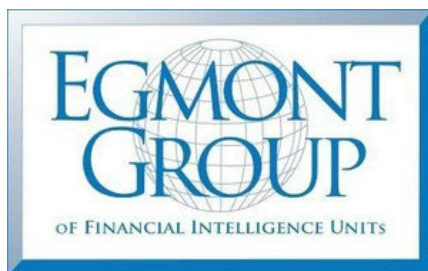
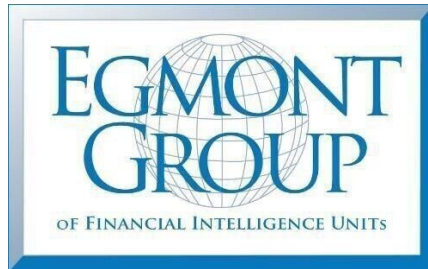


PRINCIPLES FOR INFORMATION EXCHANGE BETWEEN FINANCIAL INTELLIGENCE UNITS

APPROVED BY THE HEADS OF FIUS JULY 2025





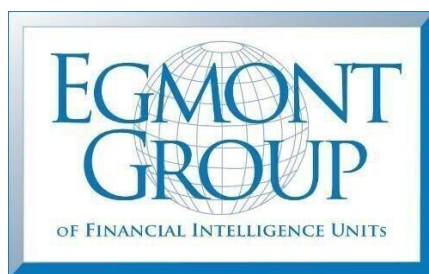
EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS

PRINCIPLES FOR INFORMATION EXCHANGE BETWEEN FINANCIAL INTELLIGENCE UNITS

**Approved by the Egmont Group
Heads of Financial Intelligence Units
July 2025**

Table of Contents

A.	Introduction	4
B.	General framework	5
C.	International Cooperation	5
	Obligations for the FIU Making the Request or Submitting Spontaneous Disclosures	6
	Obligations for the FIU Receiving the Request	7
	Unreasonable or Unduly Restrictive Conditions and Cases for Refusal of International Cooperation ..	8
	Data Protection and Confidentiality	8
	Channels for the Exchange of Information	9
D.	Glossary of Key Egmont Group Terminology	11
E.	Table of Amendments	12



EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS PRINCIPLES FOR INFORMATION EXCHANGE BETWEEN FINANCIAL INTELLIGENCE UNITS

These Principles are binding. Therefore, cases of significant and relevant non-compliance will be subject to the *Egmont Group Support and Compliance Process*.

A. Introduction

1. The Egmont Group fosters the development of Financial Intelligence Units (FIUs) and information exchange and other forms of cooperation between FIUs as prescribed by the Egmont Group Charter and the Financial Action Task Force (FATF) Standards.
2. The Egmont Group agreed in its Charter and Statement of Purpose to pursue among its priorities the stimulation of information exchange and to overcome the obstacles preventing cross-border information sharing.
3. The Egmont Group membership affirms accession to the standards set out in the Financial Action Task Force (FATF) Recommendations and Interpretative Notes, as well as to the applicable definitions in the FATF Glossary, including Confiscation and provisional measures (Recommendation 4), Financial Intelligence Units (Recommendation 29), and Other Forms of International Co-operation (Recommendation 40).
4. Information-sharing arrangements should aim to foster the widest possible cooperation between FIUs.
5. The definition of a Financial Intelligence Unit (FIU) is as stated within the Charter.
6. Terms used in these principles are either defined in the Glossary of the current document or in the Key Egmont Group Terminology, the Egmont Group Operational Guidance, and the FATF Glossary.
7. The following principles outline generally shared concepts, while allowing necessary flexibility.

B. General framework

8. FIUs should incorporate the principles outlined in this document in their information-sharing framework and ensure their staff is aware of them. FIUs should consider supporting the alignment of their national AML/CFT/CPF legal, regulatory, and institutional frameworks with the principles outlined in this document, by fostering awareness among relevant authorities and encouraging a unified, effective national approach. FIUs needing guidance to execute the principles should reach out to the Egmont Group Secretariat for coordination of the necessary support.
9. International cooperation between FIUs should be encouraged and based upon a foundation of mutual trust.
10. Information-sharing arrangements must recognize and allow room for case-by-case solutions to specific problems.

