REGULATION
on Protection of Confidential Information, Security Clearances and Security Approvals in the Field of Security and Defence

CHAPTER I
General provisions
Article 1
Objective

The objective of the present Regulation is:

a) to protect documentation, cf. Article 2, from unauthorised access, the prevention of which is imperative, provided it contains information relating to State security, defence issues, or external relations with other States or transnational organisations, i.e. information the secrecy of which is primarily in the interest of the public;

b) to fulfil obligations in accordance with international agreements concerning security and defence, which provide for confidentiality and safekeeping of specified information and documentation;

c) to secure appropriate handling and security of such documentation, irrespective of its origin; and

d) to lay down rules on company security clearance for companies which are in need of such clearance on account of their export interests.

Article 2
Scope of application

This Regulation shall apply to:

a) confidential information, covered by the Defence Act No 34/2008, including its security and handling;

b) security clearance and security approval for individuals, companies, including suppliers, service providers and exporters, organisations, communication information systems (CIS), equipment and installations within the field of security and defence, covered by the Defence Act;

c) access to confidential information, security clearances and security approvals based on the Agreement between Iceland and the European Union on Security Procedures for the Exchange of Classified Information of 12 June 2006 and its annex, Security Arrangements between the Ministry for Foreign Affairs (MFA) of the Republic of Iceland, the EU Council General Secretariat Security Office (GSCSO) and the European Commission Security Directorate (ECSD) for the Protection of Classified Information Exchanged between The Republic of Iceland and the EU;

d) access to confidential information, security clearances and security approvals based on the General Security Agreement on the Mutual Protection and Exchange of Classified Information between Denmark, Finland, Iceland, Norway and Sweden of 7 May 2012;

and

e) access to confidential information, security clearances and security approvals based on other international agreements to which Iceland is a party.

Article 3
Definitions

For the purpose of this Regulation:

a) 1. the term "**Authorisation for Access**" means: a decision taken by the director of an organisation or a company that an individual is authorised to have access to secure areas or information with a distinctive security marking, provided he/she has been given security clearance;

b) 2. the term "**Background Check**" means: an examination undertaken by the National Security Authority (NSA) of the identity of the individual concerned and of police documents, *inter alia* his/her record of convictions, including if he/she has a criminal record, as part of assessing whether it would be safe to issue a security clearance for that individual and hence authorise his/her access to sensitive areas and confidential information;

c) 3. the term "**Supplier**" means: a person or entity selling goods which relate to the handling of confidential information and are covered by the present Regulation;

d) 4. the term "**Courier Certificate**" means: a confirmation issued by an organisation that a delivery, comprising confidential information, is authorised and that the individual carrying the information does so under the authority of the Government;

e) 5. the term "**Company**" means: a legal person, including suppliers, service providers or exporters, involved in handling of confidential information covered by the present Regulation;

f) 6. the term "**Procuring Entity**" means: an administrative body purchasing goods or services from a legal person outside the Government;

g) 7. the term "**Administrative Area**" means: an access controlled area which has passed inspection by NSA and has been authorised to handle confidential information up to the security marking "*Restricted*" (incl.), in accordance with this Regulation, cf. Articles 5 and 7;

h) 8. the term "**Document**" means: data of any kind comprising information, written or in other form, that have been created, received or maintained while an organisation or an individual engages in its/his/her activities;

i) 9. the term "**Organisation**" means: an administrative body to which this Regulation applies;

j) 10. the term "**Classified Information**" means: confidential information with a distinctive security marking and where access to such information is controlled with relation to security markings, security clearances and/or security approvals and with relation to those who need to have access to it;

k) 11. the term "**Classified Data**" means: the physical form in which confidential information is stored;

l) 12. the term "**Security Marking**" means: classification and marking of confidential information with regard to the seriousness of unauthorised access;

m) 13. the term "**Registry**" means: an archive of confidential documents, where reception, registration, distribution, placing and destruction of confidential information takes place within the organisation or company concerned;

