



**ACORDO ENTRE O GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL
E O GOVERNO DA REPÚBLICA DA FINLÂNDIA
SOBRE TROCA E PROTEÇÃO MÚTUA DE
INFORMAÇÕES CLASSIFICADAS**

O Governo da República Federativa do Brasil e o Governo da República da Finlândia, doravante denominados em conjunto como “Partes”, ou separadamente, como “Parte”,

para proteger Informações Classificadas relacionadas especialmente com assuntos externos, defesa, segurança, polícia ou questões científicas, industriais e tecnológicas e trocadas diretamente entre as Partes, ou pessoas jurídicas ou físicas públicas ou privadas que tratem Informações Classificadas sob a jurisdição das Partes,

concordaram com o seguinte:

Artigo 1

Finalidade e escopo de aplicação

O objetivo deste Acordo é estabelecer regras e procedimentos para garantir a proteção das Informações Classificadas que são trocadas ou geradas no processo de cooperação entre as Partes.

Artigo 2

Definições

Para os fins deste Acordo:

- a) **Informação Classificada** significa qualquer informação, documento ou material de qualquer forma, ao qual tenha sido aplicado um nível de classificação de segurança e que tenha sido marcado de acordo com as leis e regulamentos nacionais, bem como qualquer informação, documento ou material que tenha sido gerado com base em tais Informações Classificadas e marcadas em conformidade;
- b) **Contrato Classificado** significa qualquer contrato ou subcontrato que contenha ou envolva Informação Classificada;
- c) **Parte Originária** significa a Parte que fornece Informações Classificadas ou sob cuja autoridade as Informações Classificadas são geradas;
- d) **Parte Receptora** significa a Parte, bem como qualquer pessoa jurídica pública ou privada ou pessoa física sob sua jurisdição, à qual a Informação Classificada é fornecida pela Parte Originária;

- e) **Terceiro** significa qualquer organização internacional ou estado, incluindo entidades legais ou indivíduos sob sua jurisdição, que não seja Parte deste Acordo;
- f) **Autoridade de Segurança Competente** significa uma Autoridade de Segurança Nacional ou qualquer outro órgão competente autorizado de acordo com as leis e regulamentos nacionais das Partes que seja responsável pela implementação deste Acordo;
- g) **Violação de Segurança** significa um ato ou omissão contrário às leis e regulamentos nacionais que pode levar à perda ou comprometimento de Informações Classificadas;
- h) **Autorização de Segurança** significa uma determinação positiva após um procedimento de verificação para determinar a elegibilidade de uma pessoa jurídica (Habilitação de Segurança de Instalação, HSI) ou de um indivíduo (Credencial de Segurança Pessoal, CSP) para ter acesso e lidar com Informações Classificadas em um determinado nível, de acordo com as leis e regulamentos nacionais;
- i) **Habilitação de Segurança de Instalação** significa a determinação pela Autoridade de Segurança Competente de que uma entidade implementou medidas de segurança adequadas e, portanto, foi credenciada para o tratamento de Informações Classificadas, de acordo com as leis e regulamentos nacionais de cada Parte;
- j) **Credencial de Segurança Pessoal** significa a autorização emitida por uma autoridade competente, de acordo com as suas leis e regulamentos nacionais, para que um indivíduo tenha acesso a informações classificadas;
- k) **Necessidade de conhecer** significa um princípio pelo qual o acesso a informações classificadas só pode ser concedido a indivíduos no âmbito das suas funções ou tarefas oficiais;
- l) **Contratante** significa uma pessoa física ou jurídica com capacidade jurídica para celebrar contratos.

Artigo 3

Autoridades de Segurança Competentes

As Autoridades Nacionais de Segurança (ANS) designadas pelas Partes como responsáveis pela implementação geral do presente Acordo são:

Na República Federativa do Brasil	Na República da Finlândia
O Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil	Autoridade Nacional de Segurança (ANS) Ministério das Relações Exteriores FINLÂNDIA

1. As Partes notificar-se-ão mutuamente sobre quaisquer outras Autoridades de Segurança Competentes que serão responsáveis pela implementação de aspectos deste Acordo.
2. As Partes notificar-se-ão mutuamente sobre quaisquer alterações subsequentes das Autoridades de Segurança Competentes.
3. Cada Parte fornecerá à outra os dados de contato da respectiva Autoridade de Segurança Competente, por escrito. As autoridades de segurança competentes das Partes informar-se-ão mutuamente por escrito sobre alterações nos seus dados de contato.
4. Mediante solicitação, as Autoridades de Segurança Competentes poderão ajudar-se mutuamente na execução dos procedimentos para a concessão de Credenciais de Segurança de Instalações e de Credenciais de Segurança Pessoal, mediante solicitação e de acordo com suas leis e regulamentos nacionais.
5. Mediante solicitação 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 Habilitação de Segurança de Instalação válida foi emitida.

6. As Autoridades de Segurança Competentes das Partes reconhecerão mutuamente suas Credenciais de Segurança Pessoal e Habilitações de Segurança de Instalações emitidas de acordo com suas respectivas leis e regulamentos e dentro do escopo deste Acordo.

Artigo 4

Níveis de classificação de segurança

1. As Partes acordam que os Níveis de Classificação de Segurança, de acordo com as respectivas leis e regulamentos nacionais, corresponderão entre si na seguinte forma de equivalência:

Parte Originária da Classificação	Parte receptora de classificação
ERITTÄIN SALAINEN ou YTTERST HEMLIG	ULTRASSECRETO
SALAINEN ou HEMLIG	SECRETO
LUOTTAMUKSELLINEN ou KONFIDENTIELL	SECRETO
KÄYTTÖ RAJOITETTU ou BEGRÄNSAD TILLGÅNG	RESERVADO
ULTRASSECRETO	ERITTÄIN SALAINEN ou YTTERST HEMLIG
SECRETO	SALAINEN ou HEMLIG
RESERVADO	LUOTTAMUKSELLINEN ou KONFIDENTIELL

2. A Parte Originária garantirá que todas as Informações Classificadas trocadas ou produzidas de acordo com este Acordo serão marcadas com o Nível de Classificação de Segurança da Parte Originária, de acordo com suas leis e regulamentos nacionais e conforme definido no parágrafo 1 deste artigo.

3. A Parte Receptora marcará todas as Informações Classificadas que receber da Parte Originária com o Nível de Classificação de Segurança equivalente da Parte Receptora, de acordo com o parágrafo 1 deste artigo. O Nível de Classificação de Segurança da Parte Originária será indicado primeiro, a fim de determinar o Nível de Classificação de Segurança equivalente adequado.

4. As Partes notificar-se-ão mutuamente de qualquer alteração e posterior emenda do Nível de Classificação de Segurança das Informações Classificadas.

5. A Parte Receptora não modificará ou revogará a classificação de segurança das Informações Classificadas recebidas ou geradas nos termos deste Acordo sem a aprovação prévia por escrito da Parte Originária.
6. Informações Classificadas originadas conjuntamente pelas Partes receberão Níveis de Classificação de Segurança mutuamente determinados pelas Partes.