C. International Cooperation

11. FIUs should exchange information with foreign FIUs, regardless of their status; be it administrative, law enforcement, judicial or other.
12. To this end, FIUs should have an adequate legal basis for providing cooperation on money laundering, associated predicate offences and the financing of terrorism.
13. FIUs should exchange information freely, spontaneously and upon request on the basis of reciprocity and mutual assistance. FIUs should ensure that they can rapidly, constructively, and effectively provide the widest range of international cooperation to counter money laundering, associated predicate offences and the financing of terrorism. FIUs should do so both spontaneously and upon request, and there should be a lawful basis for providing cooperation.
14. In addition to the information that entities report to the FIU (under the receipt function), the FIU should be able to obtain and use additional information from reporting entities as needed to perform its analysis properly.
15. To conduct a proper analysis, FIUs should have access to the widest possible range of financial, administrative and law enforcement information. This should include information from open or public sources, as well as relevant information collected and/or maintained by, or on behalf of, other authorities and, where appropriate, commercially held data.
16. FIUs should be able to disseminate, spontaneously and upon request, information and the results of their analysis to relevant competent authorities.

17. FIUs should use the most efficient means to cooperate. If bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), are needed, these should be negotiated and signed in a timely way with the widest range of foreign FIUs in the context of international cooperation to counter money laundering, associated predicate offences and terrorist financing.
18. FIUs should be able to conduct domestic queries on behalf of foreign FIUs as needed, and exchange with these foreign FIUs all the information that they would be able to obtain if such queries were carried out domestically. Such queries are subject to any limitations or restrictions imposed by either FIU.
19. FIUs should have mechanisms in place to allow for the exchange of information necessary to assist the provisional measures, and where possible, confiscations pursuant to FATF Recommendation 4¹. FIUs should ensure that they can expeditiously exchange information necessary to suspend or withhold consent to a transaction. Such exchange can be conducted directly with counterparts or indirectly if legally permissible. However, in the context of requests from non-counterpart authorities, FIUs should notify the counterpart FIU of the indirect information exchange.

Obligations for the FIU Making the Request or Submitting Spontaneous Disclosures

20. When requesting cooperation, FIUs should make their best efforts to provide complete, factual and as appropriate, legal information, including the description of the case being analyzed and the potential link with the country receiving the request. This includes indicating any need for urgency to enable timely and efficient execution of the requests. FIUs requests should be well-defined and specific, with clear and direct relevance to the matter at hand. The scope of the request should be limited to what is necessary and proportionate, avoiding overly broad queries that may place an undue burden on the responding FIU. When requesting information for a particularly long period, FIUs should provide a clear justification for why that timeframe is relevant.
21. An FIU making an urgent request should mark its urgency clearly and justify it sufficiently². If the FIUs participating in the exchange are not in agreement as to the urgency of the request, they should communicate to find an acceptable resolution.

¹ Before requesting a counterpart FIU to assist in measures to suspend a transaction or provisionally freeze assets, member FIUs are encouraged to research the capacity of the counterpart to carry out these measures. Relevant information supplied in the Egmont Biennial Census may be helpful in this regard.

² Urgent requests should be limited to instances where timely response is critical and must include appropriate prior consent for dissemination. To avoid duplication of efforts, urgent requests should be avoided in cases where the necessary information has already been requested through other channels by other competent authorities, such as law enforcement authorities (LEAs).

22. FIUs may decide to exchange information indirectly with non-counterparts in response to requests from competent authorities. FIUs should ensure that the competent authority requesting the information indirectly always makes it clear whom they are requesting the information for and for what purpose.
23. Upon request and whenever possible, FIUs should provide feedback to their foreign counterparts on the use of the information provided, as well as on the outcome of the analysis conducted based on the information provided.
24. An FIU requesting information should disclose, to the FIU that will process the request, the reason for the request and, to the extent possible, the purpose for which the information will be used and provide enough information to enable the FIU receiving the request to provide information lawfully.
25. Requests for information that are sent simultaneously to several FIUs should be justified with a clear explanation of the link that involves the specific set of countries. Requests for information should not be sent to large distribution lists if the link is not justifiable to all recipients.
26. FIUs are encouraged to share spontaneous disclosures of information with counterpart FIUs. These disclosures do not require a response from the receiving FIU. However, when these disclosures result in a successful ML/TF investigation or prosecution, the receiving FIU should strive to provide relevant feedback about the usefulness of the received information.

