



Luxembourg No. 1 (2016)

Agreement

between the Government of the United Kingdom of Great Britain and
Northern Ireland and the Government of the Grand Duchy of
Luxembourg Concerning the Protection of Classified Information

London, 8 September 2015

[The Agreement is not in force]

*Presented to Parliament
by the Secretary of State for Foreign and Commonwealth Affairs
by Command of Her Majesty
February 2016*



© Crown copyright 2016

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit www.nationalarchives.gov.uk/doc/open-government-licence/version/3/ or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at Treaty Section, Foreign and Commonwealth Office, King Charles Street, London, SW1A 2AH

Print ISBN 9781474127592

Web ISBN 9781474127608

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

ID P002785442 53723 02/16

Printed on paper containing 30% recycled fibre content minimum

**AGREEMENT BETWEEN THE GOVERNMENT OF THE UNITED
KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND AND THE
GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
CONCERNING THE PROTECTION OF CLASSIFIED INFORMATION**

The Government of the United Kingdom of Great Britain and Northern Ireland (“the UK”) and the Government of the Grand Duchy of Luxembourg (referred to jointly as the “Parties” or individually as the “Party”), wishing to ensure the protection of Classified Information generated by and/or exchanged between the two Parties or commercial and industrial organisations in either the UK or Luxembourg, through approved channels, have, in the interests of national security, established the following arrangements which are set out in this Agreement.

ARTICLE 1

Purpose

The purpose of this Agreement is to ensure the protection of Classified Information (as defined in Article 2 of this Agreement) generated by and/or exchanged between the Parties, between their Contractors (as defined in Article 2 of this Agreement) or between a Party and any Contractor of the other Party, and set out security procedures and arrangements for such protection.

ARTICLE 2

Definitions

For the purposes of this Agreement:

- a) **“Classified Information”** means any information of whatever form, nature or method of transmission determined, either individually by one Party or jointly by both of the Parties, to require protection against unauthorised disclosure, misappropriation or loss, to which a security classification has been applied and which has been marked accordingly under the national laws and regulations of one or both of the Parties.
- b) **“Classified Contract”** means any contract or sub-contract, including any pre-contractual negotiations, which contains or involves access to Classified Information.
- c) **“Competent Security Authority (CSA)”** means a government authority which is responsible for implementing the security requirements covered by this Agreement.

- d) **“Contract”** means an agreement between two or more parties creating and defining legally enforceable rights and obligations between the parties.
- e) **“Contractor”** means a legal entity or person possessing the legal capability to undertake contracts or sub-contracts.
- f) **“Facility Security Clearance (FSC)”** means a determination following an investigative procedure stating that a Contractor is authorised to either receive, process or store Classified Information up to a certain classification level.
- g) **“Need to Know”** means the necessity for an individual to have access to Classified Information to fulfil their official duties and/or for the performance of a specific task.
- h) **“Originator”** means the Party, as well as any public or private legal entity under its authority, which originates and provides the Classified Information. Classified Information produced by a Contractor is owned by a Party.
- i) **“Recipient”** means the Party as well as any public or private legal entity under its authority to which the Classified Information is provided by the Originator.
- j) **“Personnel Security Clearance (PSC)”** means a determination following an investigative procedure stating that an individual is eligible to have access to Classified Information up to a certain classification level.
- k) **“Security Incident”** means an act or omission contrary to national laws and regulations, which may result in the unauthorised access, disclosure, compromise or destruction of Classified Information.
- l) **“Third Party”** means a State, international organisation or any other entity which is not a Party to this Agreement or an individual that is not under the jurisdiction of either Party.

ARTICLE 3

Security Authorities

1. The security authorities designated by the Parties as ultimately responsible for the security of Classified Information received under this Agreement are the following:

In the United Kingdom of Great Britain and Northern Ireland	In the Grand Duchy of Luxembourg
National Security Authority Cabinet Office	Service de Renseignement Autorité Nationale de Sécurité

2. The Parties may designate CSAs which shall be responsible for the implementation of aspects of this Agreement.

3. For the purposes of implementing this Agreement the Parties shall notify each other in writing of their respective CSAs and any significant changes to the CSAs.

ARTICLE 4

Security Classification Levels

1. Any Classified Information generated and/or exchanged under this Agreement shall be marked with the appropriate security classification level according to the national laws and regulations of the Party providing the information.

