

Policy Title: <b>IAS Sanctions Law Compliance Policy</b>	Original Issue Date: 04/14/2021	Version Effective Date: 07/01/2021
	Most Recent Revision Date: 02/08/2022	Policy No.: <b>IASLG-004</b>



**IAS Sanctions Laws  
Compliance Policy**

**Approved By:** IAS Audit Committee  
**Policy Owner:** IAS General Counsel  
**Policy Contact:** IAS Global Compliance Officer

## Contents

1.0	Applicability and Scope	3
1.1	Applicability Boiler	3
1.2	Scope	3
2.0	Overview and Purpose	3
3.0	Policy Content	3
3.1	Definitions	3
3.2	Business Requirements	4
3.3	Types of sanctions	4
3.3.1	Comprehensive Sanctions.	4
3.3.2	List-Based Sanctions	4
3.3.3	Sectoral Sanctions	5
3.3.4	Secondary Sanctions	5
3.4	Sanctions Compliance Procedures	5
3.5	Training and Review	6
3.6	Questions and reporting	6
4.0	Policy Maintenance	6
4.1	Authority and Delegation	6
4.2	Policy Review, Renewal and Approval	6
4.3	Procedure Review, Renewal and Approval	6
5.0	Cross References	7
5.1	Related Policies	7
5.2	Related Standards	7
5.3	Related Procedures	7
5.4	Related Processes	7
5.5	Related Notices	7
6.0.	Revision History	7
7.0	Appendix	8
7.1	Employee Policy Certification	8

## 1.0 Applicability and Scope

### 1.1 Applicability

The Integral Ad Science (IAS) Sanctions Laws Compliance Policy (hereafter referred to as this "Policy") applies to the various operations within IAS, its sales platforms, all employees and, as applicable, subsidiaries, affiliates and third parties that support IAS' business activities (collectively, "IAS Entities"). This Policy establishes the minimum requirements for IAS and its entities.

This Policy applies to everyone employed by IAS or retained by IAS, including all of its officers, directors, and employees ("Company Personnel") and all agents, third-party representatives, and other intermediaries acting on behalf of IAS ("Third Parties") (together with IAS Personnel, "Covered Persons"). Each Covered Person has a personal responsibility and obligation to conduct the IAS' business activities ethically and in compliance with the law and this Policy. Failure to do so may result in disciplinary action, up to and including termination of employment, as well as civil or criminal liability.

### 1.2 Scope

This Policy is focused on compliance with Sanctions and requires that all Covered Persons:

- Not sell any products or provide any services to, or otherwise do any business involving, countries or territories subject to U.S. comprehensive Sanctions (as of the date of this Policy, **Cuba, Iran, North Korea, Syria, Venezuela, and the Crimea region of Ukraine**) unless authorized under Sanctions and approved by the Global Compliance Officer ("GCO"); and
- Not engage in any business with persons (*i.e.* individuals or entities) that are designated on, or subject to Sanctions under, U.S. or other applicable restricted party lists.

Any exceptions to this Policy must be consistent with applicable laws and will be made only with the explicit written approval of the GCO. Violations of this Policy can result in civil and criminal liability for IAS and individual employees and will result in appropriate disciplinary actions under the IAS' other policies and procedures, including possible termination of employment.

## 2.0 Overview and Purpose

This Policy provides an overview of:

- Our corporate policy regarding Sanctions,
- Procedures that we have adopted to ensure compliance with this Policy, and
- Potential penalties for violation of this Policy.

Anyone having any questions about their obligations to comply with Sanctions and this Policy, or if they suspect that any violation has occurred, should contact the GCO.

## 3.0 Policy Content

### 3.1 Definitions Required Section

The following acronyms and terms are used within this document.

Term	Definition
List of Specially Designated Nationals and Blocked Persons (the “SDN List”).	OFAC list that targets entities and individuals, as opposed to regions or nations.
Office of Foreign Assets Control (“OFAC”)	The primary U.S. government agency responsible for administering Sanctions.
Sanctions	Laws and regulations that restrict business with certain countries, individuals, and entities in order to advance specific foreign policy and national security priorities.

## 3.2 Business Requirements

IAS will not provide any products or services to or engage in any transactions with countries, territories, entities, or individuals targeted by applicable Sanctions, whether directly or indirectly, unless authorized under all applicable laws. Any opportunity to engage in transactions with sanctioned countries or sanctioned persons must be reviewed and approved in advance in writing by the GCO. The GCO will be responsible for ensuring all such transactions are only conducted if permitted under applicable Sanctions.

