in the application of the present Agreement, the National Security Authorities may be consulted whenever it is requested by one of them.
6. Representatives of the National Security Authority of one Party may visit the establishments of the National Security Authority of the other Party with the intent of acquiring knowledge of security procedures and measures applicable to Classified Information.
7. The Parties, through their National Security Authorities, shall inform each other, in time, on any changes in the title of such bodies or transfers of its competences to other bodies.
8. If requested, the Parties, through their National Security Authorities, bearing in mind the respective national laws and regulations, shall collaborate with each other in the

course of the necessary procedures for the Personnel Security Clearance of their individuals that have lived or live in the territory of the other Party.

9. The Parties mutually recognize each other's Personnel Security Clearances and Facility Security Clearances, and shall promptly inform each other about any changes in mutually recognized FSCs and PSCs.

10. To achieve and maintain comparable standards of security, the Competent Security Authorities shall, on request, provide each other with information about their national security standards, procedures and practices for the protection of Classified Information. If required, the Competent Security Authorities may conduct regular meetings.

11. Upon request, the Parties shall provide mutual assistance in carrying out Personnel Security Clearances.

Article 12

Assistance for Security Clearance Procedures

1. Upon request, the National Security Authorities of the Parties, taking into account their respective national laws and regulations, shall assist each other during the Security Clearance procedures.

2. The Parties shall recognize Security Clearances issued according to laws and regulations of the other Party.

Article 13

Security Breach

1. In case of a Security Breach related to Classified Information that involves the Parties of this agreement, the National Security Authority of the Party where the Security Breach happens shall immediately inform the National Security Authority of the other Party.

2. When the Security Breach has occurred in a Third Party, the National Security Authority of the Originating Party shall inform the National Security Authority of the other Party, as soon as possible, and ensure the appropriate investigation.

3. The competent Party shall undertake all measures in accordance with the national laws and regulations so as to limit the consequences of the breach referred to in paragraph 1 of this Article and to prevent further breaches. On request, the other Party shall provide appropriate assistance; it shall be informed of the outcome of the proceedings and the measures undertaken due to the breach.

4. The Party where the Security Breach happens shall investigate or accompany the investigation of the incident and, at the end, immediately inform the other Party about the result of the investigation and the applied corrective measures.

5. The other Party shall, if required, co-operate in the investigation.

Article 14

Costs

Each Party shall bear the costs of its own expenses resulting from the implementation and supervision of all aspects of the present Agreement.

Article 15

Disputes

1. Any dispute that should arise between the Parties regarding the interpretation or application of the present Agreement, or any related matter, shall be resolved by consultations and negotiations between the Parties, through diplomatic channels.
2. During the period of resolution of the dispute, both Parties shall continue to fulfill all of their obligations under this Agreement.

Article 16

Communications

All communications between the Parties related to the implementation of this Agreement shall be made in writing, in English.

Article 17

Entry into force

The present Agreement shall come into force on the first day of the second month after the reception of the last notification, by which the Parties have informed each other, through diplomatic channels, that their internal legal requirements necessary for its entry into force were complied with.

Article 18

Amendments

1. The present Agreement may be amended at any time, in writing, by mutual consent of the Parties.
2. The amendments shall come into force in the terms established in Article 17 of the present Agreement.

Article 19
Validity and Termination

1. This Agreement shall remain in force indefinitely.
2. Any Party may, at any time, terminate this Agreement by written notification to the other Party.
3. The termination must be notified by diplomatic channels and shall come into effect after 6 (six) months from the date on which the other Party has received the termination notification.
4. In case of termination, any Classified Information exchanged in the terms of the present Agreement shall continue to be protected in accordance with the provisions set out herein, unless the Originating Party exempts the Receiving Party from that obligation.

Article 20
Final Provisions

The Parties shall promptly notify each other of any changes to its respective national laws or regulations that affect the protection of Classified Information released under this Agreement. In the event of such changes, the Parties shall consult to consider possible changes to this Agreement. In the meantime, the Classified Information shall continue to be protected as described herein, unless otherwise requested by the Originating Party in writing.