2. The Parties agree that the following security classification levels shall correspond to one another and be considered as equivalent:

In the United Kingdom of Great Britain and Northern Ireland	In the Grand Duchy of Luxembourg
UK TOP SECRET	TRES SECRET LUX
UK SECRET	SECRET LUX
No equivalent (see paragraph 3 of this Article)	CONFIDENTIEL LUX
UK OFFICIAL-SENSITIVE	RESTREINT LUX

3. The UK shall afford CONFIDENTIEL LUX Classified Information an equivalent level of protection as it would for UK SECRET Classified Information.

4. In the event that Classified Information at the UK TOP SECRET or TRES SECRET LUX level needs to be generated and/or exchanged, additional arrangements (as provided for in Article 15 of the Agreement) may be agreed between the Parties.

5. Luxembourg shall continue to handle UK CONFIDENTIAL Classified Information generated and/or exchanged by the Parties prior to 2 April 2014 as CONFIDENTIEL LUX, and UK RESTRICTED Classified Information as RESTREINT LUX.

6. The Recipient shall ensure that security classification markings are not altered or revoked, except with the prior written authorisation of the Originator.

ARTICLE 5

Protection of Classified Information

1. The Originator shall ensure that the Recipient is informed of:
 - a) The security classification level of the information provided, and any conditions of release or limitations on its use; and
 - b) Any subsequent change in the security classification level.
2. The Recipient shall in accordance with its national laws and regulations:
 - a) Provide the Classified Information with an equivalent level of protection as the Recipient would afford to its own information at the equivalent level of security classification;
 - b) If deemed appropriate, ensure that Classified Information received is marked with its own equivalent security classification in accordance with Article 4 of this Agreement;
 - c) Take all legally available steps to apply the principle of originator consent in accordance with its national laws and regulations;
 - d) Ensure that such Classified Information is used solely for the purpose for which it has been provided (unless the Originator expressly consents in writing to a further or different specified use);
 - e) Subject to Article 8 of this Agreement, not disclose Classified Information to a Third Party, without the prior written approval of the Originator; and
 - f) Ensure that security classifications are not altered or revoked, except as authorised in writing by or on behalf of the Originator.

3. If considered necessary each Party shall allow representatives of the other Party to visit its territory in order to discuss procedures for the protection of Classified Information provided by the other Party.

ARTICLE 6

Access to Classified Information

1. Access to Classified Information at the UK TOP SECRET, TRES SECRET LUX, UK SECRET, SECRET LUX or CONFIDENTIEL LUX level shall be limited to those individuals who have a Need to Know, who hold the nationality of a country of either Party, and who have been granted an appropriate PSC in accordance with national laws and regulations.

2. Access to Classified Information at the UK TOP SECRET, TRES SECRET LUX, UK SECRET, SECRET LUX or CONFIDENTIEL LUX level by an individual not holding the nationality of a country of either Party shall be on the condition that the individual has a Need To Know, has been granted an appropriate PSC in accordance with national laws and regulations, and the Originator has been consulted and given prior written approval for the individual to have access.

3. Access to Classified Information at the UK OFFICIAL-SENSITIVE or RESTREINT LUX level shall be limited to individuals who have a Need to Know. As a minimum, individuals having such access should be subjected to basic recruitment checks which should establish proof of identity; confirm that they satisfy all legal requirements for employment; and verify their employment record. Criminal record checks should also be conducted on the individual if permissible under national laws and regulations of the Recipient. These recruitment checks may be undertaken by Contractors and the requirement for these checks prior to granting access shall be included in the Contract.

4. Individuals who are given access to Classified Information shall be briefed on their responsibilities for the protection of such Classified Information.

ARTICLE 7

Transmission of Classified Information

1. Classified Information at the UK TOP SECRET, TRES SECRET LUX, UK SECRET, SECRET LUX or CONFIDENTIEL LUX level shall normally be transmitted between the Parties through official diplomatic Government-to-Government channels unless otherwise agreed by the relevant CSAs in advance.

2. Classified Information at the UK OFFICIAL-SENSITIVE or RESTREINT LUX level shall be transmitted physically in accordance with the national laws and regulations of the Originator, which may include the use of postal services or commercial courier companies.