## 3.3 Types of sanctions

The Company and Covered Persons are required to comply with all U.S. Sanctions. With respect to applicable U.S. Sanctions, the U.S. Department of the Treasury, Office of Foreign Assets Control (“OFAC”) is the primary U.S. government agency responsible for administering Sanctions, which are laws and regulations that restrict business with certain countries, individuals, and entities in order to advance specific foreign policy and national security priorities.

OFAC maintains four types of sanctions programs, as follows:

### 3.3.1 Comprehensive Sanctions

OFAC currently administers comprehensive economic sanctions against **Cuba, Iran, North Korea, Syria, and the Crimea region of Ukraine**. U.S. persons (defined as U.S. citizens, U.S. lawful permanent residents, persons located in the United States, and U.S.-incorporated entities and their non-U.S. branches) cannot engage in any transactions or dealings with any counterparty located in a comprehensively sanctioned country, directly or indirectly (e.g., through agents, distributors, resellers), unless authorized under U.S. law. In addition to the above programs, OFAC maintains an embargo on the **Government of Venezuela**, which, when combined with the other sanctions on Venezuela described below, makes Venezuela a country subject to near comprehensive economic sanctions.

### 3.3.2 List-Based Sanctions

OFAC sanctions target entities and individuals designated on OFAC’s sanctions lists, including the List of Specially Designated Nationals and Blocked Persons (the “SDN List”). The SDN List is available on [OFAC’s website](#) at. Other OFAC sanctions lists also are available [online](#). A consolidated list that includes all [OFAC sanctions lists](#), as well as other U.S. restricted party lists are available.

***Importantly, OFAC considers any entity 50% or more owned, directly or indirectly and in the aggregate, by individuals or entities identified on the SDN List to be “blocked” and subject to the same restrictions as SDNs, even if the entity is not itself designated on the SDN List.***

Furthermore, OFAC’s list-based country sanctions currently target SDNs relating to the following

countries and regions: **Belarus, Burma/Myanmar Burundi, Central African Republic, Democratic Republic of the Congo, Hong Kong, Iraq, Lebanon, Libya, Mali, Nicaragua, Russia, Somalia, South Sudan, Sudan, Ukraine, Venezuela, the Western Balkans (i.e. Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia), Yemen, Venezuela and Zimbabwe.** These jurisdictions are generally higher-risk jurisdictions for sanctions.

Other countries, such as the United Kingdom, European Union, and United Nations Security Council (“UNSC”), also maintain restricted party lists similar to the scope of the SDN List. Such restrictions may be applicable depending on the specific circumstances of the transaction. Please reach out to the GCO for clarification on which non-U.S. restricted party lists may be applicable.

Other available lists include:

- [UK Financial Sanctions Consolidated List](#)
- [EU Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions](#)
- [UNSC Consolidated List](#)

### **3.3.3 Sectoral Sanctions**

These sanctions target specific sectors of a country’s economy. Currently, the primary sectoral sanctions that OFAC imposes relate to the Russia/Ukraine sanctions programs. Designated persons under the Russia-related sectoral sanctions are added to OFAC’s Sectoral Sanctions Identifications (“SSI”) List. Unlike with persons added to the SDN List, U.S. persons and companies may engage in most business with persons on the SSI List, subject to important restrictions that should be noted.

### **3.3.4 Secondary Sanctions**

Secondary sanctions target non-U.S.-person individuals and entities that provide support for sanctioned jurisdictions, entities, or individuals. Currently, secondary sanctions primarily target certain sectors and activities related to Iran, North Korea, Russia, Syria, and Venezuela. Also, it should be noted that the U.S. Crimea sanctions program authorizes the designation of any individual or entity worldwide determined by the U.S. government to “operate” in **Crimea**.

U.S. persons are prohibited from providing assistance of any kind that would “facilitate” transactions by third parties with sanctioned countries or persons, including referrals of sales opportunities, approvals, or brokering. Put differently, a U.S. person may not assist a third party in performing transactions with sanctioned countries or persons, even if that third party is able to do so under the laws that apply to the third party.

The Company will not provide any products or services to or engage in any transactions with countries, territories, entities, or individuals targeted by applicable Sanctions, whether directly or indirectly, unless authorized under all applicable laws. Any opportunity to engage in transactions with sanctioned countries or sanctioned persons must be reviewed and approved in advance in writing by the GCO. The GCO will be responsible for ensuring all such transactions are only conducted if permitted under applicable Sanctions.

## **3.4 Sanctions Compliance Procedures**

IAS will perform restricted party screening of certain non-U.S. customers, resellers, and vendors (“Screening Parties”) prior to onboarding to confirm whether such parties, and if applicable their owners, are the target of Sanctions, or involve any countries or parties targeted by Sanctions. The procedures for such screening are outlined in the Restricted Party Screening Procedures (“Procedures”).