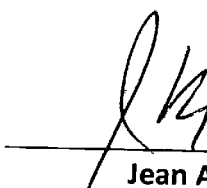
Done at New York on 25th September 2018, in two originals, each in the Portuguese, French and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

FOR THE GOVERNMENT OF THE FEDERATIVE
REPUBLIC OF BRAZIL

FOR THE GOVERNMENT OF THE GRAND
DUCHY OF LUXEMBOURG



Aloysio Nunes Ferreira
Minister of Foreign Affairs



Jean Asselborn
Minister of Foreign and European Affairs

**ACCORD ENTRE LE GOUVERNEMENT DE LA RÉPUBLIQUE FÉDÉRATIVE DU BRÉSIL ET LE
GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG CONCERNANT
L'ÉCHANGE ET LA PROTECTION RÉCIPROQUE D'INFORMATIONS CLASSIFIÉES**

Le Gouvernement de la République fédérative du Brésil

et

le Gouvernement du Grand-Duché de Luxembourg,

ci-après dénommés conjointement les « Parties » ou individuellement la
« Partie »,

Dans l'intérêt de la sécurité nationale et en vue de garantir la protection d'Informations Classifiées échangées dans le cadre de traités de coopération ou de contrats conclus entre elles, les personnes ou entités accréditées, ainsi que des entités publiques ou privées ;

Souhaitant définir un ensemble de règles et de procédures en matière de protection des Informations Classifiées, conformément à la législation nationale des Parties ;

Confirmant que le présent Accord n'affecte pas les engagements des deux Parties qui découlent d'autres accords internationaux et qu'il ne sera pas utilisé à l'encontre des intérêts, de la sécurité et de l'intégrité territoriale d'autres États ;

Conviennent ce qui suit :

Article 1

Objet et champ d'application

Le présent Accord définit les règles et procédures en matière de protection des Informations Classifiées échangées et générées dans le cadre du processus de coopération, dans le respect de leurs intérêts nationaux et de leur sécurité, entre les Parties susmentionnées, les personnes, les organismes et les entités accrédités.

Article 2 Définitions

Aux termes du présent Accord, on entend par :

- a) **Contrat Classifié** : tout contrat ou sous-contrat incluant les négociations précontractuelles entre deux Contractants ou plus, élaborant et définissant des droits et obligations contraignants entre eux et qui contient ou fournit un accès aux Informations Classifiées ;
- b) **Information Classifiée** : information, quels que soient sa forme et sa nature, ainsi que ses moyens de transmission, définie selon les lois et les réglementations de chaque Partie, protégée contre l'accès ou la communication non autorisés, qui a été classifiée et qui est échangée entre les parties ou générées par celles-ci ;
- c) **Autorité de sécurité compétente** : instance compétente autorisée conformément aux lois et réglementations nationales des Parties, qui est responsable de l'application des exigences de sécurité couvertes par le présent Accord ;
- d) **Compromission** : toute forme d'utilisation abusive, dommage ou accès, modification, communication ou destruction non autorisés d'Informations Classifiées, ainsi que toute action ou inaction, causées par une Infraction à la sécurité et entraînant la perte de sa confidentialité, d'intégrité, de disponibilité ou d'authenticité ;
- e) **Contractant** : toute personne physique, agence ou instance dotée de la capacité juridique de conclure des contrats ;
- f) **Habilitation de sécurité d'installation** : décision par une Autorité de sécurité compétente d'une Partie, qu'une instance publique ou privée située dans son pays dispose d'une habilitation de sécurité et de mesures de sécurité adaptées dans une installation spécifique pour le Traitement d'Informations Classifiées, conformément aux lois et aux réglementations nationales ;
- g) **Autorité nationale de sécurité** : organisme public désigné dans la législation des Parties qui dispose d'autorisations spéciales en matière de protection d'Informations Classifiées ;
- h) **Besoin de savoir** : condition d'accès aux Informations Classifiées accordé à une personne physique dont il est attesté qu'elle répond aux exigences en matière de connaissance ou de détention de telles informations afin de pouvoir exécuter ses fonctions et tâches officielles ;
- i) **Partie d'origine**: Partie, en ce compris les personnes physiques ou morales relevant de sa juridiction, qui délivre des Informations Classifiées ;