Artigo 5

Proteção de Informações Classificadas

1. As Partes tomarão todas as medidas adequadas, em conformidade com as suas leis e regulamentos nacionais, para proteger as informações classificadas referidas no presente Acordo. Deverão proporcionar a essas informações pelo menos a mesma proteção que conferem às suas próprias informações no nível de classificação de segurança correspondente.
2. As Partes não fornecerão acesso a Informações Classificadas a terceiros sem o consentimento prévio por escrito da Parte Originária.
3. O acesso a informações classificadas será limitado a indivíduos que tenham uma “necessidade de conhecer” e que, de acordo com as leis e regulamentos nacionais, tenham sido credenciados e autorizados a ter acesso a essas informações, bem como informados sobre as suas responsabilidades para a proteção de informações classificadas.
4. Não é necessária a Credencial de Segurança Pessoal para acesso a informações classificadas no nível KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG da Parte Finlandesa.
5. As Informações Classificadas serão utilizadas exclusivamente para os fins para os quais foram fornecidas.

Artigo 6

Contratos Classificados

1. Mediante solicitação, a Autoridade de Segurança Competente da Parte Receptora informará a Autoridade de Segurança Competente da Parte Originária se um Contratante proposto que participa de negociações pré-contratuais ou na implementação de um Contrato Classificado recebeu uma Autorização de Segurança apropriada e correspondente ao nível de classificação de segurança exigido. Se a Contratada não possuir tal Autorização de Segurança, a Autoridade de Segurança Competente da Parte Originária poderá solicitar que a Contratada seja autorizada pela Autoridade de Segurança Competente da Parte Receptora.
2. No caso de uma proposta aberta, a Autoridade de Segurança Competente da Parte Receptora poderá fornecer à Autoridade de Segurança Competente da Parte Originária os certificados de Autorização de Segurança relevantes sem um pedido formal.
3. Não é necessária uma Habilitação de Segurança de Instalação para Contratos Classificados ao nível KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG da Parte Finlandesa.
4. Para permitir supervisão e controle de segurança adequados, um Contrato Classificado deverá conter um guia de classificação de segurança e disposições de segurança apropriadas, conforme especificado no Anexo 1. Uma cópia das disposições de segurança será enviada à Autoridade de Segurança Competente da Parte em cuja jurisdição o contrato será executado.
5. Representantes das Autoridades de Segurança Competentes das Partes poderão visitar-se mutuamente para analisar a eficiência das medidas adotadas por um Contratante para a proteção de Informações Classificadas envolvidas em um Contrato Classificado.

Artigo 7

Transmissão de Informação Classificada

1. As Informações Classificadas serão transmitidas entre a Parte Originária e a Parte Receptora através de canais governamentais ou por outro meio acordado entre suas Autoridades de Segurança Competentes.
2. As Informações Classificadas serão transmitidas entre a Parte Originária e a Parte Receptora eletronicamente apenas por meios seguros acordados entre as Autoridades de Segurança Competentes.

Artigo 8

Tradução, reprodução e destruição de Informação Classificada

1. Todas as traduções e reproduções de Informações Classificadas deverão ostentar marcações de classificação de segurança adequadas e serão protegidas como as Informações Classificadas originais. A tradução e a reprodução serão limitadas ao mínimo exigido para fins oficiais.
2. Todas as traduções deverão conter uma anotação adequada, no idioma da tradução, indicando que contêm Informações Classificadas da Parte Originária.
3. As Informações Classificadas no nível ERITTÄIN SALAINEN / YTTERST HEMLIIG ou ULTRASSECRETO serão traduzidas ou reproduzidas somente mediante consentimento por escrito da Parte Originária.
4. As Informações Classificadas no nível ERITTÄIN SALAINEN / YTTERST HEMLIIG ou ULTRASSECRETO serão devolvidas à Parte Originária, salvo acordo em contrário.
5. As Informações Classificadas de nível SALAINEN/HEMLIG ou SECRETO ou inferior serão destruídas após não serem mais consideradas necessárias pela Parte Receptora, de acordo com suas leis e regulamentos nacionais.
6. Se uma situação de crise tornar impossível proteger as Informações Classificadas fornecidas ao abrigo do presente Acordo, as Informações Classificadas serão destruídas imediatamente. A Parte Receptora notificará a Autoridade de Segurança Competente da Parte Originária sobre a destruição das Informações Classificadas o mais rápido possível.

Artigo 9

Visitas

1. As visitas que impliquem acesso a Informações Classificadas de nível LUOTTAMUKSELLINEN/KONFIDENTIELL ou RESERVADO ou superior requerem autorização prévia por escrito da Autoridade de Segurança Competente da Parte anfitriã. Os visitantes só terão acesso permitido quando tiverem estado:
 - a) autorizado pela Autoridade de Segurança Competente da Parte remetente para realizar a visita ou visitas necessárias; e
 - b) concedida uma Credencial de Segurança Pessoal apropriada.
2. A Autoridade de Segurança Competente relevante da Parte requerente notificará a Autoridade de Segurança Competente relevante da Parte anfitriã da visita planejada e garantirá que esta última receba o pedido de visita pelo menos 14 dias antes da realização da visita. Em casos urgentes, as Autoridades de Segurança Competentes poderão acordar um período mais curto. A solicitação de visita deverá conter as informações especificadas no Anexo 2 deste Acordo.
3. A validade das autorizações para visitas recorrentes não deverá exceder doze (12) meses.

Artigo 10

Cooperação em segurança

1. A fim de implementar o presente Acordo, as Autoridades Nacionais de Segurança notificar-se-ão mutuamente das suas leis e regulamentos nacionais relevantes relativos à proteção de Informações Classificadas, bem como de quaisquer alterações subsequentes às mesmas.
2. A fim de assegurar uma cooperação estreita na implementação do presente Acordo, as Autoridades de Segurança Competentes consultar-se-ão. Mediante pedido, deverão fornecer mutuamente informações sobre as suas normas, procedimentos e práticas de segurança nacionais para a proteção de informações classificadas. Para o efeito, as Autoridades de Segurança Competentes poderão realizar visitas, incluindo às suas instalações.
3. Mediante solicitação, as Autoridades de Segurança Competentes deverão, de acordo com as leis e regulamentos nacionais, ajudar-se mutuamente na execução dos procedimentos de Autorização de Segurança.
4. As Autoridades de Segurança Nacionais informar-se-ão prontamente sobre alterações nos certificados de Autorização de Segurança relevantes.

Artigo 11

Violação de segurança

1. Cada Parte notificará imediatamente a outra Parte sobre qualquer suspeita ou descoberta de violação de segurança de informações classificadas.
2. A Parte com jurisdição investigará o incidente prontamente. A outra Parte deverá, se necessário, cooperar na investigação.
3. A Parte com jurisdição deverá tomar todas as medidas apropriadas possíveis, de acordo com suas leis e regulamentos nacionais, de modo a limitar as consequências da Violação de Segurança e evitar novas Violações de Segurança. A outra Parte será informada do resultado da investigação e das medidas tomadas.

Artigo 12

Custos

Cada Parte suportará os seus próprios custos incorridos no decurso da implementação das suas obrigações ao abrigo do presente Acordo.

