



ACORDO ENTRE A REPÚBLICA FEDERATIVA DO BRASIL E A REPÚBLICA DA ÍNDIA SOBRE A TROCA E A PROTEÇÃO MÚTUA DE INFORMAÇÃO CLASSIFICADA

A República Federativa do Brasil

e

A República da Índia,
Doravante conjuntamente denominadas as “Partes”, ou individualmente, como
“Parte”

No interesse da segurança nacional e com o objetivo de garantir a proteção das Informações Classificadas trocadas no âmbito de instrumentos de cooperação, contratos e outros acordos assinados entre as Partes, seus indivíduos, órgãos credenciados, bem como entidades públicas ou privadas;

Desejando estabelecer uma estrutura de regras e procedimentos relativos às Informações Classificadas de acordo com as leis e regulamentos nacionais das Partes;

Confirmando que este Acordo não afetará os compromissos de ambas as Partes que derivam de outros acordos internacionais e que não será utilizado contra os interesses, a segurança e a integridade territorial de outros Estados;

Acordaram o seguinte:

ARTIGO – I OBJETIVO

1. Este Acordo estabelece regras e procedimentos para a proteção de Informações Classificadas trocadas entre as Partes, seus indivíduos e órgãos credenciados, bem como entidades públicas ou privadas sob sua jurisdição.
2. Este Acordo não constitui uma base para obrigar a prestação ou troca de Informações Classificadas pelas Partes.



ARTIGO – II DEFINIÇÕES

Para os fins deste Acordo, o termo:

- a) **Acordo** significa este acordo incluindo seus Anexos;
- b) **Anexo** significa um anexo a este Acordo;
- c) **Contrato Classificado** significa um acordo, incluindo quaisquer negociações pré-contratuais, cuja execução requeira ou envolva acesso ou potencial acesso ou a criação de Informações Classificadas;
- d) **Informação Classificada** significa qualquer Informação, independentemente de sua forma, gerada por ou trocada entre as Partes que requeira proteção contra divulgação não autorizada e à qual tenha sido atribuída uma classificação de segurança de acordo com as leis e regulamentos nacionais das Partes;
- e) **Autoridade de Segurança Competente (ASC)** significa a autoridade de cada Parte responsável pela segurança das Informações Classificadas sob este Acordo;
- f) **Comprometimento da Informação** significa qualquer forma de uso indevido, dano ou acesso não autorizado, alteração, divulgação ou destruição de Informações Classificadas, bem como qualquer outra ação ou omissão que resulte na perda de sua confidencialidade, integridade, disponibilidade ou autenticidade;
- g) **Contratante** significa qualquer indivíduo ou entidade legal, incluindo subcontratantes, que tenha a capacidade legal para celebrar e executar contratos no escopo deste Acordo;
- h) **Autorização de Segurança da Instalação** significa a determinação pela Autoridade de Segurança Competente de que um Contratante, seja uma entidade pública ou privada, possui medidas de segurança adequadas e, portanto, foi credenciado para o Tratamento de Informações Classificadas, de acordo com as leis e regulamentos nacionais de cada Parte;

- i) **Tratamento de Informações Classificadas** significa um conjunto de ações relacionadas à produção, recepção, classificação, uso, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, descarte, destinação ou controle de Informações Classificadas em um determinado Nível de Classificação de Segurança;
- j) **Necessidade de Conhecer** significa o requisito para que um indivíduo acesse, tenha conhecimento ou posse de Informações Classificadas para o desempenho de funções e tarefas oficiais;
- k) **Parte Originária** significa a Parte sob cuja autoridade as Informações Classificadas foram criadas;
- l) **Credencial de Segurança Pessoal** significa a determinação de que um indivíduo específico foi autorizado em termos de segurança e, portanto, credenciado para o Tratamento de Informações Classificadas em um determinado Nível de Classificação de Segurança, de acordo com as leis e regulamentos nacionais de cada Parte;
- m) **Entidade Provedora** significa a Parte que fornece Informações Classificadas para a Entidade Receptora sob este Acordo;
- n) **Entidade Receptora** significa a Parte que recebe Informações Classificadas da Entidade Provedora sob este Acordo;
- o) **Violação de Segurança** significa qualquer ação ou omissão intencional ou acidental que resulte em comprometimento ou perda real ou possível de Informações Classificadas fornecidas ou geradas sob este Acordo;
- p) **Nível de Classificação de Segurança** significa o nível de proteção atribuído a Informações Classificadas, de acordo com as leis e regulamentos nacionais de cada Parte e conforme incorporado no Artigo - IV, Parágrafo 1 deste Acordo;
- q) **Terceiro** significa qualquer organização, entidade governamental estatal ou indivíduo que não seja uma das Partes deste Acordo;
- r) **Proteção de Informações Classificadas** significa a adoção de medidas legais, organizacionais, técnicas e outras para prevenir a divulgação não autorizada de

Informações Classificadas de acordo com a legislação nacional das Partes e sob este Acordo; e

- s) **Acesso a Informações Classificadas** significa a familiarização e/ou trabalho de um indivíduo com Informações Classificadas, realizado de acordo com a legislação nacional das Partes.

ARTIGO – III AUTORIDADES DE SEGURANÇA COMPETENTES

1. As Autoridades de Segurança Competentes, responsáveis pela implementação e supervisão deste Acordo, estão listadas no Anexo deste Acordo.
2. A Autoridade de Segurança Competente pode delegar partes de suas responsabilidades a uma Autoridade de Segurança Competente delegada.
3. Cada Parte fornecerá à outra os dados de contato de sua respectiva Autoridade de Segurança Competente por escrito. As Autoridades de Segurança Competentes das Partes deverão informar-se mutuamente por escrito sobre alterações em seus dados de contato.
4. Para assegurar uma cooperação próxima na implementação deste Acordo, as Autoridades de Segurança Competentes poderão consultar-se sempre que necessário.
5. Representantes de ambas as Autoridades de Segurança Competentes poderão visitar mutuamente as instalações com o intuito de adquirir conhecimento dos procedimentos e medidas de segurança aplicáveis às Informações Classificadas, sujeito à aprovação da Autoridade de Segurança Competente anfitriã.
6. Mediante solicitação, as Autoridades de Segurança Competentes poderão auxiliar-se mutuamente na realização dos procedimentos para a concessão de Autorizações de Segurança da Instalação e de Credenciais de Segurança Pessoal, a pedido e de acordo com suas leis e regulamentos nacionais.
7. A pedido da Autoridade de Segurança Competente de uma Parte, a Autoridade de Segurança Competente da outra Parte emitirá uma confirmação por escrito de que uma Credencial de Segurança Pessoal e/ou Autorização de Instalação válida foi emitida.