- j) **Habilitation de sécurité individuelle** : décision par une Autorité de sécurité compétente d'une Partie, qu'un individu dispose d'une habilitation de sécurité pour le Traitement d'Informations Classifiées, conformément à ses lois et réglementations nationales, sur la base de laquelle la personne physique est autorisée à accéder et à utiliser des Informations Classifiées selon le niveau défini dans l'habilitation ;
- k) **Partie destinataire** : Partie, en ce compris les personnes physiques ou morales relevant de sa juridiction, qui reçoit des Informations Classifiées ;
- l) **Accréditation de sécurité** : qualification positive d'entités ou d'organismes privés, ainsi que d'individus, qui, à la suite d'une procédure d'inspection ou d'une enquête de sécurité et conformément aux lois et réglementations nationales, sont autorisés à traiter des Informations Classifiées selon un certain niveau de confidentialité ;
- m) **Infraction à la sécurité** : action ou oubli, intentionnel ou accidentel, qui entraîne une atteinte réelle ou éventuelle des Informations Classifiées ;
- n) **Niveau de classification de sécurité** : catégorie qui, conformément aux lois et réglementations nationales, caractérise l'importance des Informations Classifiées, le niveau de restriction dont leur accès fait l'objet et le degré de protection dont elles doivent bénéficier de la part des Parties, ainsi que la catégorie sur la base de laquelle les informations sont identifiées ;
- o) **Habilitation de sécurité** : procédure de délivrance d'une habilitation de sécurité d'installation ou habilitation de sécurité individuelle par une Autorité de sécurité compétente, conformément aux lois et aux réglementations nationales des Parties ;
- p) **Tierce Partie** : États, organisations nationales, gouvernements ou personnes physiques représentant une entité ou une organisation étatique, y compris toute entité publique ou privée, qui ne sont pas des Parties selon les termes du présent Accord ;
- q) **Traitement d'Informations Classifiées** : ensemble d'actions de production, de réception, de classification, d'utilisation, d'accès, de reproduction, de transport, de transmission, de distribution, d'archivage, de stockage, de disposition, d'évaluation, de destination ou de contrôle d'Informations Classifiées à un quelconque niveau de classification ;
- r) **Visites** : accès à des instances publiques ou privées, dans le cadre du présent Accord, qui comprend le traitement d'Informations Classifiées.

Article 3

Niveaux de classification de sécurité

1. Conformément aux lois et réglementations nationales, les Parties reconnaissent que leurs Niveaux de classification de sécurité correspondent aux niveaux mentionnés ci-après et peuvent être considérés comme équivalents :

Au Grand-Duché de Luxembourg (Français)	Équivalent en anglais	Dans la République fédérative du Brésil (Português)
TRÈS SECRET LUX	TOP SECRET	ULTRASSECRETO
SECRET LUX	SECRET	SECRETO
CONFIDENTIEL LUX	CONFIDENTIAL	
RESTREINT LUX	RESTRICTED	RESERVADO

2. Toute Information Classifiée fournie au titre du présent accord est marquée du Niveau de classification de sécurité approprié selon les lois et les réglementations nationales de la Partie d'origine et, le cas échéant, précédée du nom du pays détenant et fournissant l'Information Classifiée.

3. Les Parties marquent toutes les Informations Classifiées reçues de l'autre Partie du Niveau de classification de sécurité équivalent conformément au paragraphe 1 du présent article.

4. Les Parties notifient toute modification de Niveau de classification de sécurité, tel que spécifié au paragraphe 1 et toute modification ultérieure de classification des Informations Classifiées transmises.

5. La Partie d'origine :

- a) informe immédiatement la Partie destinataire de toute modification apportée au Niveau de classification de sécurité des Informations Classifiées délivrées ;
- b) informe la Partie destinataire de toute condition de transmission ou de toute limite applicable à l'utilisation des Informations Classifiées.

Article 4

Protection des Informations Classifiées

1. Les Parties prennent toutes les mesures appropriées conformément à leurs lois et réglementations nationales afin de garantir que le niveau de protection accordé à l'Information Classifiée reçue est conforme au Niveau de classification de sécurité équivalent, tel qu'indiqué à l'article 3 du présent Accord.