Artigo 13

Resolução de Controvérsias

Qualquer litígio entre as Partes sobre a interpretação ou aplicação do presente Acordo será resolvido amigavelmente através de consultas entre as Partes.

Artigo 14

Disposições finais

1. As Partes notificar-se-ão mutuamente da conclusão das medidas nacionais necessárias para a entrada em vigor do presente Acordo. O Acordo entrará em vigor no primeiro dia do segundo mês seguinte ao da recepção da notificação posterior.

2. Este Acordo estará em vigor até novo aviso. O Acordo poderá ser alterado pelo consentimento mútuo e por escrito das Partes. Qualquer uma das Partes poderá propor alterações ao presente Acordo a qualquer momento. Se uma Parte assim o propor, as Partes iniciarão consultas sobre a alteração do Acordo.

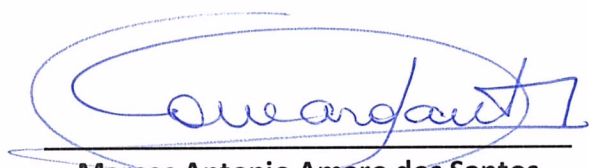
3. Qualquer uma das Partes poderá denunciar o presente Acordo mediante notificação escrita entregue à outra Parte através dos canais diplomáticos, observando um prazo de notificação de seis (6) meses. Se o Acordo for rescindido, quaisquer Informações Classificadas já fornecidas e quaisquer Informações Classificadas decorrentes do Acordo serão tratadas de acordo com as disposições do Acordo durante o tempo necessário para a proteção das Informações Classificadas.

4. Após a entrada em vigor do presente Acordo, a Parte em cujo território o Acordo for celebrado tomará medidas imediatas para que o Acordo seja registrado pelo Secretariado das Nações Unidas, em conformidade com o artigo 102.º da Carta das Nações Unidas. A outra Parte será notificada do registo e do número de registo na Série de Tratados da ONU assim que o Secretariado da ONU o emitir.

Em testemunho do que os representantes devidamente autorizados das Partes assinaram este Acordo,

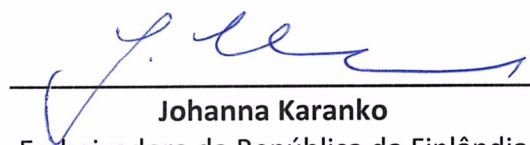
Feito em Brasília, no dia 24 de julho de 2024, em dois exemplares originais, nos idiomas português, finlandês, português e inglês, sendo cada texto igualmente autêntico. Em caso de qualquer divergência de interpretação, o texto em inglês prevalecerá.

**Pelo Governo da
República Federativa do Brasil**



Marcos Antonio Amaro dos Santos
Ministro de Estado
Chefe do Gabinete de Segurança
Institucional da Presidência da República

**Pelo Governo da
República da Finlândia**



Johanna Karanko
Embaixadora da República da Finlândia
no Brasil

Anexo 1

Contratos Classificados

Os Contratos Classificados referidos no Artigo 6 deste Acordo deverão conter cláusulas de segurança que incluam pelo menos o seguinte:

1. o nível de classificação mais elevado aplicado;
2. dados de contato das autoridades de segurança relevantes responsáveis pela execução do contrato;
3. leis e regulamentos relativos à proteção de informações classificadas;
4. procedimento e requisitos para acesso a Informação Classificada;
5. manuseio e armazenamento de informações classificadas;
6. transporte e transmissão eletrônica de Informações Classificadas;
7. marcação de Informação Classificada;
8. proteção da Informação Classificada após a rescisão do contrato;
9. destruição ou devolução de Informações Classificadas;
10. divulgação de informações contratuais.

Anexo 2

Pedido de Visita

Os pedidos de visita referidos no artigo 9.º do presente Acordo conterão as seguintes informações:

1. sobrenome e nome do visitante, local e data de nascimento e nacionalidade, o cargo do visitante, com uma especificação do empregador que o visitante representa, uma especificação do projeto em que o visitante participa, e o número do passaporte do visitante ou outro número de documento de identidade;
2. confirmação da Credencial de Segurança Pessoal do visitante de acordo com o objetivo da visita;
3. o objetivo da visita ou visitas, incluindo o mais alto nível de Informação Classificada envolvida;
4. a data prevista e a duração da visita ou visitas solicitadas. No caso de visitas recorrentes, será indicado o período total coberto pelas visitas, quando possível;
5. o nome, endereço, outras informações de contato e ponto de contato do estabelecimento ou instalação a visitar, e quaisquer outras informações úteis para determinar a justificação da visita ou visitas;
6. a data, assinatura da Autoridade de Segurança Competente remetente.



**SOPIMUS
SUOMEN TASAVALLAN HALLITUKSEN
JA BRASILIAN LIITTOTASAVALLAN HALLITUKSEN
VÄLILLÄ
TURVALLISUUSLUOKITELLUN TIEDON VAIHTAMISESTA
JA
VASTAVUOROISESTA SUOJAAMISESTA**

Suomen tasavallan hallitus ja Brasilian liittotasavallan hallitus, jäljempänä yhdessä "osapuolet" tai kumpikin erikseen "osapuoli",

suojatakseen turvallisuusluokitellun tiedon, joka liittyy erityisesti ulko-, puolustus-, turvallisuus-, poliisi-, tiede-, elinkeino- ja teknologia-asioihin ja jota vaihdetaan suoraan osapuolten välillä tai niiden lainkäyttövaltaan kuuluvien turvallisuusluokiteltua tietoa käsittelevien julkis- tai yksityisoikeudellisten oikeushenkilöiden tai luonnollisten henkilöiden välillä,

ovat sopineet seuraavasta:

1 artikla

Tarkoitus ja soveltamisala

Tämän sopimuksen tarkoituksena on määrätä säännöt ja menettelyt, joilla varmistetaan sellaisen turvallisuusluokitellun tiedon suojaaminen, jota vaihdetaan tai tuotetaan osapuolten välisessä yhteistyössä.

2 artikla

Määritelmät

Tässä sopimuksessa

- a) **turvallisuusluokiteltu tieto** tarkoittaa missä tahansa muodossa olevaa tietoa, asiakirjaa tai aineistoa, joka on turvallisuusluokiteltu ja johon on tehty luokitusmerkintä kansallisten säädösten ja määräysten mukaisesti, sekä tietoa, asiakirjaa tai aineistoa, joka on tuotettu tällaisen turvallisuusluokitellun tiedon pohjalta ja johon on tehty asianmukainen luokitusmerkintä;
- b) **turvallisuusluokiteltu sopimus** tarkoittaa sopimusta tai alihankintasopimusta, joka sisältää tai johon liittyy turvallisuusluokiteltua tietoa;
- c) **luovuttava osapuoli** tarkoittaa osapuolta, joka luovuttaa turvallisuusluokitellun tiedon tai jonka alaisuudessa turvallisuusluokiteltu tieto on tuotettu;

d) **vastaanottava osapuoli** tarkoittaa sitä osapuolta ja sen lainkäyttövaltaan kuuluvaa julkis- tai yksityisoikeudellista oikeushenkilöä tai luonnollista henkilöä, jolle luovuttava osapuoli luovuttaa turvallisuusluokitellun tiedon;