8. As Autoridades de Segurança Competentes das Partes deverão reconhecer mutuamente suas Credenciais de Segurança Pessoal e Autorizações de Segurança de Instalação emitidas de acordo com suas respectivas leis e regulamentos e dentro do escopo deste Acordo.

9. As Autoridades de Segurança Competentes deverão notificar-se mutuamente prontamente por escrito sobre alterações nas Credenciais de Segurança Pessoal e Autorizações de Segurança de Instalação reconhecidas, para as quais uma confirmação tenha sido fornecida conforme o Parágrafo 8 deste artigo.

ARTIGO – IV NÍVEIS DE CLASSIFICAÇÃO DE SEGURANÇA

1. As Partes concordam que os Níveis de Classificação de Segurança, de acordo com suas respectivas leis e regulamentos nacionais, devem corresponder entre si na seguinte forma de equivalência:

República Federativa do Brasil	भारत गणराज्य (República da Índia)	Tradução em Inglês
ULTRASSECRETO	परम गुप्त	TOP SECRET
SECRETO	गुप्त	SECRET
RESERVADO	गोपनीय	CONFIDENTIAL

2. Qualquer Informação Classificada, produzida de acordo com este Acordo, deverá ser marcada com o Nível de Classificação de Segurança equivalente da Parte Originária, conforme o Parágrafo 1 deste artigo.

3. A Entidade Receptora deverá marcar todas as Informações Classificadas sob este Acordo que tenha recebido da Entidade Provedora com o Nível de Classificação de Segurança equivalente da Entidade Receptora, de acordo com o Parágrafo 1 deste artigo. O Nível de Classificação de Segurança da Parte Originária deverá ser indicado primeiro, para determinar o equivalente apropriado de Nível de Classificação de Segurança.

4. As Partes deverão notificar-se mutuamente sobre qualquer alteração e emenda subsequente ao Nível de Classificação de Segurança das Informações Classificadas.

5. A Parte Originária poderá marcar as Informações Classificadas com requisitos de tratamento para especificar qualquer limitação quanto ao seu uso, divulgação, liberação e acesso pela Entidade Receptora.



6. A Entidade Receptora não poderá modificar ou revogar a classificação de segurança das Informações Classificadas recebidas ou geradas sob este Acordo sem a aprovação prévia por escrito da Parte Originária.

7. Informações Classificadas originadas conjuntamente pelas Partes serão atribuídas a um Nível de Classificação de Segurança mutuamente determinado pelas Partes.

ARTIGO – V

PROTEÇÃO DE INFORMAÇÕES CLASSIFICADAS

1. As Partes tomarão todas as medidas adequadas de acordo com suas leis e regulamentos nacionais para garantir a proteção das Informações Classificadas de acordo com este Acordo. Conferirão às Informações Classificadas trocadas ou geradas sob este Acordo pelo menos o mesmo nível de proteção que conferem às suas próprias Informações Classificadas no Nível de Classificação de Segurança correspondente.

2. O Tratamento de qualquer Informação Classificada trocada entre as Partes respeitará as disposições deste Acordo.

3. Cada Parte garantirá que as medidas necessárias sejam implementadas para proteger as Informações Classificadas processadas, armazenadas ou transmitidas por sistemas de comunicação e informação, de acordo com o Nível de Classificação de Segurança, com este Acordo e com as leis e regulamentos nacionais.

4. Cada Parte garantirá a confidencialidade, integridade, disponibilidade e, quando aplicável, a não-repudição, autenticidade, responsabilidade e rastreabilidade das Informações Classificadas.

5. As Partes não divulgarão qualquer Informação Classificada sem o consentimento por escrito da Parte Originária.

ARTIGO – VI

USO DE INFORMAÇÕES CLASSIFICADAS

1. Cada Parte garantirá que a Entidade Provedora:



- a) marque as Informações Classificadas com a classificação de segurança apropriada, de acordo com suas leis e regulamentos nacionais; e
- b) informe a Entidade Receptora sobre quaisquer condições de liberação ou limitações quanto ao uso das Informações Classificadas fornecidas, conforme determinado pela Parte Originária.

2. Cada Parte garantirá que a Entidade Receptora:

- a) conceda o mesmo nível de proteção às Informações Classificadas que concede às suas próprias Informações Classificadas de Nível de Classificação de Segurança equivalente, conforme determinado no Artigo - IV, Parágrafo 1;
- b) não desclassifique ou rebaixe as Informações Classificadas sem o consentimento prévio por escrito da Parte Originária;
- c) não divulgue Informações Classificadas a um Terceiro sem o consentimento prévio por escrito da Parte Originárias; e
- d) utilize as Informações Classificadas apenas para os fins para os quais foram liberadas e de acordo com os requisitos de tratamento da Parte Originária.

3. Cada Parte, de acordo com seus requisitos constitucionais, leis e regulamentos nacionais, respeitará o princípio do consentimento de origem.

ARTIGO – VII

ACESSO A INFORMAÇÕES CLASSIFICADAS

1. Cada Parte garantirá que o acesso a Informações Classificadas seja concedido com base na Necessidade de Conhecer.

2. Cada Parte garantirá que qualquer indivíduo que tenha acesso a Informações Classificadas esteja ciente de suas responsabilidades de proteger tais informações e tenha assinado uma declaração de confidencialidade de acordo com as leis e regulamentos nacionais da Entidade Receptora.



