*(Unofficial translation)*

**ICELAND**

**REGULATION**

**on Protection of Confidential Information, Security Clearances**

**and Approvals in Matters of Security and Defence**

No. 959/2012 of 28 October 2012

(Published and entered into force on 14 November 2012)

CHAPTER I

**General provisions**

Article 1

*Objective*

 The objective of this regulation is:

1. to protect data, in accordance with (i.a.w.) art. 2, which is essential to protect from unauthorised access containing information on state security, defence or relations with other countries or transnational organisations and requires confidentiality because of significant public interest;
2. to fulfil obligations according to international agreements in matters of security and defence which provide for confidentiality and particular protection of specific information or data;
3. to secure appropriate handling and protection of such data, irrespective of its origin; and
4. to lay down rules on company security clearances required for reasons of export interests.

Article 2

*Scope of application*

 This regulation shall apply to:

1. confidential information covered by the Defence Act No 34/2008, including its security and handling;
2. security clearances and approvals for individuals, companies, including suppliers, service providers and exporters, agencies, communication information systems, equipment and installations in matters of security and defence, covered by the Defence Act;
3. access to confidential information, security clearances and approvals according to 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;
4. access to confidential information, security clearances and 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
5. access to confidential information, security clearances and approvals based on other international agreements to which Iceland is a party.

Article 3

*Definitions*

 For the purpose of this regulation:

1. **Authorisation for access** means a decision taken by the director of an agency or a company that an individual is authorised to have access to secure areas or information with a particular security classification, provided he or she has been given a security clearance;
2. **Background check** *(Vetting)* means an examination undertaken by the national security authority of the identity of the individual concerned and of police documents, i.a. his or her judicial record, including whether he or she has convictions, as part of an assessment of whether it would be safe to issue a security clearance for that individual and hence authorise his or her access to sensitive areas and confidential information;
3. **Supplier** means a person or entity selling goods which relate to the handling of confidential information and are covered by this regulation;
4. **Courier certificate** meansa confirmation issued by an agency that a delivery, containing confidential information, is authorised and that the individual carrying the information does so under the authority of the Government;
5. **Company** *(Organisation outside the Government/firm)* meansa legal person, including suppliers, service providers or exporters, involved in handling of confidential information covered by this regulation;
6. **Procuring entity** means an administrative body purchasing goods or services from a legal person outside the Government;
7. **Administrative area** *(Zone)* meansan access controlled area which has passed inspection by the national security authority and has been authorised to handle confidential information up to the security classification *"Restricted"*, according to this regulation, cf. art. 5 and 7;
8. **Document** meansdata of any kind containing information, written or in other form, that has been created, received or maintained in the course of activities of an agency or individual;
9. **Agency** means an administrative body to which this regulation applies;
10. **Classified information** meansconfidential information designated by a particular security classification and where access to such information is controlled according to its security classification, security clearances and/or approvals on a need to know basis;
11. **Classified data** means the physical form in which confidential information is stored;
12. **Security classification** *(Security marking)* means classification and designation of confidential information according to the seriousness of unauthorised access;
13. **Registry** means an archive of confidential documents where reception, registration, distribution, storage and destruction of confidential information takes place within the agency or company concerned;
14. **Confidential information** means information covered by this regulation, the confidentiality of which is of vital interest;
15. **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;
16. **Security officer** means the officer of an agency or company entrusted by its director with the task of implementing this regulation;
17. **Service provider** means a party that provides services in connection with the handling of confidential information according to this regulation;
18. **Secure communication information system** *(Secure network/CIS)*means an organised combination of peripheral equipment, software, data systems and a communications network, all of which are encrypted in the appropriate manner and have been given an approval according to this regulation;
19. **Security competence** means competence of an individual, agency, company, area or equipment to receive a security clearance and/or approval for a particular security classification;
20. **Security agreement** *(Security aspects letter)* means an agreement between an administrative body and a supplier, service provider or exporter, concluded in connection with the procurement of goods or services or with classified export, before access is granted to confidential information;
21. **National security authority** means a central agency which, on behalf of the State, coordinates and oversees handling and safekeeping of confidential information, runs background checks and decides on security clearances and/or approvals for individuals, agencies, companies, areas, communication information systems and equipment on a domestic level and vis-à-vis foreign countries and international organisations, cf. also para. 1 of art. 4;
22. **Secure area** *(Security zone)* means an access controlled area which has passed inspection made by the national security authority and where confidential information may be handled with the security classification *"Confidential"* and above, according to this regulation;
23. **Inspection** means the national security authority's surveillance of agencies, companies, areas, facilities and/or buildings, information systems and equipment, which have been given a security clearance and/or approval, and of the implementation of this regulation;
24. **Personnel security clearance** means the national security authority's attestation based on a background check of an individual's security competence for having access to confidential information up to a particular security classification;
25. **Company security clearance** means the national security authority's attestation, based on a background check of individuals (chairmen of the board of directors and/or employees), and, as appropriate, an inspection of a company's facilities and its competence for engaging in activities or research which requires access to confidential information;
26. **Security approval of information systems or equipment** *(Accreditation of CIS)* means the national security authority's attestation that a system and equipment, where confidential information is kept, handled or communicated, meets the appropriate security requirements;

