



MEMORANDUM OF UNDERSTANDING

BETWEEN

**THE INSTITUTIONAL SECURITY CABINET
OF THE PRESIDENCY OF THE FEDERATIVE REPUBLIC OF
BRAZIL**

AND

**THE NATIONAL SECURITY AUTHORITY
OF THE SLOVAK REPUBLIC**

ON COOPERATION IN THE FIELD OF CYBERSECURITY

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE INSTITUTIONAL SECURITY CABINET
OF THE PRESIDENCY OF THE FEDERATIVE REPUBLIC OF BRAZIL
AND
THE NATIONAL SECURITY AUTHORITY
OF THE SLOVAK REPUBLIC

ON COOPERATION IN THE FIELD OF CYBERSECURITY

The Institutional Security Cabinet (*Gabinete de Segurança Institucional*) of the Presidency of the Federative Republic of Brazil and the National Security Authority of the Slovak Republic (*Národný bezpečnostný úrad*) hereinafter referred to collectively as the “Participants” and singularly as a “Participant”:

Recognizing the existing friendly relations between the Federative Republic of Brazil and the Slovak Republic, and the considerable progress in the development of information and communication technology;

Further recognizing that the security of network and information systems and services has become paramount, as security incidents and cyber attacks increasingly have the potential to bring severe challenges to information infrastructures supporting essential services to society;

Noting their shared interest in strengthening cooperation on cybersecurity issues between the Participants based on the principles of equality and reciprocity and thereby contributing to the mutual benefit and friendly relations between the two countries;

Reaffirming our commitment to promote an open, secure, stable, accessible, peaceful and interoperable cyberspace environment founded on respect to human rights and fundamental freedoms, where social and economic development can thrive;

Desiring to further develop cooperation between the Federative Republic of Brazil and the Slovak Republic in the field of cybersecurity by strengthening information exchange, technology sharing and capacity building;

Believing that such cooperation would serve their common interests and contributes to the development of cybersecurity between the Participants;

Respecting the principles of sovereignty, territorial integrity, mutual respect, non-interference in the internal affairs of each Participant, and

Pursuant to the relevant laws and regulations and international commitments of the Participants;

Have reached the following understandings:

ARTICLE 1

Purpose

The purpose of this Memorandum of Understanding (hereinafter referred to as "Memorandum") is to promote partnerships and provide a framework for enhancing cooperation in the field of cybersecurity between the Participants.

ARTICLE 2

Basic Principles

1. The Participants hereby confirm their intention, under this Memorandum, to promote closer and privileged cooperation and the exchange of information pertaining to cybersecurity, creating a wide-ranging partnership that reflects the shared values, democratic traditions, human rights, rule of law, national security and economic development of the Participants.
2. This Memorandum does not create, maintain or govern any legally binding obligations, rights or benefits between the Participants or between the Participants and any third party.
3. This Memorandum will be implemented subject to and in accordance with domestic laws, regulations, policies and international obligations of the Participants.
4. The Participants are committed to promote security and stability in cyberspace recognizing the applicability of international law, particularly the United Nations Charter, to responsible conduct of states in cyberspace, and to the promotion of voluntary norms of responsible state behaviour in cyberspace.
5. The Participants understand the need to work closely with the private sector and business partners, mainly those considered critical infrastructures, acknowledging that much of the innovation and investment that shapes cyberspace takes place from within the private companies and that the multiple dimensions of the cybersecurity require cooperation between governments and their respective private sectors.

ARTICLE 3

Scope of Cooperation

The scope of cooperation between the Participants may include areas relating to cybersecurity that the Participants may mutually decide upon, such as the following:

1. Strengthen Incident Response:
 - a) strengthen the response capacities and capabilities to cybersecurity threats

- and attacks;
 - b) alert the other Participant, in case a malicious activity is detected and affects the network information system of the other Participant;
 - c) assist the other Participant with incident investigation and mitigation of incident impact, if requested;
 - d) for incidents deemed by both Participants to be of highest priority, the Participants will mutually consult on the actions to be taken on emergency response and the specific action plans.
2. Bilateral cooperation on joint research including:
- a) developing operational activities and methodology in cybersecurity;
 - b) best practices on a case-by-case basis, to create secure network environment.
3. Capacity Building:
- a) support capacity building and provide training as relevant;
 - b) mutual exchange and support for the development of joint cybersecurity exercises;
 - c) providing scholarships;
 - d) raising awareness and raising the level of digital literacy in the field of cyber and information security;
 - e) site visits;
 - f) other forms of capacity building cooperation.
4. Information Sharing
- Both Participants will share information on the strategy, regulation, policy, best practices, and implementation on:
- a) cybersecurity;
 - b) cryptography;
 - c) critical national infrastructure protection;
 - d) protection of human right and freedom in cyberspace;
 - e) building awareness and competence in information security;
 - f) improvement of effectiveness in information security management.