Obligations for the FIU Receiving the Request

27. FIUs should have the power to exchange:
 - a. All information required to be accessible or obtainable directly or indirectly by the FIU under the FATF Recommendations, in particular under Recommendation 29; and
 - b. Any other information which they have the power to obtain or access, directly or indirectly, at the domestic level, subject to the principle of reciprocity.
28. FIUs should acknowledge receipt of requests, respond to requests for information, and provide interim partial or negative responses in a timely manner. FIUs are encouraged to provide at least an interim partial or negative response within 30 business days from receipt. An FIU receiving an urgent request should make its best efforts to provide its response within the timeframe indicated in the request.
29. FIUs should specify the scope of dissemination of the information in the response, including the permissible uses of information.

Unreasonable or Unduly Restrictive Conditions and Cases for Refusal of International Cooperation

30. FIUs should not prohibit or place unreasonable or unduly restrictive conditions on exchanging information or providing assistance. In particular, FIUs should not refuse a request for assistance on the grounds that:
- a. The request is also considered to involve fiscal matters,
 - b. Laws require financial institutions or designated non-financial businesses and professions (except where the relevant information that is sought is held under circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality.
 - c. There is an inquiry, investigation or proceeding underway in the country receiving the request unless the assistance would impede that inquiry, investigation or proceeding, and/or
 - d. The nature or status (civil, administrative, law enforcement etc.) of the requesting counterpart authority is different from its foreign FIU.
31. FIUs receiving requests may, as appropriate, refuse to provide information if the requesting FIU cannot protect the information effectively.
32. FIUs receiving requests should promptly and to the largest extent possible, grant prior consent to disseminate the information to competent authorities. The FIU receiving the request should not refuse consent to such dissemination unless this would fall beyond the scope of application of its AML/CFT provisions, could impair a criminal investigation, would be clearly disproportionate to the legitimate interests of a natural or legal person or the State of the providing FIU, or would otherwise not be in accordance with fundamental principles of its national law. Any such refusal to grant consent should be explicit and appropriately explained. Unless explicitly refused by the requested FIU, the requesting FIU may assume consent to disseminate the information to the authorities indicated in the request.
33. Cooperation may also be refused, as appropriate, on the grounds of lack of reciprocity or recurring inadequate cooperation. All cases that are refused must be justified, and FIUs should make all efforts to provide an explanation when the requested cooperation cannot be provided.

Data Protection and Confidentiality

34. Information exchanged by FIUs must be securely protected, exchanged and used only in accordance with agreed procedures, policies, and applicable laws and regulations. The information exchanged should be accompanied by clear confidentiality clauses.

35. FIUs must, therefore, have rules in place governing the security and confidentiality of such information, including procedures for handling, storage, deletion, dissemination and protection of, as well as access to, such information.
36. FIUs should ensure their staff members have the necessary security clearance levels and understand their responsibilities in handling and disseminating sensitive and confidential information.
37. FIUs should ensure there is limited access to their facilities and information, including information technology systems.
38. Exchanged information should be used only for the purpose for which the information was sought out or provided. Any dissemination of the information to other authorities or third parties, or any use of this information for administrative, investigative, prosecutorial or judicial purposes beyond those originally approved, should be subject to prior authorization by the requested FIU.
39. At a minimum, exchanged information must be treated and protected by the same confidentiality provisions that apply to similar information from domestic sources obtained by the FIU receiving the request.
40. FIUs should utilize technological solutions, including encryption, secure communication and decommissioning protocols, and authentication mechanisms, to ensure the confidentiality and integrity of exchanged data. All measures should comply with recognized cybersecurity frameworks, EG security guidelines, and applicable laws and regulations.
41. In instances when other competent authorities have direct access to FIU data, information received from a foreign counterpart FIU must be stored by the receiving FIU in a way that can only be accessed in accordance with the consent provided by the sending FIU.