3. As Partes garantirão que o acesso a Informações Classificadas seja concedido apenas a indivíduos que possuam uma Credencial de Segurança Pessoal no nível correspondente ou que estejam devidamente autorizados a acessar Informações Classificadas em razão de suas funções, conforme as leis e regulamentos nacionais da Entidade Receptora.
4. Cada Parte garantirá que qualquer entidade sob sua jurisdição que possa receber ou gerar Informações Classificadas possua autorização de segurança.

ARTIGO – VIII

TRADUÇÃO, REPRODUÇÃO E DESTRUIÇÃO DE INFORMAÇÕES CLASSIFICADAS

1. Todas as traduções e reproduções de Informações Classificadas devem ser protegidas e controladas da mesma forma que as Informações Classificadas originais, recebendo o mesmo Nível de Classificação de Segurança que as Informações Classificadas originais.
2. Traduções de Informações Classificadas devem conter uma anotação adequada no idioma da tradução, indicando que contêm Informações Classificadas da Parte Originária.
3. O número de reproduções de Informações Classificadas deve ser limitado à quantidade necessária para o propósito oficial.
4. Informações Classificadas com Nível de Classificação de Segurança equivalente a ULTRASSECRETO/परम गुप्त/TOP SECRET não devem ser reproduzidas ou traduzidas sem o consentimento prévio por escrito da Parte Originária.
5. Informações Classificadas com Nível de Classificação de Segurança equivalente a ULTRASSECRETO/परम गुप्त/TOP SECRET não devem ser destruídas sem o consentimento prévio por escrito da Parte Originária. Elas devem ser devolvidas à Parte Originária quando não forem mais consideradas necessárias pela Entidade Receptora.
6. Informações Classificadas com Nível de Classificação de Segurança equivalente a SECRETO/गुप्त/SECRET devem ser destruídas de acordo com as leis, regras e regulamentos nacionais após não serem mais consideradas necessárias pela Entidade Receptora.
7. Se uma situação de crise tornar impossível para a Entidade Receptora proteger as Informações Classificadas fornecidas sob este Acordo, as Informações Classificadas deverão ser destruídas imediatamente. A Entidade Receptora deverá notificar prontamente por escrito a

Autoridade de Segurança Competente da Parte Originária sobre a destruição dessas Informações Classificadas.

ARTIGO – IX

TRANSMISSÃO DE INFORMAÇÕES CLASSIFICADAS

1. Informações Classificadas com Nível de Classificação de Segurança ULTRASSECRETO/परम गुप्त/TOP SECRET e SECRETO/गुप्त/SECRET deverão ser transmitidas entre as Partes por canais diplomáticos, garantindo sua proteção contra divulgação não autorizada ou conforme acordado por escrito pelas respectivas Autoridades de Segurança Competentes.
2. Níveis de Classificação de Segurança não incluídos no Parágrafo 1 deverão ser transmitidos de acordo com as leis e regulamentos nacionais da Parte Originária.
3. Informações Classificadas transmitidas por sistemas de comunicação, redes ou outros meios eletromagnéticos devem utilizar meios criptografados mutuamente aceitos pelas respectivas Autoridades de Segurança Competentes.
4. No caso de transmissão de Informações Classificadas que exijam procedimentos especiais para seu transporte, um plano logístico deve ser previamente acordado por escrito pelas Autoridades de Segurança Competentes.

ARTIGO – X

VISITAS

1. As visitas de representantes de uma das Partes a instalações seguras onde Informações Classificadas serão acessadas, processadas ou registradas estão sujeitas à aprovação prévia por escrito da Autoridade de Segurança Competente da Parte anfitriã, a menos que acordado de outra forma pelas Autoridades de Segurança Competentes. Tal aprovação só será concedida a indivíduos que atendam aos requisitos estabelecidos no Artigo - VII deste Acordo.
2. A solicitação deve ser submetida à Autoridade de Segurança Competente da Parte anfitriã, incluindo os seguintes dados, que serão utilizados apenas para fins da visita:
 - a) o nome completo, data e local de nascimento, nacionalidade, outras cidadanias e número da carteira de identidade/passaporte;



- b) cargo oficial, título e função, bem como o nome e endereço da organização pelo qual o visitante é empregado ou que ele representa;
- c) a especificação do projeto no qual o visitante está participando;
- d) a confirmação da Credencial de Segurança Pessoal do visitante, seu nível e validade;
- e) o nome da instalação a ser visitada;
- f) o propósito da visita;
- g) o Nível de Classificação de Segurança mais alto previsto das Informações Classificadas a serem acessadas, processadas ou armazenadas;
- h) o nome, endereço, número de telefone, endereço de e-mail e ponto de contato da instalação a ser visitada;
- i) a data e a duração da visita;
- j) o período total, quando as visitas forem recorrentes; e
- k) a data e assinatura de um representante da Autoridade de Segurança Competente do visitante.

3. O pedido de visita deve ser submetido, no mínimo, 21 (vinte e um) dias corridos antes da data proposta para a visita, a menos que as Autoridades de Segurança Competentes concordem em um período diferente.

4. As Autoridades de Segurança Competentes podem acordar uma lista de visitantes autorizados a visitas recorrentes por um período não superior a 12 (doze) meses. As Autoridades de Segurança Competentes deverão acordar mais detalhes sobre essas visitas recorrentes.

5. A Autoridade de Segurança Competente da Parte anfitriã deverá informar os responsáveis pela segurança da organização a ser visitada sobre os detalhes dos indivíduos cujos pedidos de visita foram aprovados. Uma vez concedida a aprovação, os arranjos de visita para

indivíduos com aprovação para visitas recorrentes podem ser feitos diretamente com a agência, instalação ou organização em questão.