e) **kolmas osapuoli** tarkoittaa kansainvälistä järjestöä tai valtiota, mukaan lukien sen lainkäyttövaltaan kuuluvat oikeushenkilöt ja luonnolliset henkilöt, joka ei ole tämän sopimuksen osapuoli;

f) **toimivaltainen turvallisuusviranomainen** tarkoittaa osapuolten kansallisten säädösten ja määräysten mukaisesti valtuutettua kansallista turvallisuusviranomaista tai muuta toimivaltaista elintä, joka vastaa tämän sopimuksen täytäntöönpanosta;

g) **tietoturvaloukkaus** tarkoittaa kansallisten säädösten ja määräysten vastaista tekoa tai laiminlyöntiä, jonka johdosta turvallisuusluokiteltu tieto saatetaan menettää tai se saattaa vaarantua;

h) **turvallisuusselvitys** tarkoittaa selvitysmenettelyyn perustuvaa myönteistä arviota siitä, voidaanko oikeushenkilölle (yrittysturvallisuusselvitys) tai luonnolliselle henkilölle (henkilöturvallisuusselvitys) sallia pääsy tiettyyn turvallisuusluokkaan kuuluvaan turvallisuusluokiteltuun tietoon ja tämän tiedon käsittely kansallisten säädösten ja määräysten mukaisesti;

i) **yrittysturvallisuusselvitys** tarkoittaa toimivaltaisen turvallisuusviranomaisen arviota, jonka mukaan oikeushenkilö on toteuttanut asianmukaiset turvallisuustoimet ja hyväksytään sen perusteella käsittelemään turvallisuusluokiteltua tietoa osapuolen kansallisten säädösten ja määräysten mukaisesti;

j) **henkilöturvallisuusselvitys** tarkoittaa toimivaltaisen viranomaisen kansallisten säädöstensä ja määräystensä mukaisesti antamaa lupaa, jolla luonnolliselle henkilölle sallitaan pääsy turvallisuusluokiteltuun tietoon;

k) **tiedonsaantitarve** tarkoittaa periaatetta, jonka mukaan luonnollisille henkilöille voidaan sallia pääsy turvallisuusluokiteltuun tietoon ainoastaan heidän virallisen toimintansa ja virallisten tehtäviensä yhteydessä;

l) **hankeosapuoli** tarkoittaa luonnollista henkilöä tai oikeushenkilöä, jolla on oikeudellinen kelpoisuus tehdä sopimuksia.

3 artikla

Toimivaltaiset turvallisuusviranomaiset

1. Osapuolet ovat nimenneet seuraavat kansalliset turvallisuusviranomaiset vastaamaan yleisesti tämän sopimuksen täytäntöönpanosta:

Suomen tasavallassa	Brasilian liittotasavallassa
Kansallinen turvallisuusviranomainen (National Security Authority, NSA) Ulkoministeriö SUOMI	Brasilian liittotasavallan presidentinhallinnon institutionaalisen turvallisuuden virasto (The Institutional Security Cabinet of the Presidency of the Federative Republic of Brazil)

2. Osapuolet ilmoittavat toisilleen mahdolliset muut toimivaltaiset turvallisuusviranomaiset, jotka vastaavat tämän sopimuksen täytäntöönpanosta eri osin.

3. Osapuolet ilmoittavat toisilleen mahdolliset myöhemmät toimivaltaisten turvallisuusviranomaisten vaihdokset.

4. Osapuolet antavat toisilleen kirjallisesti toimivaltaisten turvallisuusviranomaistensa yhteystiedot. Osapuolten toimivaltaiset turvallisuusviranomaiset ilmoittavat toisilleen kirjallisesti yhteystietojensa muutokset.

5. Toimivaltaiset turvallisuusviranomaiset voivat pyynnöstä avustaa toisiaan kansallisten säädöstensä ja määräystensä mukaisesti menettelyissä yritys- ja henkilöturvallisuusselvitysten tekemiseksi.

6. Toisen osapuolen toimivaltaisen turvallisuusviranomaisen pyynnöstä toisen osapuolen toimivaltainen turvallisuusviranomainen antaa kirjallisen vahvistuksen voimassa olevasta henkilö- ja/tai yritysturvallisuusselvityksestä.

7. Osapuolten toimivaltaiset turvallisuusviranomaiset tunnustavat vastavuoroisesti toistensa tekemät henkilö- ja yritysturvallisuusselvitykset, jotka on tehty osapuolten kansallisten säädösten ja määräysten mukaisesti tätä sopimusta sovellettaessa.

4 artikla

Turvallisuusluokat

1. Osapuolet sopivat, että niiden kansallisten säädösten ja määräysten mukaiset turvallisuusluokat vastaavat toisiaan seuraavasti:

Luovuttavan osapuolen luokitus	Vastaanottavan osapuolen luokitus
ERITTÄIN SALAINEN tai YTTERST HEMLIG	ULTRASSECRETO
SALAINEN tai HEMLIG	SECRETO
LUOTTAMUKSELLINEN tai KONFIDENTIELL	SECRETO
KÄYTTÖ RAJOITETTU tai BEGRÄNSAD TILLGÅNG	RESERVADO
ULTRASSECRETO	ERITTÄIN SALAINEN tai YTTERST HEMLIG

SECRETO	SALAINEN tai HEMLIG
RESERVADO	LUOTTAMUKSELLINEN tai KONFIDENTIELL

2. Luovuttava osapuoli varmistaa, että kaikkeen tämän sopimuksen mukaisesti vaihdettavaan tai tuotettavaan turvallisuusluokiteltuun tietoon merkitään luovuttavan osapuolen turvallisuusluokka sen kansallisten säädösten ja määräysten mukaisesti sekä sellaisena kuin se on määriteltyä tämän artiklan 1 kohdassa.

3. Vastaanottava osapuoli merkitsee kaikkeen tässä sopimuksessa tarkoitettuun turvallisuusluokiteltuun tietoon, jonka se saa luovuttavalta osapuolelta, tämän artiklan 1 kohdan mukaisen vastaavan turvallisuusluokkansa. Luovuttavan osapuolen turvallisuusluokka merkitään ensin, jotta pystytään määrittämään asianmukainen vastaava turvallisuusluokka.

4. Osapuolet ilmoittavat toisilleen turvallisuusluokitellun tiedon turvallisuusluokan mahdolliset vaihdokset ja myöhemmät muutokset.

5. Vastaanottava osapuoli ei saa muuttaa eikä kumota tämän sopimuksen mukaisesti vastaanotetun tai tuotetun turvallisuusluokitellun tiedon turvallisuusluokitusta ilman luovuttavan osapuolen kirjallista ennakkosuostumusta.

6. Molemmilta osapuolilta yhteisesti peräisin oleva turvallisuusluokiteltu tieto luokitellaan turvallisuusluokkaan, jonka osapuolet päättävät keskenään.