Channels for the Exchange of Information

42. Exchanges of information should take place in a secure way, and through reliable channels or mechanisms.
43. To this end, FIUs should use the Egmont Secure Web or other recognized networks that ensure levels of security, reliability and effectiveness at least equivalent to those of the Egmont Secure Web (for example, the FIU.NET).
44. FIUs should ensure access to, and use of, the Egmont Secure Web or other appropriate channels of communication that are securely protected and reserved to authorized personnel. The equipment and passwords used for these channels should also be securely protected.

45. FIUs should be aware of the standards of security, reliability, efficiency and effectiveness applied in the use of the Egmont Secure Web or other appropriate channels.
46. FIUs should establish an emergency response framework that can respond to time sensitive threats if needed.

D. Glossary of Key Egmont Group Terminology

The Glossary of Key Egmont Group Terminology will remain in force until the new definitions are agreed, and consensus is reached by the Heads of FIUs.

Terms	Definitions
Information	Refers to raw data or factual details that may be collected by various entities, including financial institutions or law enforcement. In the context of the Egmont principle, "information" can denote data that may not yet have been analyzed or processed for specific intelligence purposes.
Financial Intelligence	<p>Refers to information that has been collected and analyzed about financial transactions and related data suspected to be linked to money laundering, associated predicate offenses, and the financing of terrorism. It often originates from raw data in Suspicious Transaction Reports (STRs), currency transaction reports, cross-border declarations, and other sources, is transformed by analyses to become actionable, and is disseminated as appropriate.</p> <p>Financial intelligence is the core output of FIUs operational activities or strategic analyses and serves as a critical input for law enforcement, judicial authorities, national security bodies, and international counterparts.</p>
Joint Analysis	Refers to the collaborative examination and evaluation of financial intelligence and data by two or more FIUs or relevant authorities. This process involves sharing information, methodologies, and analytical tools to enhance the understanding of complex financial crimes and emerging trends. The goal is to produce actionable financial intelligence that can assist in investigation and enforcement actions.
Joint Investigation	Refers to a cooperative effort between multiple jurisdictional authorities, acting in accordance with their individual legal powers. It may include FIUs, law enforcement agencies, and regulatory bodies, and is aimed at collaboratively probing suspected financial crimes. This approach fosters the sharing of expertise, resources, and information between countries or agencies to build comprehensive cases against entities or individuals engaged in illicit financial activities.
Legal Privilege	Refers to the principle that protects certain communications or information from disclosure due to their confidential nature under legal or professional standards. For FIUs, this may apply to information held by lawyers, notaries, and other legal professionals with a legal obligation to maintain secrecy.
Secure Communication Protocols	Refers to frameworks and technical mechanisms that guarantee the confidentiality, integrity, and authenticity of data exchanged between FIUs. These protocols often include, but are not limited to, encryption standards, secure socket, and multi-factor authentication.
Timely Manner	Refers to the obligation of both the requesting and responding FIUs to ensure that the exchange of information is carried out as swiftly as possible and as prescribed in the Egmont Group Principles for Information Exchange between FIUs.

E. Table of Amendments

“Any amendment to, or revision of, these Principles may be proposed by the Egmont Committee or the Heads of FIUs. These Principles can be amended by the Heads of FIUs. Each amendment will enter into force when consensus is reached by the Heads of FIUs, as the governing body of the Egmont Group, pursuant subsection 6.1 of Egmont Group of Financial Intelligence Units Charter.

Approved by the Egmont Group HoFIU at the 21st Plenary in South Africa in July 2013.

First amendment, Revised out-of-session by Egmont Group HoFIU in May 2022.

Second amendment, Revised out-of-session by Egmont Group HoFIU in January 2023.

Third amendment, Revised by the Egmont Group HoFIU in Luxemburg, in July 2025.”