ARTICLE 4

Implementation

In order to implement the scope of cooperation identified in Article 3, the Participants will seek to develop the following programme:

- a) identify opportunities to discuss cybersecurity incidents of mutual interest (e.g. APT activities, Ransomware, Phishing, Denial of Service attacks, serious scan attacks, and forgery/defacement of government websites and other forms of Cyber incidents);
- b) support each other in taking appropriate measures in order to prevent recurrence of such cybersecurity incidents and to bolster their efforts to

- increase threat information sharing (e.g. exchange of indicators of compromise and cyber actor tactics, techniques and procedures);
- c) exchange assessments of the prevailing IT security trend, as observed by each country, periodically;
 - d) organise visits of officials from both Participants to discuss current issues on cybersecurity. Hold regular bilateral discussions;
 - e) invite each other, as well as representatives from the private sector, academia and civil society, to seminars/conferences held in respective countries to discuss cybersecurity issues;
 - f) any other areas of cooperation regarding cybersecurity as may be mutually decided upon.

ARTICLE 5

Point of Contact

1. For the purpose of identifying and facilitating programs under Article 3, the Participants will designate representatives to maintain contact with each other. The designated points of contact will be responsible for seeking any required approval for the conduct of specific cooperative activities from their respective Governments.
2. The representatives from the Participants responsible for implementing the scope of cooperation, as set out in Article 3 above, may hold consultations to identify and define future activities under Article 4, review activities in progress or discuss matters related to such activities. Where necessary, and by mutual agreement, the Participants may hold working meetings alternately in the Federative Republic of Brazil and the Slovak Republic at a mutually agreed date.
3. Both Participants respectively appoint dedicated Point of Contacts (PoCs) responsible for the contact and coordination with each other. Details of the PoCs are included in the Annex of this Memorandum.
4. A formal notification to the other Participant in the Memorandum is sufficient to amend the PoC. This information shall be effective from the time of its written communication to the other party. The amendment of the Annex to the Memorandum does not affect the amendment of the Memorandum as such.

ARTICLE 6

Intellectual Property Rights

1. Each Participant will ensure appropriate protection of Intellectual Property Rights (hereinafter referred to as "IPR") generated from cooperation pursuant to this Memorandum consistent with their respective laws, rules regulations and international agreements to which both Participants are committed.

2. The Participants will not assign any rights and obligations arising out of the IPR generated to inventions or activities carried out under this Memorandum to any third-party without consent of the other Participant.

ARTICLE 7

Financial Arrangements

1. Each Participant will bear its own costs associated with the activities and participation under this Memorandum.
2. There is no claim or obligation for any payment towards the other Participant regarding to the cooperation based on this Memorandum.
3. Other financial arrangements may be carried out mutually by the Participants, which shall be confirmed by written agreement.

ARTICLE 8

Settlement of Dispute

Any and all disputes between the Participants concerning the interpretation and/or implementation of this Memorandum will be settled amicably through consultations and/or negotiations between the Participants.

ARTICLE 9

Confidentiality and Release of Information

1. Both Participants shall use the information and knowledge obtained in the course of the activities contemplated under this Memorandum solely for the purpose of implementing it. Neither Participant will disclose nor distribute to any third-party any information transmitted by the other side in the process of cooperative activities under this Memorandum, except with the prior written consent of the other Participant.
2. The Participants will take all appropriate measures to protect the confidentiality of information, documents, technology, and/or data exchanged and/or generated between the Participants under this Memorandum against any unauthorised disclosure, in accordance with the Participants' domestic laws, regulations, policies, and directives.
3. In accordance with domestic law and of the Participants for protecting classified information, non-disclosure agreement, and informal non-disclosure agreement including but not limited to Traffic Light Protocol (TLP), the information exchanged according to this Memorandum should only be limited to internal use by both Participants and shall not be disclosed to any third party, except with the written permission of the delivering Participant.