5 artikla

Turvallisuusluokitellun tiedon suojaaminen

1. Osapuolet toteuttavat kaikki asianmukaiset kansallisten säädöstensä ja määräystensä mukaiset toimet suojataksaan tässä sopimuksessa tarkoitetun turvallisuusluokitellun tiedon. Ne antavat tälle tiedolle vähintään saman tasoisen suojan kuin omalle vastaavaan turvallisuusluokkaan kuuluvalla tiedolle.

2. Osapuolet eivät salli kolmansille osapuolille pääsyä turvallisuusluokiteltuun tietoon ilman luovuttavan osapuolen kirjallista ennakkosuostumusta.

3. Pääsy turvallisuusluokiteltuun tietoon sallitaan ainoastaan sellaisille luonnollisille henkilöille, joilla on tiedonsaantitarve, joista on tehty turvallisuusselvitys kansallisten säädösten ja määräysten mukaisesti ja joille on sallittu pääsy tällaiseen tietoon sekä selvitetty heidän vastuunsa turvallisuusluokitellun tiedon suojaamisesta.

4. Pääsy turvallisuusluokiteltuun tietoon, joka kuuluu Suomen osapuolen turvallisuusluokkaan KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG, ei edellytä henkilöturvallisuusselvitystä.

5. Turvallisuusluokiteltua tietoa saa käyttää ainoastaan siihen tarkoitukseen, jota varten se on luovutettu.

6 artikla

Turvallisuusluokitellut sopimukset

1. Vastaanottavan osapuolen toimivaltainen turvallisuusviranomainen ilmoittaa pyynnöstä luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle, onko ehdotetusta hankeosapuolesta, joka osallistuu turvallisuusluokiteltua sopimusta edeltäviin neuvotteluihin tai tällaisen sopimuksen täytäntöönpanoon, tehty vaadittua turvallisuusluokkaa vastaava asianmukainen turvallisuusselvitys. Jollei hankeosapuolella ole tällaista turvallisuusselvitystä, luovuttavan osapuolen toimivaltainen turvallisuusviranomainen voi pyytää vastaanottavan osapuolen toimivaltaista turvallisuusviranomaista tekemään hankeosapuolta koskevan turvallisuusselvityksen.

2. Jos on kyse avoimesta tarjouskilpailusta, vastaanottavan osapuolen toimivaltainen turvallisuusviranomainen voi antaa luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle asianmukaiset turvallisuusselvitystodistukset ilman virallista pyyntöä.

3. Suomen osapuolen turvallisuusluokkaan KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG kuuluvia turvallisuusluokiteltuja sopimuksia varten ei vaadita yritysturvallisuusselvitystä.

4. Jotta turvallisuutta voidaan valvoa ja ohjata asianmukaisesti, turvallisuusluokitellussa sopimuksessa on oltava tämän sopimuksen liitteessä 1 tarkoitetut turvallisuusluokitusohjeet ja asianmukaiset turvallisuusmääräykset. Kopio turvallisuusmääräyksistä toimitetaan sen osapuolen toimivaltaiselle turvallisuusviranomaiselle, jonka lainkäyttöalueella turvallisuusluokiteltu sopimus pannaan täytäntöön.

5. Osapuolten toimivaltaisten turvallisuusviranomaisten edustajat voivat vierailla toistensa luona arvioimassa niiden toimien tehokkuutta, jotka hankeosapuoli on toteuttanut suojatakseen turvallisuusluokiteltuun sopimukseen liittyvän turvallisuusluokitellun tiedon.

7 artikla

Turvallisuusluokitellun tiedon välittäminen

1. Luovuttava osapuoli ja vastaanottava osapuoli välittävät turvallisuusluokitellun tiedon toisilleen käyttäen hallitusten välisiä kanavia tai siten kuin niiden toimivaltaiset turvallisuusviranomaiset muutoin keskenään sopivat.

2. Luovuttava osapuoli ja vastaanottava osapuoli välittävät turvallisuusluokiteltua tietoa toisilleen sähköisesti ainoastaan toimivaltaisten turvallisuusviranomaisten keskenään sopimilla turvallisilla keinoilla.

8 artikla

Turvallisuusluokitellun tiedon kääntäminen, kopiointi ja hävittäminen

1. Kaikkiin turvallisuusluokitellun tiedon käännöksiin ja kopioihin tehdään asianmukaiset turvallisuusluokitusmerkinnät, ja ne suojataan kuten alkuperäinen turvallisuusluokiteltu tieto. Käännöksiä tehdään ja kopioita otetaan ainoastaan viralliseen tarkoitukseen tarvittava vähimmäismäärä.

2. Kaikkiin käännöksiin tehdään asianmukainen käännöskielinen merkintä siitä, että käännökset sisältävät luovuttavan osapuolen turvallisuusluokiteltua tietoa.

3. Turvallisuusluokkaan ERITTÄIN SALAINEN / YTTERST HEMLIG tai ULTRASSECRETO kuuluvaa tietoa saa kääntää tai kopioida ainoastaan luovuttavan osapuolen kirjallisella suostumuksella.

4. Turvallisuusluokkaan ERITTÄIN SALAINEN / YTTERST HEMLIG tai ULTRASSECRETO kuuluva tieto palautetaan luovuttavalle osapuolelle, jollei muuta sovita.

5. Turvallisuusluokkaan SALAINEN/HEMLIG tai SECRETO tai sitä alempaan turvallisuusluokkaan kuuluva tieto hävitetään sen jälkeen, kun vastaanottava osapuoli katsoo, ettei sitä enää tarvita, vastaanottavan osapuolen kansallisten säädösten ja määräysten mukaisesti.

6. Jos kriisitilanne estää tämän sopimuksen mukaisesti luovutetun turvallisuusluokitellun tiedon suojaamisen, tieto hävitetään välittömästi. Vastaanottava osapuoli ilmoittaa turvallisuusluokitellun tiedon hävittämisestä luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle mahdollisimman pian.

9 artikla

Vierailut

1. Vierailuihin, joihin liittyy pääsy turvallisuusluokkaan LUOTTAMUKSELLINEN/KONFIDENTIELL tai RESERVADO tai sitä ylempään turvallisuusluokkaan kuuluvaan tietoon, vaaditaan isäntäosapuolen toimivaltaisen turvallisuusviranomaisen kirjallinen ennakkolupa. Vierailijoille sallitaan pääsy turvallisuusluokiteltuun tietoon ainoastaan, jos

a) vieraat lähettävän osapuolen toimivaltainen turvallisuusviranomainen on antanut heille luvan pyydettyyn yhteen tai useampaan vierailuun, ja

b) heistä on tehty asianmukainen henkilöturvallisuusselvitys.

2. Vierailupyynnön esittävän osapuolen asianomainen toimivaltainen turvallisuusviranomainen ilmoittaa suunnitellusta vierailusta isäntäosapuolen asianomaiselle toimivaltaiselle turvallisuusviranomaiselle ja varmistaa, että kyseinen isäntäosapuolen turvallisuusviranomainen saa vierailupyynnön vähintään 14 päivää ennen vierailun ajankohtaa. Kiireellisissä tapauksissa toimivaltaiset turvallisuusviranomaiset voivat sopia lyhyemmästä ajasta. Vierailupyynnön on sisällettävä tämän sopimuksen liitteessä 2 tarkoitetut tiedot.