Date/Reason for Update	Amendment
<p>First amendment, HoFIU reached consensus out-of-session in May 2022</p> <p>As a result of the Recommendations to address impediments regarding information exchange project.</p>	<p>Recommendation 3: Revising Principle 26 of the Egmont Group of Financial Intelligence Units Principles for Information Exchange between Financial Intelligence Units (July 2013).</p> <p>32. The PPWG proposes the following: <i>FIUs receiving requests should promptly and, to the largest extent possible, grant prior consent to disseminate the information to competent authorities. The FIU receiving the request should not refuse consent to such dissemination unless this would fall beyond the scope of application of its AML/CFT provisions, could impair a criminal investigation, would be clearly disproportionate to the legitimate interests of a natural or legal person or the State of the providing FIU, or would otherwise not be in accordance with fundamental principles of its national law. Any such refusal to grant consent should be <u>explicit and appropriately explained. Unless explicitly refused by the requested FIU, the requesting FIU may assume consent to disseminate the information to the authorities indicated in the request.</u></i></p>
<p>Second amendment, HoFIU reached consensus out-of-session in January 2023</p> <p>As a result of the Policy and Procedures Working Group (PPWG) project to develop a Glossary of Key Egmont Group Terminology</p>	<p>On January 19th, 2023, the Egmont Group Chair concluded, via out-of-session procedure, the consensus of the Egmont Group Heads of Financial Intelligence Units to approve the PPWG developed <i>Glossary of Key Egmont Group Terminology</i> and to include it as part of the <i>Egmont Group Principles for Information Exchange between Financial Intelligence Units</i>.</p>

**Third amendment, HoFIU
consensus in Luxembourg on
July 2025**

As a result of major
amendments in the FATF
recommendations and
technological developments

In July 2025, during the Plenary meeting in Luxembourg, the HoFIU agreed to the following amendments of the Egmont Group Principles for Information Exchange between Financial Intelligence Units:

- In principle 3. The Egmont Group membership affirms accession to the standards set out in the Financial Action Task Force (FATF) Recommendations and Interpretative Notes, as well as to the applicable definitions in the FATF Glossary, including Confiscation and provisional measures (Recommendation 4), Financial Intelligence Units (Recommendation 29), and Other Forms of International Co-operation (Recommendation 40).
- New principle 4. Information-sharing arrangements should aim to foster the widest possible cooperation between FIUs.
- New principle 6. Terms used in these principles are either defined in the Glossary of the current document or in the Key Egmont Group Terminology, the Egmont Group Operational Guidance, and the FATF Glossary.
- Former para 5 has been deleted:
- New principle 8. FIUs should incorporate the principles outlined in this document in their information-sharing framework and ensure their staff is aware of them. FIUs should consider supporting the alignment of their national AML/CFT/CPF legal, regulatory, and institutional frameworks with the principles outlined in this document, by fostering awareness among relevant authorities and encouraging a unified, effective national approach. FIUs needing guidance to execute the principles should reach out to the Egmont Group Secretariat for coordination of the necessary support.
- In the new Principle 13 (previous 11). FIUs should exchange information freely, spontaneously and upon request on the basis of reciprocity and mutual assistance. FIUs should ensure that they can rapidly, constructively, and effectively provide the widest range of international cooperation to counter money laundering, associated predicate offences and the financing of terrorism. FIUs should do so both spontaneously and upon request, and there should be a lawful basis for providing cooperation.
- In Principle 18 (previously 16). FIUs should be able to conduct domestic queries on behalf of foreign FIUs as needed, and exchange with these foreign FIUs all the information that they would be able to obtain if such queries were carried out domestically. Such queries are subject to any limitations or restrictions imposed by either FIU.