4. Any information exchanged under this Memorandum will not be deemed confidential if:
 - a) it was already known by the receiving Participant at the time of sharing,
 - b) it is, or becomes, publicly known without any relation to the receiving Participant,
 - c) it is delivered to the receiving Participant from a third party on an unrestricted channel, or
 - d) it is clearly marked as allowed for disclosure by the originating Participant.

ARTICLE 10 **Amendment**

The Participants may revise or amend this Memorandum at any time by mutual written consent. Such revisions or amendments will enter into force on such a date that will be determined by the Participants and will form an integral part of this Memorandum.

ARTICLE 11 **Commencement, Duration, and Termination**

1. This Memorandum will come into effect on the date of signature by both Participants for period of 5 (five) years, and shall be automatically extended for a further 5 (five) year periods.
2. The Participants may at any time terminate this Memorandum by giving a written notification to the other Participant 3 (three) months before intended termination date. The Memorandum will be terminated on intended termination date when the other Participant confirms the receipt of the above notification.
3. Any intent to terminate or extend this Memorandum will be communicated not only through diplomatic channels.

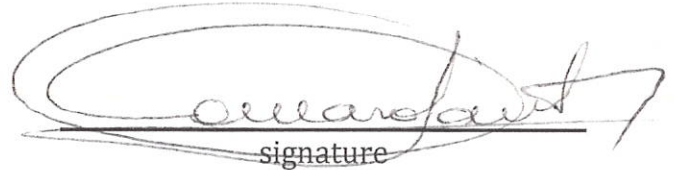
IN WITNESS WHEREOF, the undersigned being duly authorized thereto by their respective Governments, have signed this Memorandum.

Signed in Bratislava, on this **29th day of May, 2025**, in three originals in Portuguese, Slovak and English languages, all texts being equally valid. In case of any divergence of interpretation, the English text shall prevail.

Signed for and on behalf of the
Institutional Security Cabinet of the
Presidency of 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



signature

29/5/25

date

Signed for and on behalf of the
Head of National Security Authority
of the Slovak Republic

Roman Konečný

Director
of National Security Authority



signature

29/5/25

date

ANNEX

To the Memorandum of Understanding between the Institutional Security Cabinet of the Presidency of the Federative Republic of Brazil and the National Security Authority of the Slovak Republic

Designated points of contact for information sharing under the scope of the Memorandum:

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

● Duty Service: : ctir@ctir.gov.br (Tel) +55 613411-3477, INOC-DBA BR: 266031*800, GSM: +55 61999957859

● PoCs:

Topic	PoC	Email	Telephone	GSM
Incident Handling	Adão dos Santos	adao.santos@presidencia.gov.br	+5561992203732	+55613411-3978
Cooperation & Information	Cesar Montenegro Justo	cesar.montenegro@presidencia.gov.br	+5561983423915	+55613411-3195
Management Liaison	Daniel Maier de Carvalho	daniel.maier@presidencia.gov.br	+5561999957859	+55613411-1554

Office hours: Monday – Friday 9:00 AM – 6:00 PM (GMT-3).

Duty service: for partners (Memorandum) 24/7

National Security Authority of the Slovak Republic

- **Duty Service:** sk-cert@nbu.gov.sk (Tel) +421 2 6869 2915, (Fax) +421 2 6869 1700, GSM: +421 903 993 706

- **PoCs:**

Topic	PoC	Email	Telephone	GSM
Incident Handling	Ján Doboš	incident@nbu.gov.sk	+421 2 6869 2997	+421 903 993 706
International Cooperation and Legal Affairs	René Baran	rene.baran@nbu.gov.sk	+421 2 6869 2350	+421 903 993 163
Accreditation and Certification	Matej Šalmík	matej.salmik@nbu.gov.sk	+421 2 6869 2858	+421 903 993 723
Security Studies and National Strategy	Jaroslav Krcheň	jaroslav.krchen@nbu.gov.sk	+421 2 6869 2262	+421 903 993 151
Management Liaison	Jaroslav Ďurovka	jaroslav.durovka@nbu.gov.sk	+421 2 6869 2950	+421 905 011 225

Office hours: Monday – Friday 7:30 – 15:30 (GMT+1 / GMT+2 with DST which starts on the last Sunday in March and ends on the last Sunday in October)

Duty service: for partners (Memorandum) 24/7