3. Where large volumes of Classified Information at the UK TOP SECRET, TRES SECRET LUX, UK SECRET, SECRET LUX or CONFIDENTIEL LUX level are to be transmitted as freight, the means of transport, the route and any escort requirement shall be the subject of a transportation plan mutually agreed on a case-by-case basis by the relevant CSAs of both Parties.

4. If Classified Information is to be transmitted electronically within a Party it shall be protected by means applicable to the security classification level of the Classified Information being transmitted.

5. If Classified Information is to be transmitted electronically between the Parties it shall not be sent in clear text. Such transmissions shall be protected by cryptographic means that are mutually accepted by the relevant CSAs of both Parties. However, and only if the Originator approves, Classified Information at the UK OFFICIAL-SENSITIVE level may be transmitted in clear text if suitable cryptographic means are not available.

ARTICLE 8

Restrictions on Use and Disclosure

1. Subject to the provisions of paragraph 2 of this Article unless prior written consent is given to the contrary, the Recipient shall not use any Classified Information generated by and/or exchanged under this Agreement except for the purposes and within any limitations stated by or on behalf of the Originator.

2. Within the scope of national laws and regulations regarding public access to information the Recipient shall take all reasonable steps available to it to keep Classified Information generated and/or exchanged under this Agreement free from disclosure. If there is any request to declassify or disclose any Classified Information generated and/or exchanged under this Agreement the Recipient shall immediately notify the Originator in writing, and both Parties shall consult each other before a decision is taken to release the information.

3. Subject to the provisions of paragraph 2 of this Article, and to the national laws and regulations of the Recipient, Classified Information generated and/or exchanged under this Agreement shall not be disclosed to a Third Party without the prior written approval of the Originator.

ARTICLE 9

Translation, Reproduction and Destruction of Classified Information

1. All translations or reproductions of Classified Information shall bear the same security classification markings as the original and be protected accordingly.
2. Individuals undertaking a translation must hold an appropriate PSC.
3. All translations shall contain a suitable annotation, in the language of translation, indicating that they contain Classified Information of the Originator.
4. Information classified as UK TOP SECRET or TRES SECRET LUX shall be reproduced or translated only after obtaining the prior written consent of the Originator.
5. The number of reproductions shall be limited to the minimum required for an official purpose or in the course of a Classified Contract, and shall be made only by individuals who hold an appropriate PSC.
6. When it is no longer considered necessary to retain information for the purpose for which it was provided Classified Information shall either be returned to the Originator, or be destroyed in accordance with the Recipient's national laws or regulations applicable to the security classification level of the information concerned.
7. If a crisis situation makes it impossible for a Recipient to protect Classified Information generated and/or exchanged under this Agreement the Classified Information shall be destroyed using any appropriate means to avoid a Security Incident. The Recipient shall notify the CSA of the Originator in writing should Classified Information provided under this Agreement need to be destroyed in a crisis situation.
8. The Originator may prohibit the creation of translations or reproductions, or the alteration or destruction of Classified Information by giving it an appropriate marking or by attaching a written notice.

ARTICLE 10

Visits

1. If a Government official from a Party is required to visit a Government facility of the other Party where access to Classified Information marked UK TOP SECRET, TRES SECRET LUX, UK SECRET, SECRET LUX or CONFIDENTIEL LUX is involved, they must submit details of their PSC to the host facility ahead of such a visit.

2. If a Government official from a Party is required to visit a Contractor facility of the other Party or a Contractor under the jurisdiction of a CSA of one Party is required to visit a Government or Contractor facility where access to Classified Information marked UK TOP SECRET, TRES SECRET LUX, UK SECRET, SECRET LUX or CONFIDENTIEL LUX is involved, the procedure as set out in paragraphs 3, 4, 5 and 6 of this Article shall be applied.

3. Visitors, as referred to in paragraph 2 of this Article, who require access to Classified Information at the level of UK TOP SECRET, TRES SECRET LUX, UK SECRET, SECRET LUX or CONFIDENTIEL LUX shall only be allowed access where they have been:

- a) granted an appropriate PSC by the CSA of the requesting Party, have a Need to Know, and are authorised to have access to Classified Information in accordance with the national laws and regulations of the host Party; and
- b) authorised by the appropriate CSA of the requesting Party to conduct the required visit or visits.