3. Toistuvia vierailuja koskevat luvat ovat voimassa enintään kaksitoista (12) kuukautta.

10 artikla

Turvallisuusyhteistyö

1. Tämän sopimuksen täytäntöön panemiseksi kansalliset turvallisuusviranomaiset ilmoittavat toisilleen sovellettavat turvallisuusluokitellun tiedon suojaamista koskevat kansalliset säädöksensä ja määräyksensä sekä niiden mahdolliset myöhemmät muutokset.

2. Varmistaakseen läheisen yhteistyön tämän sopimuksen täytäntöönpanossa toimivaltaiset turvallisuusviranomaiset neuvottelevat keskenään. Ne antavat pyynnöstä toisilleen tietoa turvallisuusluokitellun tiedon suojaamista koskevista kansallisista turvallisuusnormeistaan, menettelyistään ja käytännöistään. Tätä tarkoitusta varten toimivaltaiset turvallisuusviranomaiset voivat tehdä keskinäisiä vierailuja, myös niiden alaisuudessa toimiviin laitoksiin.

3. Toimivaltaiset turvallisuusviranomaiset avustavat pyynnöstä toisiaan turvallisuus selvitysmenettelyissä, kansallisten säädöstensä ja määräystensä mukaisesti.

4. Kansalliset turvallisuusviranomaiset ilmoittavat viipymättä toisilleen kulloinkin kyseeseen tulevien turvallisuus selvitystodistusten muutoksista.

11 artikla

Tietoturvaloukkaus

1. Kumpikin osapuoli ilmoittaa viipymättä toiselle osapuolelle epäilyistä tai todetusta turvallisuusluokiteltuun tietoon kohdistuneesta tietoturvaloukkauksesta.

2. Se osapuoli, jonka lainkäyttövaltaan asia kuuluu, tutkii tapauksen viipymättä. Toinen osapuoli tekee tarvittaessa tutkintayhteistyötä.

3. Se osapuoli, jonka lainkäyttövaltaan asia kuuluu, toteuttaa kansallisten säädöstensä ja määräystensä mukaisesti kaikki mahdolliset asianmukaiset toimet rajoittaakseen tietoturvaloukkauksen seurauksia ja estääkseen uudet tietoturvaloukkaukset. Toiselle osapuolelle ilmoitetaan tutkinnan ja toteutettujen toimien tuloksista.

12 artikla

Kustannukset

Kumpikin osapuoli vastaa omista kustannuksistaan, jotka sille aiheutuvat tästä sopimuksesta johtuvien velvoitteiden täyttämisestä.

13 artikla

Riitojen ratkaiseminen

Osapuolten väliset riidat tämän sopimuksen tulkinnasta tai soveltamisesta ratkaistaan sovinnollisesti osapuolten välisillä neuvotteluilla.

14 artikla

Loppumääräykset

1. Osapuolet ilmoittavat toisilleen, kun tämän sopimuksen voimaantulon edellyttämät kansalliset toimet on toteutettu. Sopimus tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun jälkimmäinen ilmoitus on vastaanotettu.

2. Tämä sopimus on voimassa toistaiseksi. Sopimusta voidaan muuttaa osapuolten keskinäisellä kirjallisella suostumuksella. Osapuoli voi milloin tahansa

ehdottaa tämän sopimuksen muuttamista. Jos jompikumpi osapuoli sitä ehdottaa, osapuolet aloittavat neuvottelut sopimuksen muuttamisesta.

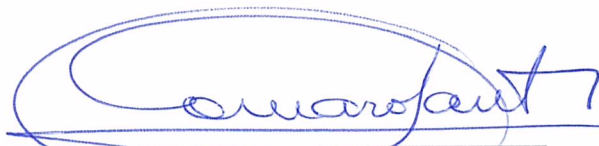
3. Osapuoli voi irtisanoa tämän sopimuksen ilmoittamalla asiasta kirjallisesti toiselle osapuolelle diplomaattitietse kuuden (6) kuukauden irtisanomisaikaa noudattaen. Jos sopimus irtisanotaan, sopimuksen perusteella jo luovutettua ja sen perusteella syntyvää turvallisuusluokiteltua tietoa käsitellään sopimuksen määräysten mukaisesti niin kauan kuin se on tarpeen kyseisen tiedon suojaamiseksi.

4. Tämän sopimuksen tultua voimaan se osapuoli, jonka alueella sopimus on tehty, toteuttaa viipymättä toimet sopimuksen kirjaamiseksi Yhdistyneiden kansakuntien sihteeristön Yhdistyneiden kansakuntien peruskirjan 102 artiklan mukaisesti. Kirjaaminen ja Yhdistyneiden kansakuntien sopimussarjan kirjaamisnumero ilmoitetaan toiselle osapuolelle heti, kun Yhdistyneiden kansakuntien sihteeristö on antanut numeron.

Tämän vakuudeksi asianmukaisesti valtuutetut osapuolten edustajat ovat allekirjoittaneet tämän sopimuksen

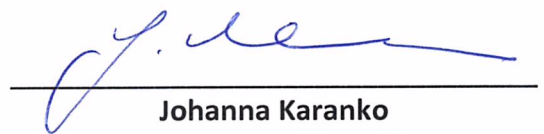
Brasíliassa 24.heinäkuussa 2024, kahtena alkuperäiskappaleena suomen, portugalın ja englannin kielellä, kaikkien tekstien ollessa yhtä todistusvoimaiset. Jos syntyy tulkintaeroja, englanninkielinen teksti on ratkaiseva.

**Brasilian liittotasavallan hallituksen
puolesta**



Marcos Antonio Amaro dos Santos
Brasilian liittotasavallan hallituksen
puolesta

**Suomen tasavallan hallituksen
puolesta**



Johanna Karanko
Suomen suurlähettiläs
Brasilian liittotasavalta

Liite 1

Turvallisuusluokitellut sopimukset

Tämän sopimuksen 6 artiklassa tarkoitettujen turvallisuusluokiteltujen sopimusten on sisällettävä turvallisuuslausekkeet, joissa on vähintään seuraavat tiedot:

1. korkein sovellettava turvallisuusluokka;
2. sopimuksen täytäntöönpanosta vastaavien toimivaltaisten turvallisuusviranomaisten yhteystiedot;
3. turvallisuusluokitellun tiedon suojaamista koskevat säädökset ja määräykset;
4. menettely ja vaatimukset turvallisuusluokiteltuun tietoon pääsemiseksi;
5. turvallisuusluokitellun tiedon käsittely ja säilyttäminen;
6. turvallisuusluokitellun tiedon siirtäminen ja sähköinen välittäminen;
7. turvallisuusluokitellun tiedon merkitseminen;
8. turvallisuusluokitellun tiedon suojaaminen turvallisuusluokitellun sopimuksen voimassaolon päätyttyä;
9. turvallisuusluokitellun tiedon hävittäminen tai palauttaminen;
10. turvallisuusluokiteltua sopimusta koskevan tiedon luovuttaminen.