n) 14. the term "**Confidential Information**" means: information covered by the present Regulation, the confidentiality of which is of vital interest;

o) 15. the term "**Information**" means: information of any kind, irrespective of its form, including documents (in electronic or paper form), such as maps, photographs or video and audio recordings, or other data;

p) 16. the term "**Security Officer**" means: officer of an organisation or a company entrusted by its director with the task of implementing this Regulation;

q) 17. the term "**Service Provider**" means: a party that provides services relevant to the handling of confidential information in accordance with the present Regulation;

r) 18. the term "**Secure Communication Information System (CIS)**" means: organised combination of peripheral equipment, software, data systems and communications network, all of which are encrypted in the appropriate manner and have been security approved in accordance with the present Regulation;

s) 19. the term "**Security Competence**" means: competence of an individual, organisation, company, area or equipment to receive security clearance and/or security approval for a distinctive security marking;

t) 20. the term "**Security Agreement**" means: agreement between an administrative body and a supplier, service provider or an exporter concluded, concurrent with classified procurement of goods or services or with classified export, before access is granted to confidential information;

u) 21. the term "**National Security Authority (NSA)**" means: central organisation which, on behalf of the State, coordinates and oversees handling and safekeeping of confidential information, runs background checks and determines security clearance and/or security approval for individuals, organisations, companies, areas, communication information systems (CIS) and equipment on a domestic level and vis-à-vis foreign countries and international organisations, cf. also Article 4(1);

v) 22. the term "**Secure Area**" means: an access controlled area which has passed inspection made by NSA and where it is authorised to handle confidential information with the security marking "C*onfidential*" and above, in accordance with this Regulation;

w) 23. the term "**Inspection**" means: NSA's surveillance of organisations, companies, areas, facilities and/or buildings, communication information systems (CIS) and equipment, which have been security cleared and/or security approved, and surveillance of implementation of the present Regulation;

x) 24. the term "**Personnel Security Clearance**" means: NSA's attestation based on a background check on an individual's security competence for having access to confidential information up to a distinctive security marking;

y) 25. the term "**Company Security Clearance**" means: NSA's attestation, based on background checks on individuals (chairmen of the Board of Directors and/or employees), and, as appropriate, inspection made on the facilities of a company and on its competence for engagement in activities or research which require access to confidential information;

z) 26. the term "**Security Approval of CIS**" means: NSA's attestation of the fact that a system or equipment, in which confidential information is placed or handled or to which and/or from which such information is communicated, meets the appropriate security requirements;

27. the term "**Security Approval of Facilities**" means: NSA's attestation, based on inspection made to determine whether a certain space, area or facility, within an organisation or a company, meets the appropriate requirements applicable to administrative areas and secure areas I or II for storing confidential information up to a distinctive security marking, cf. Articles 5 and 7;

28. the term "**Classified Procurement**" means: a procuring entity's procurement, the nature of which requires suppliers or service providers to have access to confidential

information, equipment or objects, or requires that they need to be security cleared for other reasons;

Article 4
Responsibility and Surveillance

The National Commissioner of the Icelandic Police (NCIP) performs the role of NSA, as defined in this Regulation, subject to the international organisations' rules with relevance to the present Regulation.

The director of an organisation or the manager of a company, which has received security clearance or has security cleared employees in its services, is responsible for implementation of this Regulation within the said organisation or company. He or she shall:

(a) himself or herself be security cleared in accordance with this Regulation;
(b) entrust one of his or her employees to be security cleared in accordance with this Regulation and to perform the role of security officer;
(c) ensure that the employees of the organisation or the company, who need access to classified information in accordance with this Regulation, will be security cleared as the Regulation stipulates;
(d) ensure that the rules of procedure of the organisation or the company are in line with this Regulation;
(e) compile internal instructions for the handling of classified information and security instructions, based on the provisions of this Regulation, elaborated in more detail as may be required;
(f) brief his or her employees regularly on this Regulation, the rules of procedure of the organisation or company in question, internal security instructions and on more detailed elaboration thereof; and
(g) secure the operation of a registry within the organisation or the company, where relevant.