6. Qualquer Informação Classificada transmitida ao visitante oficial será considerada Informação Classificada sob este Acordo e deverá ser tratada de acordo com as disposições deste Acordo. Além disso, o visitante oficial deve cumprir os regulamentos de segurança da Parte anfitriã.

7. As Partes garantirão, conforme suas leis e regulamentos nacionais, a proteção dos dados pessoais dos indivíduos solicitando uma visita. Os dados pessoais não devem ser utilizados para nenhum outro propósito além de determinar a solicitação de visita.

8. Quando autorizado, a Autoridade de Segurança Competente da Parte anfitriã deverá notificar a Parte solicitante, o mais breve possível, sobre a visita e também notificar a instalação a ser visitada.

ARTIGO – XI VIOLAÇÃO DE SEGURANÇA

1. Quando uma Violação de Segurança relacionada a Informações Classificadas sob este Acordo for suspeitada ou constatada pela Entidade Receptora, a Autoridade de Segurança Competente da Parte onde ocorreu a Violação de Segurança deverá imediatamente informar a Autoridade de Segurança Competente da outra Parte. A notificação deve conter detalhes suficientes para que a Parte Originária avalie as consequências e circunstâncias da Violação de Segurança suspeitada ou constatada.

2. A Autoridade de Segurança Competente da Parte onde ocorreu a Violação de Segurança deverá imediatamente tomar todas as medidas necessárias, conforme suas leis e regulamentos nacionais, para investigar qualquer Violação de Segurança suspeita ou constatada. A Autoridade de Segurança Competente da Parte Originária poderá, se acordado, cooperar na investigação. A Parte Originária será sempre informada sobre o resultado da investigação e as medidas tomadas, se houver.

3. A Autoridade de Segurança Competente da Parte onde ocorreu a Violação de Segurança tomará todas as medidas, incluindo, mas não se limitando, a medidas legais, de acordo com suas leis e regulamentos nacionais, para mitigar as consequências de uma Violação de Segurança e evitar qualquer recorrência.

4. Quando uma Violação de Segurança ocorrer em um Terceiro, a Autoridade de Segurança Competente da Parte que transmitiu a informação ao Terceiro deverá imediatamente informar a Autoridade de Segurança Competente da Parte Originária sobre a Violação de Segurança e garantir que a Violação de Segurança seja devidamente investigada, comunicando o resultado da investigação e quaisquer medidas tomadas.

5. Qualquer Parte poderá solicitar informações sobre o processo de investigação da Violação de Segurança.

ARTIGO – XII

CONTRATOS CLASSIFICADOS

1. Se uma Parte ou um Contratante, incluindo um Subcontratante, propuser a concessão de um Contrato Classificado com um Contratante sob a jurisdição da outra Parte, deve primeiro obter a confirmação por escrito da Autoridade de Segurança Competente da outra Parte de que o Contratante possui uma Autorização de Segurança de Instalação no Nível de Classificação de Segurança apropriado.

2. A Autoridade de Segurança Competente da Parte onde o Contrato Classificado é executado deverá garantir que o Contratante e, se aplicável, o subcontratante:

- a) garantam que todos os indivíduos com acesso a Informações Classificadas estejam informados sobre suas responsabilidades de proteger essas informações de acordo com as condições definidas neste Acordo e com as leis e regulamentos nacionais;
- b) monitorem a conduta de segurança dentro de suas instalações, de acordo com as leis e regulamentos nacionais;
- c) notifiquem prontamente sua Autoridade de Segurança Competente sobre qualquer incidente de segurança relacionado aos Contratos Classificados; e
- d) possuam uma Autorização de Segurança de Instalação apropriada para proteger as Informações Classificadas e que os indivíduos que necessitem de acesso a Informações Classificadas possuam uma Credencial de Segurança Pessoal apropriada.

3. Todo Contrato Classificado, incluindo subcontratos classificados concluídos de acordo com este Acordo, deverá incluir requisitos de segurança que identifiquem os seguintes aspectos:

- a) um guia de classificação de segurança, que deverá sempre incluir a tabela do Artigo - IV, Parágrafo 1, especificando os Níveis de Classificação de Segurança aplicáveis a cada parte do Contrato Classificado;
- b) um procedimento para a comunicação de mudanças no Nível de Classificação de Segurança;
- c) os canais e procedimentos a serem usados para o transporte e/ou transmissão de Informações Classificadas;
- d) instruções para o tratamento e armazenamento de Informações Classificadas;
- e) dados de contato das Informações Classificadas relacionadas ao Contrato Classificado; e
- f) obrigação de notificar qualquer Violação de Segurança.

4. A Autoridade de Segurança Competente da Parte que autoriza a concessão do Contrato Classificado deverá encaminhar uma cópia do capítulo de requisitos de segurança à Autoridade de Segurança Competente da Entidade Receptora para facilitar a supervisão de segurança do Contrato Classificado.

ARTIGO – XIII CUSTOS

Cada Parte arcará com os custos de suas próprias despesas resultantes da implementação e supervisão de todos os aspectos deste Acordo, salvo disposição em contrário mutuamente determinada pelas Partes.

ARTIGO – XIV
RESOLUÇÃO DE DISPUTAS

1. Qualquer disputa entre as Partes decorrente da interpretação, implementação ou aplicação deste Acordo, ou de qualquer questão relacionada, será resolvida amigavelmente, exclusivamente por meio de consultas e negociações entre as Partes, e não será encaminhada a qualquer tribunal internacional ou Terceiro para resolução.
2. Durante o período de resolução de disputas, ambas as Partes continuarão a cumprir suas obrigações sob este Acordo.
3. Os procedimentos de resolução de disputas entre ambas as Partes serão conduzidos com base no princípio da confidencialidade.

ARTIGO – XV
COMUNICAÇÃO

Todas as comunicações formais entre as Partes relativas à implementação deste Acordo deverão ser feitas por escrito, em língua Inglesa.