Liite 2

Vierailupyyntö

Tämän sopimuksen 9 artiklassa tarkoitettujen vierailupyyntöjen on sisällettävä seuraavat tiedot:

1. vierailijan suku- ja etunimi, syntymäpaikka ja -aika sekä kansalaisuus; vierailijan asema ja tiedot hänen edustamastaan työnantajasta; tiedot hankkeesta, johon vierailija osallistuu, sekä vierailijan passin tai muun henkilöllisyystodistuksen numero;
2. vahvistus vierailun tarkoitusta vastaavasta vierailijan henkilöturvallisuusselvityksestä;
3. vierailun tai vierailujen tarkoitus sekä maininta vierailuun liittyvän turvallisuusluokitellun tiedon korkeimmasta tasosta;
4. pyydetyn yhden tai useamman vierailun oletettu ajankohta ja kesto; toistuvien vierailujen osalta mahdollisuuksien mukaan ajanjakso, jolle vierailut ajoittuvat;
5. vierailun kohteena olevan toimipaikan tai yksikön nimi, osoite, muut yhteystiedot ja yhteyshenkilö sekä muut vierailun tai vierailujen perusteltavuuden määrittämiseksi tarpeelliset tiedot;
6. päiväys sekä vierailupyynnön lähettävän toimivaltaisen turvallisuusviranomaisen allekirjoitus.



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

The Government of the Federative Republic of Brazil and the Republic of Finland, hereinafter referred to together as “Parties”, or separately, as “Party”,

in order to protect Classified Information related especially to foreign affairs, defence, security, police or scientific, industrial and technological matters and exchanged directly between the Parties, or public or private legal entities or individuals that handle Classified Information under the jurisdiction of the Parties,

have agreed as follows:

**Article 1
Purpose and scope of application**

The purpose of this Agreement is to establish rules and procedures to ensure the protection of Classified Information that is exchanged or generated in the process of cooperation between the Parties.

**Article 2
Definitions**

For the purposes of this Agreement:

- a) **Classified Information** means any information, document or material of whatever form, to which a security classification level has been applied and which has been marked in accordance with national laws and regulations, as well as any information, document or material that has been generated on the basis of such Classified Information and marked accordingly;
- b) **Classified Contract** means any contract or sub-contract, which contains or involves Classified Information;
- c) **Originating Party** means the Party which provides Classified Information or under whose authority Classified Information is generated;

- d) **Receiving Party** means the Party, as well as any public or private legal entity or individual under its jurisdiction, to which the Classified Information is provided by the Originating Party;
- e) **Third party** means any international organization or state, including legal entities or individuals under its jurisdiction, which is not a Party to this Agreement;
- f) **Competent Security Authority** means a National Security Authority or any other competent body authorised in accordance with the national laws and regulations of the Parties which is responsible for the implementation of this Agreement;
- g) **Breach of Security** means an act or an omission contrary to national laws and regulations which may lead to the loss or compromise of Classified Information;
- h) **Security Clearance** means a positive determination following a vetting procedure to ascertain the eligibility of a legal entity (Facility Security Clearance, FSC) or an individual (Personnel Security Clearance, PSC) to have access to and to handle Classified Information on a certain level in accordance with national laws and regulations;
- i) **Facility Security Clearance** means the determination by the Competent Security Authority that an entity 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;
- j) **Personal Security Clearance** means the authorization issued by a competent authority, in accordance with its national laws and regulations, for an individual to have access to classified information;
- k) **Need-to-know** means a principle by which access to Classified Information may only be granted to individuals in connection with their official duties or tasks;
- l) **Contractor** means an individual or legal entity possessing the legal capacity to undertake contracts.

Article 3 Competent Security Authorities

1. The National Security Authorities (NSAs) designated by the Parties as responsible for the general implementation of this Agreement are:

In the Federative Republic of Brazil	In the Republic of Finland
The Institutional Security Cabinet of the Presidency of the Federative Republic of Brazil	National Security Authority (NSA) Ministry for Foreign Affairs FINLAND

2. The Parties shall notify each other of any other Competent Security Authorities, which shall be responsible for the implementation of aspects of this Agreement.
3. The Parties shall notify each other of any subsequent changes of the Competent Security Authorities.
4. 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.
5. 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.

6. 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 Security Clearance has been issued.

7. 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.

Article 4 **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:

Classification Originating Party	Classification Receiving Party
ERITTÄIN SALAINEN or YTTERST HEMLIG	ULTRASSECRETO
SALAINEN or HEMLIG	SECRETO
LUOTTAMUKSELLINEN or KONFIDENTIELL	SECRETO
KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG	RESERVADO
ULTRASSECRETO	ERITTÄIN SALAINEN or YTTERST HEMLIG
SECRETO	SALAINEN or HEMLIG
RESERVADO	LUOTTAMUKSELLINEN or KONFIDENTIELL

2. Originating Party shall ensure that all Classified Information exchanged or produced pursuant to this Agreement shall be marked with Originating Party's Security Classification Level in accordance with their national laws and regulations and as defined in paragraph 1 of this article.

3. The Receiving Party shall mark all the Classified Information under this Agreement that it has received from the Originating Party with the equivalent Security Classification Level of the Receiving Party 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 Receiving Party 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.
6. Classified Information jointly originated by the Parties shall be assigned a Security Classification Level that is mutually determined by the Parties.

Article 5

Protection of Classified Information

1. The Parties shall take all appropriate measures in accordance with their national laws and regulations to protect Classified Information referred to in this Agreement. They shall afford such information at least the same protection as they afford to their own information at the corresponding security classification level.
2. The Parties shall not provide access to Classified Information to third parties without the prior written consent of the Originating Party.
3. Access to Classified Information shall be limited to individuals who have a 'need-to-know' and who, in accordance with national laws and regulations, have been security cleared and authorised to have access to such information as well as briefed on their responsibilities for the protection of Classified Information.
4. A Personnel Security Clearance is not required for access to Classified Information at the level KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG of the Finnish Party.
5. Classified Information shall be used solely for the purpose for which it has been provided.

Article 6

Classified Contracts

1. Upon request, the Competent Security Authority of the Receiving Party shall inform the Competent Security Authority of the Originating Party whether a proposed Contractor participating in precontract negotiations or in the implementation of a Classified Contract has been issued an appropriate Security Clearance corresponding to the required security classification level. If the Contractor does not hold such a Security Clearance, the Competent Security Authority of the Originating Party may request that the Contractor be security cleared by the Competent Security Authority of the Receiving Party.
2. In the case of an open tender, the Competent Security Authority of the Receiving Party may provide the Competent Security Authority of the Originating Party with the relevant Security Clearance certificates without a formal request.
3. A Facility Security Clearance is not required for Classified Contracts at the level KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG of the Finnish Party.
4. To allow adequate security supervision and control, a Classified Contract shall contain a security classification guide and appropriate security provisions as specified in Annex 1. A copy of the security provisions shall be forwarded to the Competent Security Authority of the Party under whose jurisdiction the contract is to be performed.
5. Representatives of the Competent Security Authorities of the Parties may visit each other in order to analyse the efficiency of the measures adopted by a Contractor for the protection of Classified Information involved in a Classified Contract.