2. Aucune disposition du présent Accord ne porte atteinte aux lois et aux réglementations nationales de Parties s'agissant des droits des personnes à obtenir l'accès aux

documents publics ou à des informations de caractère public, la protection de données personnelles ou la protection d'Informations Classifiées.

3. Conformément aux lois et aux réglementations nationales, chacune des Parties veillera à la mise en œuvre de mesures appropriées en vue de protéger des Informations Classifiées lors de leur traitement, stockage ou transmission via des systèmes de communication et d'information, tant que jugé nécessaire. Ces mesures devront garantir la confidentialité, l'intégrité, la disponibilité et, le cas échéant, le non-rejet et l'authenticité des Informations Classifiées ainsi qu'un niveau approprié de responsabilité et de traçabilité de toute action liée à ces informations.

Article 5

Divulgation et utilisation d'Informations Classifiées

1. Chaque Partie s'assure que les Informations Classifiées fournies ou échangées au titre du présent Accord ne sont pas :

- a) déclassées ou déclassifiées sans consentement écrit préalable de la Partie d'origine ;
- b) utilisées à d'autres fins que celles définies par la Partie d'origine ;
- c) divulguées à une Tierce Partie sans l'accord écrit préalable de la Partie d'origine, et qu'un accord ou un arrangement approprié pour la protection d'Informations Classifiées est en place avec la Tierce Partie concernée.

2. Chaque Partie, conformément à ses exigences constitutionnelles et à sa législation nationale, respecte le principe du consentement de la Partie d'origine.

Article 6

Accès aux Informations Classifiées

1. Chaque Partie s'assure que l'accès aux Informations Classifiées est accordé sur la base du principe du « Besoin de savoir ».

2. Chaque Partie s'assure que toutes les personnes qui se voient octroyer l'accès à des Informations Classifiées sont tenues informées de leurs responsabilités en matière de protection de telles informations, conformément aux réglementations relatives à la sécurité appropriées.

3. Les Parties s'assurent que l'accès aux Informations Classifiées est uniquement accordé aux personnes disposant d'une habilitation de sécurité individuelle adaptée ou aux personnes dûment autorisées en raison de leurs fonctions, conformément à la législation nationale.

4. En vertu de ses lois et réglementations nationales, chaque Partie s'assure que chaque entité relevant de sa juridiction susceptible de recevoir ou de générer des Informations

Classifiées dispose d'une habilitation de sécurité appropriée et est en mesure de fournir une protection adaptée, tel que mentionnée à l'article 4, paragraphe 1, du présent accord, au niveau de sécurité approprié.

Article 7

Traduction, reproduction et destruction d'Informations Classifiées

1. Toutes les traductions et reproductions d'Informations Classifiées comportent le Niveau de classification de sécurité approprié et les Parties les protègent et les contrôlent de la même manière que la version originale.
2. Toutes les traductions d'Informations Classifiées incluent une note appropriée, dans la langue de traduction, indiquant qu'elles contiennent des Informations Classifiées de la Partie d'origine.
3. Conformément à l'article 6, paragraphe 3, du présent accord, les traducteurs doivent disposer d'une habilitation de sécurité individuelle adaptée au niveau de confidentialité de l'Information Classifiée à traduire.
4. La traduction ou la reproduction d'Informations Classifiées Top secret (TRÈS SECRET LUX/ULTRASSECRETO) sont autorisées uniquement avec l'accord écrit de la Partie d'origine.
5. Les Informations Classifiées reçues au titre du présent Accord ne doivent pas être détruites. Lorsque la Partie destinataire ne les estime plus nécessaires, ces informations sont remises à la Partie d'origine.
6. La Partie destinataire ne doit pas reproduire des Informations Classifiées sans l'accord écrit préalable de la Partie d'origine.