ARTIGO – XVI
ENTRADA EM VIGOR

Este Acordo entrará em vigor no primeiro dia do segundo mês seguinte ao recebimento da última notificação, através da qual as Partes informarão uma à outra, por canais diplomáticos, que os requisitos legais internos necessários para sua entrada em vigor foram concluídos.

ARTIGO – XVII
EMENDAS

1. Este Acordo, incluindo seu Anexo, poderá ser alterado a qualquer momento, por escrito, por meio de emendas e com o consentimento mútuo entre as Partes. As emendas devem ser propostas por meio de canais diplomáticos.
2. As emendas entrarão em vigor nos termos estabelecidos no Artigo - XVI deste Acordo, com exceção das emendas do Anexo, que entrarão em vigor em uma data a ser acordada pelas Partes.

ARTIGO – XVIII
VIGÊNCIA E RESCISÃO

1. Este Acordo permanecerá em vigor por um período de 10 (dez) anos e será renovado por consentimento tácito por novos períodos de 5 (cinco) anos, a menos que uma das Partes Contratantes notifique a outra de sua intenção de não renová-lo, por escrito, com 6 (seis) meses de antecedência em relação ao término do período de validade atual.
2. Qualquer uma das Partes pode, a qualquer momento, rescindir este Acordo mediante notificação por escrito, através de canais diplomáticos, à outra Parte.
3. A rescisão entrará em vigor 6 (seis) meses após a data em que a outra Parte receber a notificação de rescisão.
4. Após a rescisão, qualquer Informação Classificada trocada, liberada ou gerada sob este Acordo continuará a ser protegida de acordo com os termos deste Acordo antes de sua rescisão, enquanto a Informação Classificada permanecer classificada.

ARTIGO – XIX
DISPOSIÇÕES FINAIS

A Autoridade de Segurança Competente informará mutuamente sobre suas respectivas leis, normas e regulamentos nacionais e notificará prontamente uma à outra sobre modificações que afetem a proteção de Informações Classificadas fornecidas sob este Acordo e

ANEXO

As Autoridades de Segurança Competentes, responsáveis pela implementação e supervisão deste Acordo, são:

a) Em nome da República da Índia —

Ministério do Interior e Ministério da Defesa da República da Índia;

b) Em nome da República Federativa do Brasil —

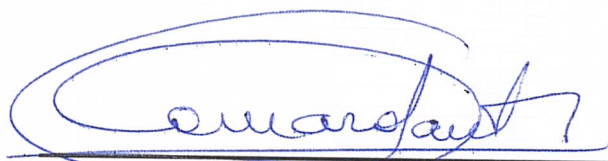
O Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil.

tenham impacto sobre o Acordo. Em caso de tais mudanças, as Partes deverão discutir a necessidade de revisar este Acordo.

EM TESTEMUNHO DISSO, os abaixo-assinados, devidamente autorizados por seus respectivos Governos, assinaram este Acordo.

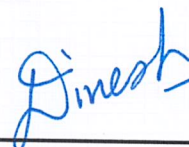
FEITO em Brasília, em 9 de julho de 2025, em duas cópias originais, cada uma nos idiomas Português, Hindi e Inglês, sendo todos os textos igualmente autênticos. Em caso de divergências de interpretação, o texto em Inglês prevalecerá.

PELA REPÚBLICA FEDERATIVA DO BRASIL

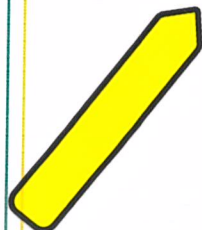


Marcos Antonio Amaro dos Santos
Ministro-Chefe do Gabinete de Segurança
Institucional da Presidência da República
Federativa do Brasil

PELA REPÚBLICA DA ÍNDIA



Dinesh Bhatia
Embaixador da Índia no Brasil



**AGREEMENT BETWEEN THE FEDERATIVE REPUBLIC OF BRAZIL AND THE REPUBLIC OF INDIA
ON THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION**

The Federative Republic of Brazil

and

The Republic of India,

Hereinafter jointly referred to as the "Parties", or individually, as a "Party"

In the interest of national security and for the purpose of ensuring the protection of Classified Information exchanged within the scope of cooperation instruments, contracts and other agreements signed between the Parties, their accredited individuals, bodies;

Desiring to establish a framework of rules and procedures related to Classified Information in accordance with national laws and regulations of the Parties;

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

Have agreed as follows:

**ARTICLE – I
PURPOSE**

1. This Agreement establishes rules and procedures for the protection of Classified Information exchanged between the Parties, their accredited individuals and bodies under their jurisdiction.
2. This Agreement does not constitute a basis to compel the provision or exchange of Classified Information by the Parties.

ARTICLE – II DEFINITIONS

For the purpose of this Agreement, the term:

- a) **Agreement** means this agreement including its Annexes;
- b) **Annex** means an attachment to this Agreement;
- c) **Classified Contract** means an agreement, including any pre-contractual negotiations, the performance of which requires or involves access or potential access to or the creation of Classified Information;
- d) **Classified Information** means any Information, regardless of its form, generated by or exchanged between the Parties which requires protection against unauthorized disclosure and to which a security classification has been assigned in accordance with the national laws and regulations of the Parties;
- e) **Competent Security Authority (CSA)** means the authority of each Party responsible for the security of Classified Information under this Agreement;
- f) **Information Compromise** means any form of misuse, damage or unauthorized access, alteration, disclosure or destruction of Classified Information, as well as any other action or non-action that results in the loss of its confidentiality, integrity, availability or authenticity;
- g) **Contractor** means an individual or an entity including sub-contractors, having the legal capacity to enter into and perform contracts within the scope of this Agreement;
- h) **Facility Security Clearance (FSC)** means the determination by the Competent Security Authority that a Contractor has in place appropriate security measures and has therefore been accredited for the Handling of Classified Information, in accordance with the national laws and regulations of each Party;
- i) **Handling of Classified Information** means a set of actions related to the production, reception, classification, use, access, reproduction, transport, transmission, distribution, archiving, storage, disposal, destination or control of Classified Information at a certain Security Classification Level;