4. Visit applications shall include at least the following information:

- a) Full name of visitor, date and place of birth, nationality and passport or identity card number;
- b) Official title of the visitor and the name of the establishment or contractor he/she represents;
- c) Date and duration of the requested visit or visits;
- d) Purpose of the visit(s) and subject(s) to be discussed;
- e) Whether the visit is a Government or commercial initiative and whether the visit is being initiated by the requesting establishment or facility or by the establishment or facility to be visited;
- f) Names of establishments and Contractors to be visited;
- g) Names of persons in the host Party establishment or facility to be visited;
- h) The full name and telephone number of the point of contact or the person with whom the arrangement for the visit has been made;
- i) The anticipated security classification level of Classified Information to be involved; and
- j) Confirmation and date of expiry of the visitor's PSC.

5. In cases involving a specific project or a particular Classified Contract it may be possible, subject to the approval of the relevant CSAs, to establish recurring visitor lists. These lists shall be valid for an initial period not exceeding 12 months (from the date of authorisation) and may be extended for further periods subject to the prior approval of those CSAs. Such a list shall be submitted to the relevant CSA in accordance with paragraphs 3 and 4 of this Article. Once a recurring visitor list has been approved, visit arrangements may be made directly between the establishments or Contractors involved in respect of listed individuals.

6. The CSA of the requesting Party shall notify the CSA of the host Party of the details of visitors at least 20 working days prior to the planned visit. In urgent cases the requesting and host CSA may agree a shorter period.

7. All visitors shall be required to comply with the national laws and regulations of the host facility concerning the protection of Classified Information.

8. Any Classified Information which may be provided to visitors, or which may come to the notice of visitors, shall be treated by them as if such Classified Information has been provided in accordance with the provisions of this Agreement.

9. Visits involving access to Classified Information at the UK OFFICIAL-SENSITIVE or RESTREINT LUX levels shall be arranged directly between the sending facility and the facility to be visited.

ARTICLE 11

Classified Contracts

1. If a CSA of one Party proposes to place (or authorise a Contractor under its jurisdiction to place) a Classified Contract involving information at the UK TOP SECRET, TRES SECRET LUX, UK SECRET, SECRET LUX or CONFIDENTIEL LUX level with a Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation of the relevant FSC from the CSA of that Party prior to entering into that Contract in accordance with Article 12.

2. A CSA which has granted a FSC shall be responsible for monitoring the security conduct of that Contractor in accordance with its national laws and regulations.

3. Contracts placed as a consequence of the pre-contract enquiries specified in paragraphs 1 and 2 of this Article shall contain a security requirements clause incorporating at least the following provisions:

- a) The definition of the term Classified Information and the equivalent levels of security classification of the two Parties as set out in Article 4 of this Agreement;
- b) The names of the CSA of each of the two Parties empowered to authorise the release and to co-ordinate the safeguarding of Classified Information related to the Contract;
- c) The channels to be used for the transmission of the Classified Information in accordance with Article 7 of this Agreement;
- d) The procedures for the translation, reproduction, and destruction of Classified Information in accordance with Article 9 of this Agreement;
- e) The procedures and mechanisms for communicating changes that may arise in respect of Classified Information either because of changes in its security classification or because protection is no longer necessary;
- f) The procedures for the approval of visits associated with Contract activity by personnel of one Party to Contractors of the other Party which are covered by the Contract in accordance with Article 10 of this Agreement; and
- g) The requirement that the Contractor shall immediately notify its CSA of any actual or suspected Security Incident concerning Classified Information relating to the Classified Contract and take all reasonable steps to assist in mitigating the effects of such a Security Incident.

4. The CSA of the Originator shall pass a copy of the relevant parts of the Classified Contract to the relevant CSA of the Recipient to allow adequate security monitoring.

5. Each Contract shall contain a supplement/annex providing guidance on the security requirements and on the security classification of each aspect/element of the Contract. For the UK this guidance shall be contained in specific security clauses in the Contract and in a Security Aspects Letter (SAL). For Luxembourg this guidance shall be contained in a security annex to the Contract. The guidance must identify each classified aspect of the Contract, or any classified aspect which is to be generated by the Contractor, and allocate to it a specific security classification. Changes in the requirements or to the aspects/elements shall be notified to the other CSA as and when necessary. The Originator shall notify the Recipient when all or any of the information has been declassified.