Article 8

Échange entre les Parties

1. Les Informations Classifiées sont échangées entre les Parties par la voie diplomatique ou par toute autre voie autorisée par les Parties.
2. Les Informations Classifiées doivent être transmises par le biais de systèmes, de réseaux de communications protégés ou d'autres supports électromagnétiques approuvés par les deux Parties. Ces transmissions doivent être cryptées selon une méthode acceptée par les Autorités nationales de sécurité, conformément aux lois et aux réglementations nationales.
3. Les Informations Classifiées marquées Top secret (TRES SECRET LUX/ULTRASSECRETO) sont envoyées uniquement par la voie diplomatique.
4. Des Informations Classifiées désignées RESTREINT LUX/RESERVADO peuvent également être transmises par la voie postale ou un autre service de messagerie conformément aux lois et réglementations nationales.

5. Lorsque la transmission porte sur un envoi de grand volume qui comprend des Informations Classifiées, les procédures de ce transport sont convenues et appréciées, au cas par cas, par les Autorités de sécurité compétentes des deux Parties.

Article 9

Visites

1. Les visites d'établissements dans lesquels des Informations Classifiées sont traitées ou stockées sont soumises à l'autorisation préalable de l'Autorité nationale de sécurité de la Partie hôte, sauf accord contraire mutuel.

2. Toute demande de visite est remise à l'Autorité nationale de sécurité de la Partie hôte et inclut les données suivantes qui sont uniquement utilisées aux fins de la visite :

- a) nom, date et lieu de naissance, nationalité et numéro du passeport ou de la carte d'identité du visiteur ;
- b) qualité et fonction du visiteur, et nom et adresse de l'établissement qui l'emploie ;
- c) descriptif du projet auquel le visiteur participe ;
- d) validité et niveau de l'habilitation de sécurité du visiteur ;
- e) nom, adresse, numéro de téléphone, adresse électronique et personne de contact de l'établissement à visiter ;
- f) objectif de la visite, y compris établissements qu'il souhaite visiter et le plus haut niveau de classification de sécurité des Informations Classifiées concernées ;
- g) date et durée de la visite. Dans le cas de visites récurrentes, il convient d'indiquer la période totale couverte par les visites ;
- h) toute autre donnée, si convenue par les Autorités nationales de sécurité ;
et
- i) date et signature.

3. Toute demande de visite est remise au moins 30 (trente) jours avant la date de visite prévue, sauf accord contraire mutuel des autorités de sécurité compétentes.

4. Toute Information Classifiée remise à un visiteur est considérée comme une Information Classifiée reçue en vertu du présent Accord. Tous les visiteurs se conforment aux règles de sécurité de la Partie hôte.

5. Une Partie accorde une autorisation aux visiteurs d'une autre Partie, uniquement si ceux-ci :

- a) disposent d'une habilitation de sécurité individuelle octroyée par leur pays d'origine ; et
- b) sont autorisés à recevoir ou à avoir accès aux Informations Classifiées sur la base du principe du Besoin de savoir.

6. Une fois la visite autorisée, l'Autorité nationale de sécurité du pays hôte le notifie à l'Autorité nationale de sécurité du pays du visiteur au moins 10 (dix) jours avant la date prévue de la visite et fournit une copie de la demande à l'établissement objet de la visite.

7. Les Autorités de sécurité compétentes peuvent convenir d'établir une liste des visiteurs autorisés à effectuer des visites récurrentes. Cette liste est valable pour une première période maximale de 12 (douze) mois qui peut être prolongée pour une nouvelle période maximale de 12 (douze) mois. Toute demande de visites récurrentes est présentée conformément au paragraphe 3 du présent article. Une fois la liste approuvée, les visites peuvent être organisées directement par les établissements concernés.

Article 10

Contrats Classifiés en lien avec l'Accord

1. Dans le cas de Contrats Classifiés conclus et mis en œuvre sur le territoire d'une des Parties, l'Autorité nationale de sécurité ou l'Autorité de sécurité compétente de l'autre Partie obtient une garantie préalable écrite que le Contractant proposé détient une habilitation de sécurité d'installation et toutes les habilitations de sécurité individuelles nécessaires pour le niveau approprié

2. Le Contractant s'engage à :

- a) garantir que ses locaux disposent des conditions adéquates pour le Traitement d'Informations Classifiées ;
- b) disposer d'une Habilitation de sécurité d'installation ;
- c) garantir que toutes les personnes ayant accès aux Informations Classifiées disposent d'une Habilitation de sécurité individuelle et connaissent leur responsabilité s'agissant de leur protection, conformément aux lois et réglementations ;
- d) autoriser des inspections de sécurité de ses locaux.