- j) **Need-to-Know** means the requirement for an individual to access, have knowledge of or possess Classified Information for the performance of official functions and tasks;
- k) **Originating Party** means the Party under whose authority Classified Information has been created;
- l) **Personnel Security Clearance (PSC)** means the determination that a given individual has been security cleared and has therefore been accredited for the Handling of Classified Information, at a given Security Classification Level, in accordance with national laws and regulations of each Party;
- m) **Providing Entity** means the Party which provides Classified Information to the Receiving Entity;
- n) **Receiving Entity** means the Party which receives Classified Information from the Providing Entity;
- o) **Security Breach** means any intentional or accidental action or omission that results in an actual or possible compromise or loss of Classified Information provided or generated under this Agreement;
- p) **Security Classification Level** means the level of protection assigned to Classified Information, in accordance with the national laws and regulations of each Party and as incorporated in Article - IV, Paragraph 1 of this Agreement;
- q) **Third Party** means any organization, state government entity or individual which is not a Party to this Agreement;
- r) **Protection of Classified Information** means taking legal, organizational, technical and other measures on prevention of unauthorized disclosure of Classified Information in accordance with the national legislation of the Parties and under this Agreement; and
- s) **Access to Classified Information** means the familiarization and/or work of an individual with Classified Information carried out in accordance with the national legislation of the Parties.

ARTICLE – III
COMPETENT SECURITY AUTHORITIES

1. The Competent Security Authorities, responsible for the implementation and supervision of this Agreement, are listed in the Annex to this Agreement.
2. The Competent Security Authority may delegate parts of its responsibilities to a delegated Competent Security Authority.
3. Each Party shall provide the other with the contact details of their respective Competent Security Authority in writing. The Competent Security Authorities of the Parties shall inform each other in writing about changes in their contact details.
4. In order to ensure close cooperation in the implementation of this Agreement, the Competent Security Authorities may consult each other whenever necessary.
5. Representatives of both Competent Security Authorities may mutually visit the facilities with the intention of acquiring knowledge of security procedures and measures applicable to Classified Information, subject to the approval of the host Competent Security Authority.
6. Upon request, the Competent Security Authorities may assist each other in carrying out the procedures for the award of Facility Security Clearances and Personnel Security Clearances, on request and in accordance with their national laws and regulations.
7. Upon request of the Competent Security Authority of one Party, the Competent Security Authority of the other Party shall issue a written confirmation that a valid Personnel Security Clearance and/or Facility Clearance has been issued.
8. The Competent Security Authorities of the Parties shall mutually recognize their Personnel Security Clearances and Facility Security Clearances issued in accordance with their respective laws and regulations and within the scope of this Agreement.
9. The Competent Security Authorities shall promptly notify each other in writing about changes in recognized Personnel Security Clearances and Facility Security Clearances for whom or for which a confirmation has been provided according to Paragraph 8 of this Article.

ARTICLE – IV
SECURITY CLASSIFICATION LEVELS

1. The Parties agree that the Security Classification Levels, in accordance with their respective national laws and regulations, shall correspond to each other in the following form of equivalence:

Federative Republic of Brazil	भारत गणराज्य (Republic of India)	English Translation
ULTRASSECRETO	परम गुप्त	TOP SECRET
SECRETO	गुप्त	SECRET
RESERVADO	गोपनीय	CONFIDENTIAL

2. Any Classified Information produced pursuant to this Agreement shall be marked with the Originating Party's equivalent Security Classification Level in accordance with Paragraph 1 of this Article.

3. The Receiving Entity shall mark all the Classified Information under this Agreement that it has received from the Providing Entity with the equivalent Security Classification Level of the Receiving Entity in accordance with Paragraph 1 of this Article. The Security Classification Level of the Originating Party shall be indicated first, in order to determine the proper equivalent Security Classification Level.

4. The Parties shall notify each other of any change and subsequent amendment to the Security Classification Level of Classified Information.

5. The Originating Party may mark the Classified Information with handling requirements to specify any limitation on its use, disclosure, release and access by the Receiving Entity.

6. The Receiving Entity shall not modify or revoke the security classification of received or generated Classified Information under this Agreement without the prior written approval of the Originating Party.

7. Classified Information jointly originated by the Parties shall be assigned a Security Classification Level that is mutually determined by the Parties.

ARTICLE – V
PROTECTION OF CLASSIFIED INFORMATION

1. The Parties shall take all appropriate measures under their national laws and regulations to ensure the protection of Classified Information in accordance with this Agreement. They shall accord Classified Information exchanged or generated under this Agreement at least the same protection as they accord to their own Classified Information at the corresponding Security Classification Level.
2. The Treatment of any Classified Information exchanged between the Parties shall respect the provisions of this Agreement.
3. Each Party shall ensure that necessary measures are implemented for the protection of Classified Information processed, stored or transmitted by communication and information systems, in accordance with the Security Classification Level, with this Agreement, and with national laws and regulations.
4. Each Party shall ensure the confidentiality, integrity, availability and, where applicable, non-repudiation, authenticity, accountability and traceability of Classified Information.
5. The Parties shall not disclose any Classified Information without the Originating Party's written consent.

ARTICLE – VI
USE OF CLASSIFIED INFORMATION

1. Each Party shall ensure that the Providing Entity:
 - a) marks Classified Information with the appropriate security classification in accordance with its national laws and regulations; and
 - b) informs the Receiving Entity of any conditions of release or limitations on the use of the Classified Information provided, as determined by the Originating Party.
2. Each Party shall ensure that the Receiving Entity:

- 
- a) affords the same level of protection to the Classified Information as afforded to its national Classified Information of an equivalent Security Classification Level as determined in Article - IV, Paragraph 1;
 - b) shall not declassify or downgrade Classified Information without the prior written consent of the Originating Party;
 - c) shall not disclose Classified Information to a Third Party without prior written consent of the Originating Party; and
 - d) shall use Classified Information only for the purposes that it has been released for and in accordance with any handling requirements of the Originating Party.
3. Each Party, in accordance with its constitutional requirements, national laws and regulations, shall respect the principle of consent of origin.