6. Contracts involving UK OFFICIAL-SENSITIVE or RESTREINT LUX information shall include appropriate security clauses informing the Contractor of the minimum security requirements for the protection and handling of this information.

ARTICLE 12

Security Co-operation

1. When the requesting CSA requires confirmation of a Contractor's FSC they shall submit a formal written request to the CSA of the Contractor in the country of the Party where it is located providing at least the following information:
 - a) Full name of the Contractor;
 - b) Address of the Contractor; and
 - c) Full name, position, and contact details of the requesting CSA.
2. When the requesting CSA requires confirmation of an individual's PSC they shall submit an official request to the appropriate CSA providing at least the following information:
 - a) Full name of the individual;
 - b) Date and place of birth;
 - c) Nationality of the individual; and
 - d) Name and address of the organisation or Contractor which employs the individual.
3. The relevant CSA in each Party shall notify the requesting CSA of the FSC/PSC status of a Contractor or individual in response to such a request.
4. If the Contractor or individual does not have a FSC/PSC, or the clearance is at a lower security level than that which has been requested, the requesting CSA shall be notified. If the original request asked for it, the notification shall state whether action is being taken to grant or upgrade the FSC/PSC.
5. On request, the CSAs shall, in accordance with national laws and regulations, assist each other in carrying out FSC/PSC checks.
6. If information comes to the attention of the CSA providing a FSC/PSC assurance which raises doubt as to whether the relevant Contractor or individual should continue to hold their current clearance status, the requesting CSA shall be notified promptly. The CSA that provided the FSC/PSC assurance shall conduct a review and advise the requesting CSA whether any changes to the FSC/PSC previously issued are proposed.
7. If either CSA suspends or takes action to revoke access which has been granted to a Contractor or individual of the other Party, the other Party shall be notified in writing.

ARTICLE 13

Security Incidents

1. Any suspected Security Incident concerning the Classified Information of the other Party shall be investigated immediately by the Party of the country where the incident occurs.
2. If a Security Incident concerning the Classified Information of the other Party is confirmed the relevant CSA of the Party of the country where the incident occurred shall take appropriate measures according to its national laws and regulations to limit the consequences. Where appropriate, that CSA shall institute disciplinary and/or legal proceedings in accordance with its national laws and regulations.
3. If a Security Incident results in the actual or suspected unauthorised disclosure or loss of Classified Information of the other Party the relevant CSA of the Party where the incident occurred shall inform the other relevant CSA of the outcome of the investigation in writing as soon as possible and of any actions taken to prevent a recurrence.

ARTICLE 14

Costs

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

ARTICLE 15

Implementing Arrangements

The Parties may develop detailed procedures as necessary for the implementation of this Agreement. Such procedures shall be agreed between the Parties through mutual consultation.

ARTICLE 16

Resolution of Disputes

Any dispute or disagreement between the Parties on the interpretation or application of this Agreement, or any other dispute or disagreement arising out of this Agreement, shall be resolved by means of consultations between the Parties and shall not be referred to any national or international tribunal or other body for settlement. During these consultations both Parties shall continue to fulfil all of their obligations under this Agreement.

ARTICLE 17

Final Provisions

1. Each Party shall notify the other once the internal procedures necessary for entry into force of this Agreement have been completed. This Agreement shall enter into force on the first day of the second month following the receipt of the later notification.

2. This Agreement may be amended with 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 the amendment of the Agreement. Agreed amendments shall enter into force under the conditions laid down in paragraph 1 of this Article.

3. This Agreement shall remain in force until further notice. A Party may terminate this Agreement by written notification delivered to the other Party through diplomatic channels, observing a period of notice of 6 months from the date of the notification. If this Agreement is terminated, any Classified Information already transmitted and any Classified Information generated and/or exchanged under this Agreement shall be handled by the Parties in accordance with the provisions of this Agreement for as long as the security classification level remains valid.

4. After the entry into force of this Agreement, the Party in whose territory the Agreement is concluded shall take immediate measures so as 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, in London on the Eighth day of September, 2015 in two original copies, each one in the English language.

.....
**For the Government of the
United Kingdom of Great Britain
and Northern Ireland:**

DAVID LIDINGTON

.....
**For the Government of the
Grand Duchy of Luxembourg:**

PATRICK ENGELBERG

ISBN 978-1-4741-2759-2



9 781474 127592