Article 7

Transmission of Classified Information

1. Classified Information shall be transmitted between the Originating Party and the Receiving Party through government-to-government channels or as otherwise agreed between their Competent Security Authorities.
2. Classified Information shall be transmitted between the Originating Party and the Receiving Party electronically only by secure means agreed between the Competent Security Authorities.

Article 8

Translation, reproduction and destruction of Classified Information

1. All translations and reproductions of Classified Information shall bear appropriate security classification markings and be protected as the original Classified Information. Translation and reproduction shall be limited to the minimum required for an official purpose.
2. All translations shall contain a suitable annotation, in the language of translation, indicating that they contain Classified Information of the Originating Party.
3. Classified Information at the level ERITTÄIN SALAINEN / YTTERST HEMLIIG or ULTRASSECRETO shall be translated or reproduced only upon the written consent of the Originating Party.
4. Classified Information at the level ERITTÄIN SALAINEN / YTTERST HEMLIIG or ULTRASSECRETO shall be returned to the Originating Party unless otherwise agreed.
5. Classified Information at the level SALAINEN/HEMLIG or SECRETO or lower shall be destroyed after it is no longer considered necessary by the Receiving Party, in accordance with its national laws and regulations.
6. If a crisis situation makes it impossible to protect Classified Information provided under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the Competent Security Authority of the Originating Party about the destruction of the Classified Information as soon as possible.

Article 9

Visits

1. Visits entailing access to Classified Information at the level LUOTTAMUKSELLINEN/KONFIDENTIELL or RESERVADO or above require prior written authorisation from the Competent Security Authority of the host Party. Visitors shall only be allowed access where they have been:
 - a) authorised by the Competent Security Authority of the sending Party to conduct the required visit or visits; and
 - b) granted an appropriate Personnel Security Clearance.
2. The relevant Competent Security Authority of the requesting Party shall notify the relevant Competent Security Authority of the host Party of the planned visit, and shall make sure that the latter receives the request for visit at least 14 days before the visit takes place. In urgent cases, the Competent Security Authorities may agree on a shorter period. The request for visit shall contain the information specified in Annex 2 to this Agreement.

3. The validity of authorisations for recurring visits shall not exceed twelve (12) months.

Article 10 **Security co-operation**

1. In order to implement this Agreement, the National Security Authorities shall notify each other of their relevant national laws and regulations regarding the protection of Classified Information as well as of any subsequent amendments thereto.
2. In order to ensure close co-operation in the implementation of this Agreement the Competent Security Authorities shall consult each other. On request, they shall provide each other with information about their national security standards, procedures and practices for the protection of Classified Information. To this aim, the Competent Security Authorities may visit each other, including their facilities.
3. On request, Competent Security Authorities shall, in accordance with national laws and regulations, assist each other in carrying out Security Clearance procedures.
4. The National Security Authorities shall promptly inform each other about changes in relevant Security Clearance certificates.

Article 11 **Breach of Security**

1. Each Party shall immediately notify the other Party of any suspected or discovered Breach of Security of Classified Information.
2. The Party with jurisdiction shall investigate the incident without delay. The other Party shall, if required, co-operate in the investigation.
3. The Party with jurisdiction shall undertake all possible appropriate measures in accordance with its national laws and regulations to limit the consequences of the Breach of Security and to prevent further Breaches of Security. The other Party shall be informed of the outcome of the investigation and of the measures undertaken.

Article 12 **Costs**

Each Party shall bear its own costs incurred in the course of implementing its obligations under this Agreement.

Article 13 **Resolution of disputes**

Any dispute between the Parties on the interpretation or application of this Agreement shall be resolved amicably by means of consultations between the Parties.

Article 14

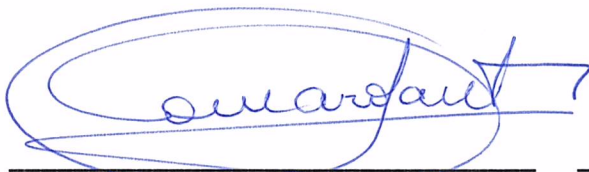
Final provisions

1. The Parties shall notify each other of the completion of the national measures necessary for the entry into force of this Agreement. The Agreement shall enter into force on the first day of the second month following the receipt of the later notification.
2. This Agreement shall be in force until further notice. The Agreement may be amended by the mutual, written consent of the Parties. Either Party may propose amendments to this Agreement at any time. If one Party so proposes, the Parties shall begin consultations on amending the Agreement.
3. Either Party may terminate this Agreement by written notification delivered to the other Party through diplomatic channels, observing a period of notice of six (6) months. If the Agreement is terminated, any Classified Information already provided and any Classified Information arising under the Agreement shall be handled in accordance with the provisions of the Agreement for as long as necessary for the protection of the Classified Information.
4. After the entry into force of this Agreement, the Party in whose territory the Agreement is concluded shall take immediate measures to have the Agreement registered by the Secretariat of the United Nations in accordance with Article 102 of the UN Charter. The other Party shall be notified of the registration and of the registration number in the UN Treaty Series as soon as the UN Secretariat has issued it.

In witness whereof, the duly authorised representatives of the Parties have signed this Agreement.

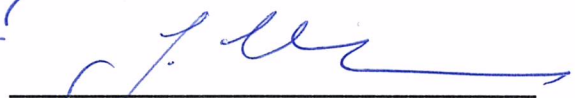
Done in Brasília, on the 24th of July, 2024, in two original copies, in the Portuguese, Finnish and English languages, each text being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

**For the Government of the
Federative Republic of Brazil**



Marcos Antonio Amaro dos Santos
Minister of State, Head of the
Institutional Security Cabinet of the
Presidency of the Republic

**For the Government of the
Republic of Finland**



Johanna Karanko
Ambassador of the Republic of Finland
to Brazil

Annex 1

Classified Contracts

Classified Contracts referred to in Article 6 of this Agreement shall contain security clauses including at least the following:

1. the highest classification level applied;
2. contact details of the relevant security authorities responsible for implementing the contract;
3. laws and regulations concerning the protection of Classified Information;
4. procedure and requirements for access to Classified Information;
5. handling and storing of Classified Information;
6. transportation and electronic transmission of Classified Information;
7. marking of Classified Information;
8. protection of Classified Information after termination of the contract;
9. destroying or returning of Classified Information;
10. release of contract information.

Annex 2

Request for visit

Requests for visit referred to in Article 9 of this Agreement shall contain the following information:

1. the visitor's family name, first name, place and date of birth and nationality, the visitor's position, with a specification of the employer which the visitor represents, a specification of the project in which the visitor participates, and the visitor's passport number or other identity document number;
2. confirmation of Personnel Security Clearance of the visitor in accordance with the purpose of the visit;
3. the purpose of the visit or visits, including the highest level of Classified Information to be involved;
4. the expected date and duration of the requested visit or visits. In the case of recurring visits the total period covered by the visits shall be stated, when possible;
5. the name, address, other contact information and point of contact of the establishment or facility to be visited, and any other information useful for determining the justification for the visit or visits;
6. the date, signature of the sending Competent Security Authority.