ARTICLE – VII

ACCESS TO CLASSIFIED INFORMATION

1. Each Party shall ensure that access to Classified Information is granted on a Need-to-know basis.
2. Each Party shall ensure that any individual who has been granted access to Classified Information is informed of its responsibilities to protect such information and has signed a statement of confidentiality in accordance with national laws and regulations of the Receiving Entity.
3. The Parties shall ensure that access to Classified Information is granted only to individuals who hold a Personnel Security Clearance at the corresponding level or who are duly authorized to access Classified Information by virtue of their duties pursuant to national laws and regulations of the Receiving Entity.
4. Each Party shall ensure that any entity under its jurisdiction that may receive or generate Classified Information should be security cleared.



ARTICLE – VIII

TRANSLATION, REPRODUCTION AND DESTRUCTION OF CLASSIFIED INFORMATION

1. All translations and reproductions of Classified Information must be protected and controlled in the same manner as the original Classified Information. It shall receive the same Security Classification Level as the original Classified Information.
2. Translations of Classified Information shall contain a suitable annotation in the language of translation, indicating that they contain Classified Information of the Originating Party.
3. The number of reproductions of Classified Information shall be limited to the amount required for its official purpose.
4. Classified Information with Security Classification Level equivalent to ULTRASSECRETO/परम गुप्त/TOP SECRET shall not be reproduced or translated without the prior written consent of the Originating Party.
5. Classified Information with Security Classification Level equivalent to ULTRASSECRETO/परम गुप्त/TOP SECRET shall not be destroyed without the prior written consent of the Originating Party. It shall be returned to the Originating Party after it is no longer considered necessary by the Receiving Entity.
6. Classified Information with Security Classification Level equivalent to SECRETO/गुप्त/SECRET shall be destroyed in accordance with national laws, rules and regulations after it is no longer considered necessary by the Receiving Entity.
7. If a crisis situation makes it impossible for the Receiving Entity to protect Classified Information provided under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Entity shall promptly notify in writing the Competent Security Authority of the Originating Party about the destruction of this Classified Information.

ARTICLE – IX

TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information with Security Classification Level ULTRASSECRETO/ परम गुप्त/TOP SECRET and SECRETO/गुप्त/SECRET shall be transmitted between the Parties, through diplomatic channels, ensuring its protection against unauthorized disclosure or as agreed in writing by the respective Competent Security Authorities.

2. Security Classification Levels that are not included in Paragraph 1 shall be transmitted in accordance with national laws and regulations of the Originating Party.

3. Classified Information transmitted through communication systems, networks or other electromagnetic medium must use encrypted means mutually accepted by the respective Competent Security Authorities.

4. In the event of transmission of Classified Information that requires special procedures for its transport, a logistic plan must be previously agreed, in writing, by both Competent Security Authorities.

ARTICLE – X VISITS

1. Visits of representatives of either Party to secure facilities where Classified Information will be accessed, processed or recorded are subject to prior written approval of the Competent Security Authority of the host Party, unless otherwise agreed by the Competent Security Authorities. Such approval will only be granted to individuals who meet the requirements set forth in Article - VII of this Agreement.

2. The request must be submitted to the Competent Security Authority of the host Party, including the following data that will be used only for the purpose of the visit:

- a) first and last name, date and place of birth, nationality, other citizenships and identification card number/passport number;
- b) official position and function, as well as the name and address of the organization by whom the visitor is employed or that the visitor represents;
- c) the specification of the project in which the visitor is participating;
- d) the confirmation of the visitor's Personnel Security Clearance and its level and validity;
- e) the name of the facility to be visited;
- f) the purpose of the visit;
- g) the anticipated highest Security Classification Level of the Classified Information to be accessed, processed or stored;

- 
- h) the name, address, phone number, e-mail address and point of contact of the facility to be visited;
 - i) the date and duration of the visit;
 - j) the total period, when visits are recurring; and
 - k) the date and signature of a representative of the visitor's Competent Security Authority.

3. The visit request must be submitted, at least, 21 (twenty one) calendar days in advance of the proposed visit date, unless the Competent Security Authorities agree on a different period.

4. The Competent Security Authorities may agree on a list of individuals entitled to recurring visits for a period not exceeding 12 (twelve) months. The Competent Security Authorities shall agree on the further details of these recurring visits.

5. The Competent Security Authority of the host Party shall inform the security officials of the organization to be visited, of the details of those individuals whose visit requests have been approved. Once approval has been given, visiting arrangements for individuals who have been given approval for recurring visits may be made directly with the agency, facility or organization concerned.

6. Any Classified Information transmitted to the official shall be deemed Classified Information under this Agreement and shall be handled in accordance with the provisions of this Agreement. In addition, the official must comply with the host Party's security regulations.

7. The Parties shall ensure, pursuant to their national laws and regulations, the protection of personal data of the individuals requesting a visit. The personal data shall not be used for any other purpose than determining the request for a visit.

8. When authorized, the Competent Security Authority of the host Party shall notify the requesting Party, as soon as possible, of the visit and also notify the facility to be visited.