The GCO will be responsible for ensuring that restricted party screening is conducted at onboarding and that existing Screening Parties are periodically rescreened in accordance with the Procedures to ensure they have not become the target of Sanctions as a result of changes to Sanctions. If a country or party subject to Sanctions may be involved in a potential transaction or other agreement, do not proceed. Report the situation to the GCO immediately.

### 3.5 Training and Review

IAS will conduct periodic internal reviews of this Policy to confirm that the Policy is operating correctly and effectively. The review will include a review and potential update of the Policy and testing of the restricted party screening procedures. IAS may also periodically conduct external audits of its compliance procedures with a third-party auditor. IAS will provide training to Covered Persons on this Policy as warranted. All Covered Persons are required to read, understand, and comply with this policy and to complete the certification attached hereto as Appendix A at the time of hire or onboarding. The HR Department is responsible for collecting such certifications.

### 3.6 Questions and reporting

IAS expects and requires any Covered Persons who have knowledge of, or reason to suspect, a violation of this Policy to contact the GCO immediately. Failure to report known or suspected violations of policy may result in disciplinary action, up to and including termination. Reports of known or suspected violations that are made honestly and in good faith will not result in adverse employment-related action or retaliation.

## 4.0 Policy Maintenance

### 4.1 Authority and Delegation

The IAS Audit Committee has approved this Policy. The IAS Audit Committee hereby delegates to the General Counsel ("**Policy Owner**") responsibility for this Policy and its maintenance, including authority to review and approve procedures established in accordance with this Policy.

Any authority granted by the IAS Audit Committee and any responsibility they assign to the Policy Owner under this Policy may be delegated at his/her discretion, except as otherwise provided in this Policy.

### 4.2 Policy Review, Renewal and Approval

**Approval:** The IAS Audit Committee shall review and approve all material revisions to this Policy. The IAS Audit Committee approval shall be documented in the meeting minutes of the appropriate governing body.

**Periodic Renewal:** The IAS Audit Committee shall renew this Policy periodically, but no less frequently than annually.

**Periodic Review:** The Global Compliance Officer shall review this Policy on an annual basis to evaluate its effectiveness and accuracy. Any resulting revisions shall be submitted for review and approval as outlined in the Approval section above and documented in the Revision History section of the Appendix. If no revisions are needed, the Global Compliance Officer or assigned delegate shall communicate the outcome of the review to the General Counsel.

**Additional Triggers:** Certain events, including but not limited to audit findings or changes in business activities, shall trigger unscheduled additional review and revision to this Policy.

### 4.3 Process Review, Renewal and Approval

All related procedures are expected to be in compliance with the spirit and letter of this Policy. The General Counsel has delegated to the Global Compliance Officer to review and approve all

material revisions to related procedures. The Global Compliance Officer must review and renew all related procedures no less frequently than annually.

In addition, any related procedures created by functions outside of Information Technology requires approval from the function leader most closely aligned with the procedure subject matter. Only those procedures that reflect material deviations from this Policy must be raised to the attention of the Global Compliance Officer or his/her delegate for review.

## 5.0 Cross References

### 5.1 Related Policies

None

### 5.2 Related Standards

None

### 5.3 Related Procedures

None

### 5.4 Related Processes

None

### 5.5 Related Notices

[OFAC's website](#) (SDN list)

[OFAC sanctions lists](#) (Consolidated lists)

[Other OFAC sanctions lists](#)

[UK Financial Sanctions Consolidated List](#)

[EU Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions](#)

[UNSC Consolidated List](#)

## 6.0 Revision History

Version	Approval Date	Effective Date	Description of Revisions:
I.0	07/01/2021	07/01/2021	Initial creation of policy
	02/08/2022	02/08/2022	Approval entity changed to IAS Audit Committee

## 7.0 Appendix

### 7.1 Employee Policy Certification

I hereby acknowledge that I have received, read, and fully understood the Company's Sanctions Laws Compliance Policy (the "Policy"). I agree to comply with all the rules contained therein. I further agree to participate in any trainings conducted by Company in relation to the Policy. I certify that, after due inquiry and investigation, I am not aware of any fact or circumstance that indicates that a violation of this Policy has occurred as of the date of this Certificate. I further certify that I will promptly report any non-compliance or potential violations in accordance with this Policy. I understand that failure to comply with the Policy or applicable Sanctions may result in immediate termination and could lead to prosecution, which may result in civil or criminal liability, fines, and/or imprisonment.

Should I have any questions regarding the Policy or become aware of any deviations or violations, I will contact the GCO immediately.

Signature: \_\_\_\_\_

Name (print): \_\_\_\_\_

Company: \_\_\_\_\_

Department: \_\_\_\_\_

Date: \_\_\_\_\_

(The signed receipt must be returned to the HR Department and filed in the employee's personnel file).