3. Lors de toute attribution de marché, la Partie d'origine informe la Partie destinataire du niveau de sécurité des Informations Classifiées transférées.

4. Les Contrats Classifiés doivent également prévoir les conditions supplémentaires suivantes :

- a) responsabilité en cas de non-conformité avec les procédures et mesures de sécurité applicables aux Informations Classifiées ;
 - b) obligation d'informer de toute Infraction à la sécurité ou aux Informations Classifiées à son Autorité de sécurité compétente ;
 - c) responsabilité pour dommages résultant des infractions à la sécurité.
5. Tout sous-traitant doit satisfaire aux mêmes obligations de sécurité que celles du Contractant.

Article 11

Autorités nationales de sécurité et coopération en matière de sécurité

1. Les Autorités nationales de sécurité en charge de la mise en œuvre et de la supervision du présent Accord sont les suivantes :

Dans la République fédérative du Brésil :

Gabinete de Segurança Institucional da Presidência da República – GSI/PR
Autoridade Nacional de Segurança
(Autorité nationale de sécurité)

Au Grand-Duché de Luxembourg :

Service de renseignement de l'État
Autorité nationale de Sécurité
(Autorité nationale de sécurité)

2. Chacune des Parties communique par écrit, à l'autre Partie, les coordonnées de contact nécessaires de ses Autorités nationales de sécurité.
3. Les Autorités nationales de sécurité se tiennent mutuellement informées des lois et réglementations nationales en vigueur en matière de sécurité des Informations Classifiées.
4. Les Autorités nationales de sécurité se tiennent mutuellement informées de toute modification de cette législation ou concernant les Habilitations de sécurité des personnes, des agences et des entités.
5. En vue de garantir une étroite collaboration pendant la mise en œuvre du présent Accord, les Autorités nationales de sécurité peuvent être consultées dès lors que l'une d'entre elles en fait la demande.
6. Les représentants de l'Autorité nationale de sécurité d'une Partie peuvent visiter les établissements de l'Autorité nationale de sécurité d'une autre Partie dans le but d'obtenir des connaissances en matière de procédures et de mesures de sécurité applicables aux Informations Classifiées.

7. Les Parties, par le biais de leurs Autorités nationales de sécurité, se tiennent mutuellement informées, à temps, de toute modification de leur fonction ou de tout transfert de compétences vers une autre entité.
8. Sur demande, les Parties, par le biais de leurs Autorités nationales de sécurité, collaborent selon leurs lois et réglementations nationales dans le cadre des procédures nécessaires à l'obtention de l'Habilitation de sécurité individuelle des personnes qui ont vécu ou qui vivent sur le territoire de l'autre Partie.
9. Les Parties reconnaissent mutuellement les Habilitations de sécurité individuelles et Habilitations d'installation de l'autre Partie et se tiennent immédiatement informées de toute modification desdites Habilitations mutuellement reconnues.
10. En vue d'appliquer et de conserver des normes de sécurité similaires, et sur demande, les Autorités de sécurité compétentes se tiennent mutuellement informées des normes, procédures et pratiques de sécurité nationales qu'elles appliquent en matière de protection d'Informations Classifiées. Si nécessaire, les Autorités de sécurité compétentes peuvent effectuer des visites régulières.
11. Sur demande, les Parties fournissent une assistance mutuelle à la mise en œuvre des Habilitations de sécurité individuelles.

Article 12

Assistance aux procédures d'Habilitation de sécurité

1. Sur demande, les Autorités nationales de sécurité des Parties, en tenant compte de leurs lois et réglementations nationales respectives, s'entraident dans le cadre des procédures d'Habilitation de sécurité.
2. Les Parties reconnaissent les Habilitations de sécurité délivrées conformément aux lois et réglementations nationales de l'autre Partie.