ARTICLE – XI
SECURITY BREACH

1. When a Security Breach related to Classified Information under this Agreement is suspected or ascertained by the Receiving Entity, the Competent Security Authority of the Party where the Security Breach occurred shall immediately inform the Competent Security Authority of the other Party. The notice must contain sufficient details for the Originating Party to assess the consequences and circumstances of the suspected or ascertained Security Breach.
2. The Competent Security Authority of the Party where the Security Breach occurred shall immediately take all necessary steps, in accordance with its national laws and regulations, to investigate any suspected or ascertained Security Breach. The Competent Security Authority of the Originating Party may, if agreed, cooperate in the investigation. The Originating Party shall always be informed about the outcome of the investigation and the measures taken, if any.
3. The Competent Security Authority of the Party where the Security Breach occurred shall take all steps, including but not limited to legal steps, in accordance with its national laws and regulations, to mitigate the consequences of a Security Breach and to prevent any recurrence.
4. When a Security Breach has occurred in a Third Party, the Competent Security Authority of the Party that transmitted the information to the Third Party shall immediately inform the Competent Security Authority of the Originating Party about the Security Breach and make sure the Security Breach is investigated properly and communicate the outcome of the investigation and any measures taken.
5. Any Party may request information regarding the Security Breach investigation process.

ARTICLE – XII
CLASSIFIED CONTRACTS

1. If a Party or a Contractor including a Sub-Contractor proposes to grant a Classified Contract, with a Contractor under the jurisdiction of the other Party, it must first obtain written confirmation from the Competent Security Authority of the other Party that the Contractor has received a Facility Security Clearance at the appropriate Security Classification Level.

2. The Competent Security Authority of the Party where the Classified Contract is performed shall ensure that the Contractor and, if applicable, its sub-contractor:

- a) ensures that all individuals granted access to Classified Information are informed of their responsibilities to protect Classified Information in accordance with the conditions defined in this Agreement and with national laws and regulations;
- b) monitors the security conduct within its facilities in accordance with national laws and regulations;
- c) notifies promptly its Competent Security Authority of any security incident relating to the Classified Contracts; and
- d) holds an appropriate Facility Security Clearance in order to protect the Classified Information and that the individuals requiring access to Classified Information hold an appropriate Personnel Security Clearance.

3. Every Classified Contract including classified sub-contracts concluded in accordance with this Agreement shall include security requirements which identify the following aspect:

- a) a security classification guide, which shall always include the table of Article - IV, Paragraph 1 specifying the applicable Security Classification Levels of each part of the Classified Contract;
- b) a procedure for communication of changes in the Security Classification Level;
- c) the channels and procedures to be used for the transport and/or transmission of Classified Information;
- d) instructions for the handling and storage of Classified Information;
- e) contact details of the Classified Information related to the Classified Contract; and
- f) obligation to notify any Security Breaches.

4. The Competent Security Authority of the Party authorizing the award of the Classified Contract shall forward a copy of the security requirements chapter to the

Competent Security Authority of the Receiving Entity, to facilitate the security oversight of the Classified Contract.

ARTICLE – XIII COSTS

Each Party shall bear the costs of its own expenses resulting from the implementation and supervision of all aspects of this Agreement, unless otherwise mutually determined by the Parties.

ARTICLE – XIV DISPUTE SETTLEMENT

1. Any dispute between the Parties arising out of the interpretation or implementation or application of this Agreement, or any related matter, shall be resolved amicably exclusively through consultations and negotiations between the Parties and shall not be referred to any international court or Third Party for settlement.
2. During the dispute settlement period, both Parties will continue to fulfill their obligations under this Agreement.
3. Dispute settlement procedures between both Parties shall be conducted based on the principle of confidentiality.

ARTICLE – XV COMMUNICATION

All formal communication between the Parties relating to the implementation of this Agreement shall be in writing, in the English language.

ARTICLE – XVI ENTRY INTO FORCE

This Agreement shall enter into force on the first day of the second month following the receipt of the last notification by which the Parties shall inform each other, through diplomatic channels that their domestic legal requirements necessary for its entry into force have been completed.

ARTICLE – XVII AMENDMENTS

1. This Agreement, including its Annex, may be amended at any time, in writing, by means of amendments and with the mutual consent between the Parties. Amendments shall be proposed through diplomatic channels.
2. The amendments shall enter into force under the terms set out in Article - XVI of this Agreement, with the exception of amendments of the Annex, which shall enter into force on a date to be agreed upon by the Parties.

ARTICLE – XVIII VALIDITY AND TERMINATION

1. This Agreement shall remain in force for a period of 10 (ten) years and be renewed by tacit consent for fresh five-year periods unless one of the contracting Parties notifies the other of its intention not to renew it in writing 6 (six) months prior to the end of its current period of validity.
2. Either Party may, at any time, terminate this Agreement by giving written notice, through diplomatic channels, to the other Party.
3. Termination shall take effect 6 (six) months after the date on which the other Party receives notice of termination.
4. Upon termination, any Classified Information exchanged, released or generated under this Agreement shall continue to be protected in accordance with the terms of this Agreement before it was terminated, for as long as the Classified Information remains classified.

ARTICLE - XIX FINAL DISPOSITIONS

The Competent Security Authorities shall inform each other about their respective national laws, rules and regulations and shall promptly notify each other about modifications that affect the protection of Classified Information provided under this

ANNEX

The Competent Security Authorities, responsible for the implementation and supervision of this Agreement, are:

a) On behalf of the Republic of India —

Ministry of Home Affairs and Ministry of Defence of the Republic of India;

b) On behalf of the Federative Republic of Brazil —

The Institutional Security Cabinet of the Presidency of the Federative Republic of Brazil.

Agreement and have an impact on this Agreement. In the event of such changes, the Parties shall discuss the necessity of reviewing this Agreement.

IN WITNESS WHEREOF, the undersigned being duly authorized thereof by their respective Governments, have signed this Agreement.

DONE at Brasília on the 9th of July of 2025, in two original copies, each in the Portuguese, Hindi and English languages, all texts being equally authentic. In case of divergences in interpretation, the English text shall prevail.

FOR THE FEDERATIVE REPUBLIC OF BRAZIL

Marcos Antonio Amaro dos Santos
Minister-Chief of the Institutional Security
Cabinet of the Presidency of the Federative
Republic of Brazil

FOR THE REPUBLIC OF INDIA

Dinesh Chatia
Ambassador of India to Brazil