- New Principle 19. FIUs should have mechanisms in place to allow for the exchange of information necessary to assist the provisional measures, and where possible, confiscations pursuant to FATF Recommendation 4¹. FIUs should ensure that they can expeditiously exchange information necessary to suspend or withhold consent to a transaction. Such exchange can be conducted directly with counterparts or indirectly if legally permissible. However, in the context of requests from non-counterpart authorities, FIUs should notify the counterpart FIU of the indirect information exchange.
- A footnote to the new Principle 19 has been drafted: Before requesting a counterpart FIU to assist in measures to suspend a transaction or provisionally freeze assets, member FIUs are encouraged to research the capacity of the counterpart to carry out these measures. Relevant information supplied in the Egmont Biennial Census may be helpful in this regard.
- Section “Obligations for the FIU Making the Request” was amended to: “Obligations for the FIU Making the Request or Submitting Spontaneous Disclosures”
- In Principle 20 (previously 17). When requesting cooperation, FIUs should make their best efforts to provide complete, factual and as appropriate, legal information, including the description of the case being analyzed and the potential link with the country receiving the request. This includes indicating any need for urgency to enable timely and efficient execution of the requests. FIUs requests should be well-defined and specific, with clear and direct relevance to the matter at hand. The scope of the request should be limited to what is necessary and proportionate, avoiding overly broad queries that may place an undue burden on the responding FIU. When requesting information for a particularly long period, FIUs should provide a clear justification for why that timeframe is relevant.
- New Principle 21. An FIU making an urgent request should mark its urgency clearly and justify it sufficiently². If the FIUs participating in the exchange are not in agreement as to the urgency of the request, they should communicate to find an acceptable resolution.
- New footnote was also added to Principle 21: Urgent requests should be limited to instances where timely response is critical and must include appropriate prior consent for dissemination. To avoid duplication of efforts, urgent requests should

¹ Before requesting a counterpart FIU to assist in measures to suspend a transaction or provisionally freeze assets, member FIUs are encouraged to research the capacity of the counterpart to carry out these measures. Relevant information supplied in the Egmont Biennial Census may be helpful in this regard.

² Urgent requests should be limited to instances where timely response is critical and must include appropriate prior consent for dissemination. To avoid duplication of efforts, urgent requests should be avoided in cases where the necessary information has already been requested through other channels by other competent authorities, such as law enforcement authorities (LEAs).

be avoided in cases where the necessary information has already been requested through other channels by other competent authorities, such as law enforcement authorities (LEAs).

- New Principle 26. FIUs are encouraged to share spontaneous disclosures of information with counterpart FIUs. These disclosures do not require a response from the receiving FIU. However, when these disclosures result in a successful ML/TF investigation or prosecution, the receiving FIU should strive to provide relevant feedback about the usefulness of the received information.
- In Principle 28 (previously 23). FIUs should acknowledge receipt of requests, respond to requests for information, and provide interim partial or negative responses in a timely manner. FIUs are encouraged to provide at least an interim partial or negative response within 30 business days from receipt. An FIU receiving an urgent request should make its best efforts to provide its response within the timeframe indicated in the request.
- New Principle 29. FIUs should specify the scope of dissemination of the information in the response, including the permissible uses of information.
- Section “Unreasonable or Unduly Restrictive Conditions and Cases for Refusal to International Cooperation”, changed to “Unreasonable or Unduly Restrictive Conditions and Cases for Refusal of International Cooperation”
- In Principle 34 (previously 28). Information exchanged by FIUs must be securely protected, exchanged and used only in accordance with agreed procedures, policies, and applicable laws and regulations. The information exchanged should be accompanied by clear confidentiality clauses.
- In Principle 35 (previously 29). FIUs must, therefore, have rules in place governing the security and confidentiality of such information, including procedures for handling, storage, deletion, dissemination and protection of, as well as access to, such information.
- New Principle 40. FIUs should utilize technological solutions, including encryption, secure communication and decommissioning protocols, and authentication mechanisms, to ensure the confidentiality and integrity of exchanged data. All measures should comply with recognized cybersecurity frameworks, EG security guidelines, and applicable laws and regulations.
- New Principle 41. In instances when other competent authorities have direct access to FIU data, information received from a foreign counterpart FIU must be stored by the receiving FIU in a way that can only be accessed in accordance with the consent provided by the sending FIU.
- New Principle 46. FIUs should establish an emergency response framework that can respond to time sensitive threats if needed.