In case of suspicion of a breach of the present Regulation, this shall be notified without delay to the security officer, the director of the organisation and the manager of the company concerned, and the NCIP. If a breach is confirmed, this shall be notified to the security officer of the Ministry for Foreign Affairs.

The NCIP shall inspect organisations, companies, areas, communication information systems (CIS) and equipment, which the NCIP has security cleared or security approved, cf. Article 37.

CHAPTER II
Classification, Storage, Handling and Communication of Classified Information
Article 5
Classification

Classified information shall be used exclusively for the purpose specified and shall be handled in line with its classification, as provided for in this Article.

Classified information may be handed over only to individuals who, in the course of their work, need access to the information and have been security cleared for that purpose in accordance with this Regulation.

Confidential information shall be classified according to a distinct security marking, which shall be clearly designated. Classification of confidential information with distinct security markings is based on estimation of the damage that could result from unauthorised release thereof. Confidential data shall be classified and marked with one of the following security markings; from the highest (a) to the lowest (d):

a) (a) ALGJÖRT LEYNDARMÁL (“YDERST HEMMELIGT”, “COSMIC TOP SECRET”, “TRÈS SECRET UE” or equivalent) shall be used in cases when the security

of Iceland, other States or international organisations, relations with foreign Governments or international organisations, or other vital interests of the State may suffer deadly serious damage by unauthorised release thereof;

b) (b) LEYNDARMÁL ("HEMMELIGT", "NATO SECRET", "SECRET UE" or equivalent) shall be used in cases when the security of Iceland, other States or international organisations, relations with foreign Governments or international organisations, or other vital interests of the State may be seriously damaged by unauthorised release thereof;

c) (c) TRÚNAÐARMÁL ("FORTROLIGT", "NATO CONFIDENTIAL", "CONFIDENTIEL UE" or equivalent) shall be used in cases when the security of Iceland, other States or international organisations, relations with foreign Governments or international organisations, or other vital interests of the State may be damaged by unauthorised release thereof; and

d) (d) TAKMARKAÐUR AÐGANGUR ("TIL TJENESTEBRUG", "NATO RESTRICTED", "RESTREINT UE" or equivalent) shall be used in cases when it may be contrary to the interests of Iceland, of other States or international organisations, or may have adverse effects on relations with foreign Governments or international organisations, if the information is released to unauthorised parties.

Data marked "NATO UNCLASSIFIED" are the property of the North Atlantic Treaty Organisation, whereas their release is subject to NATO regulations.

The originator of classified data shall ensure that they have appropriate security marking. Classified data shall not have higher security marking than is necessary. The period of validity for a security marking according to this Article shall not be longer than is necessary. Icelandic classified data to be communicated abroad shall be marked "ISL" plus the appropriate security marking (e.g. *"ISL Restricted"*), unless international agreements state otherwise.

Article 6
Handling of Classified Information

Classified information shall be handled as follows:

a) the information shall be protected and kept safe in a secure manner;

b) where the information is used in new data, the data shall have the same security marking as the document of origin;

c) should the information be copied or translated, the document shall have the same security marking as the document of origin; A translation of such confidential document shall include a detail specifying that the document contains classified information from the State or organisation of origin,

d) where information with the security marking "C*osmic Top Secret*" is no longer needed, it shall be given long-term physical protection, cf. Article 13, it shall be destroyed, cf. Article 12, or it shall be returned to the state or organisation of origin, as appropriate. Documents with the security marking "*Secret*" or below shall be destroyed as provided for in this Regulation; and

e) if a crisis situation makes it impossible to protect classified information, the information shall be destroyed.

Furthermore, it is unauthorised, without a prior written authorization from the State or organisation by which the information is originated:

a) to change the security marking of a document;

b) to translate, copy or destroy documents with the security marking "C*osmic Top Secret*";

c) to release classified information to other States, organisations or unauthorized parties, except with explicit authorisation and when this is strictly necessary; and