Article 13

Infraction à la sécurité

1. Dans le cas d'une Infraction à la sécurité liée aux Informations Classifiées qui incluent les Parties au présent accord, l'Autorité nationale de sécurité de la Partie où l'Infraction à la sécurité se produit en informe immédiatement l'Autorité nationale de sécurité de l'autre Partie.
2. Dans le cas où une Infraction à la sécurité se produit au sein d'une Tierce partie, l'Autorité nationale de sécurité de la Partie d'origine en avise dès que possible l'Autorité nationale de sécurité de l'autre Partie et lance une enquête appropriée.
3. L'Autorité compétente concernée prendra toutes les mesures appropriées possibles, conformément à ses lois et réglementations nationales, afin de limiter les conséquences de toute infraction telle que définie au paragraphe 1 du présent article, ou d'empêcher toute violation ultérieure. Sur demande, l'autre Partie participe à l'enquête ; elle

est tenue informée du résultat de cette dernière et des mesures correctives entreprises à la suite de l'infraction.

4. La Partie au sein de laquelle se produit l'infraction à la sécurité effectue une enquête ou accompagne le processus d'enquête sur l'incident et, ensuite, informe immédiatement l'autre Partie des résultats de l'enquête et des mesures correctives appliquées.

5. Si nécessaire, l'autre Partie coopère à l'enquête.

Article 14

Frais

Chaque Partie assume les frais de la mise en œuvre et de la supervision de tous les aspects du présent Accord.

Article 15

Litiges

1. Tout éventuel litige entre les Parties s'agissant de l'interprétation ou de la mise en application du présent Accord ou de toute question y afférente est réglé par le biais de consultations et de négociations entre les Parties, par la voie diplomatique.

2. Lors de la phase de règlement du litige, les deux Parties continuent à remplir toutes leurs obligations au titre du présent Accord.

Article 16

Communications

Toutes les communications entre les Parties relatives à la mise en œuvre du présent accord ont lieu sous forme écrite et en anglais.

Article 17

Entrée en vigueur

Le présent Accord prend effet le premier jour du deuxième mois qui suit la réception de la dernière des notifications écrites par lesquelles les Parties se sont tenues mutuellement informées, par la voie diplomatique, de l'accomplissement des exigences légales internes requises pour son entrée en vigueur.

Article 18

Modifications

1. Le présent Accord peut être modifié à tout moment, par écrit, moyennant l'accord commun des Parties.
2. Ces modifications entrent en vigueur selon les termes de l'article 17 du présent Accord.

Article 19
Validité et dénonciation

1. Le présent Accord reste en vigueur pour une durée indéterminée.
2. Chacune des Parties peut, à tout moment, dénoncer le présent Accord moyennant une notification écrite.
3. La dénonciation doit être notifiée par voie diplomatique et prend effet 6 (six) mois à compter de la date de réception de l'avis de dénonciation par l'autre Partie.
4. Dans ce cas, toute Information Classifiée échangée dans le cadre du présent Accord reste protégée selon les dispositions y incluses, sauf si la Partie d'origine exempte la Partie destinataire de cette obligation.

Article 20
Dispositions finales


Les Parties se tiennent mutuellement informées sans délai de toute modification apportée à leurs lois ou réglementations nationales respectives, susceptible d'affecter la protection des Informations Classifiées délivrées en vertu du présent Accord. Dans le cas de telles modifications, les Parties se consultent en vue d'envisager d'éventuelles modifications du présent Accord. Entre-temps, les Informations Classifiées continuent d'être protégées conformément au présent Accord, sauf demande écrite contraire de la Partie d'origine.

Fait à New York, le 25 septembre 2018, en deux exemplaires, chacun en langues portugaise, française et anglaise, tous les textes faisant également foi. Dans le cas d'un désaccord quant à l'interprétation des dispositions du présent Accord, le texte anglais prévaut.

POUR LE GOUVERNEMENT DE LA
REPUBLICQUE FEDERATIVE DU BRESIL

POUR LE GOUVERNEMENT DU
GRAND-DUCHE DE LUXEMBOURG


Aloysio Nunes Ferreira
Ministre des Affaires étrangères


Jean Asselborn
Ministre des Affaires étrangères et
européennes