(þ) **Facility approval** means the national security authority's attestation, based on an inspection to determine whether a certain space, area or facility, within an agency or company, meets the appropriate requirements applicable to administrative areas and secure areas I or II for storing confidential information up to a particular security classification, cf. art. 5 and 7;

(æ) **Classified procurement** meansa purchase by a procurement agency of the kind that requires suppliers or service providers to have access to confidential information, equipment or object or requires that they have a security clearance for other reasons;

Article 4

*Responsibility and Surveillance*

 The National Commissioner of Police serves as the national security authority, as defined in this regulation, cf. international organisations' rules pertaining to this regulation.

 The director of an agency or the managing director of a company, which has received a security clearance or has security cleared employees, is responsible for implementing this regulation within that agency or company. He or she shall:

(a) himself or herself have a security clearance according to this regulation;

(b) entrust one of his or her employees to obtain a security clearance according to this regulation and to perform the role of security officer;

(c) ensure that employees of an agency or company, who need access to classified information according to this regulation, obtain a security clearance according to the regulation;

(d) ensure that the operational rules of the agency or company are in line with this regulation;

(e) compile internal guidance 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 operational rules of the agency or company in question and internal security guidance and their elaboration; and

(g) ensure the operation of a registry within the agency or company, as applicable.

 If a violation is suspected of this regulation, this shall be notified immediately to the security officer, the director of the agency or the managing director of the company concerned and Tthe National Commissioner of Police. If a violation is confirmed this shall be notified to the security officer of the Ministry for Foreign Affairs.

 The National Commissioner of Police performs security inspections of agencies, companies, areas, communication information systems and equipment, which he has security cleared or approved, cf. art. 37.

CHAPTER II

**Classification, Storage, Handling and Communication of Classified Information**

Article 5

*Classification*

 Classified information shall be used exclusively for the purpose intended and shall be handled in accordance with its classification, as provided for in this article.

 Classified information may only be given to individuals who, in the course of their work, need access to the information and have been security cleared for that purpose according to this regulation.

 Confidential information shall be assigned a classification and such classification shall be clearly designated. Classification of confidential information is based on an evaluation of the damage that could result from its unauthorised release. Confidential data shall be classified and designated with one of the following security classifications, from the highest (a) to the lowest (d):

1. TOP SECRET ("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 particularly severe damage by its unauthorised release;
2. SECRET ("LEYNDARMÁL", "HEMMELIGT", "NATO SECRET", "SECRET UE" or equivalent) shall be used in cases when the security of Iceland, other states or international agencies, relations with foreign governments or international agencies or other vital interests of the State may be suffer severe damage by its unauthorised release;
3. CONFIDENTIAL ("TRÚNAÐARMÁL", "FORTROLIGT", "NATO CONFIDENTIAL", "CONFIDENTIEL UE" or equivalent) shall be used in cases when the security of Iceland, other states or international agencies, relations with foreign governments or international agencies or other vital interests of the State may suffer damage by its unauthorised release; and
4. RESTRICTED ("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 agencies or may have adverse effects on relations with foreign governments or international agencies if the information is released to unauthorised parties.

 Data designated as "NATO UNCLASSIFIED" are the property of the North Atlantic Treaty Organisation and NATO rules apply to their release.

 The originator of classified data shall ensure that they are designated by an appropriate security classification. Classified data shall not be designated by a higher security classification than is necessary. The validity period of a security classification according to this Article shall be no longer than necessary. Icelandic classified data to be transmitted abroad shall be designated as “ISL” plus the appropriate security classification (e.g. *“ISL Restricted”*), unless international agreements state otherwise.

Article 6

*Handling of Classified Information*

 Classified information shall be handled as follows:

1. the information shall be protected and kept in a secure manner;
2. if the information is used in new data, the data shall have the same security classification as the document of origin;
3. if the information is copied or translated, the document shall have the same security classification as the document of origin. The translation of such confidential document shall specify that the document contains classified information from the state or agency of origin,
4. if information with the security classification *"Top secret"* is no longer needed, it shall be put in long-term storage, cf. art. 13, it shall be destroyed, cf. art. 12 or it shall be returned to the state or agency of origin, as appropriate. Documents with the security classification *"Secret"* or below shall be destroyed as provided for in this regulation; and
5. if an emergency makes it impossible to protect classified information, the information shall be destroyed.

 Furthermore, it not permitted without prior written authorization from the state or agency from which the information originated:

1. to change the security classification of a document;
2. to translate, copy or destroy documents with the security classification *"Top secret"*;
3. to release classified information to other states, agencies or unauthorized parties, except by explicit authorisation and when strictly necessary; and
4. to transport classified information abroad, except with explicit authorisation and when strictly necessary.

Article 7

*Storage of Classified Information*

 Classified information shall be stored in secure storage units, a certified information system or in areas for this purpose where specific handling rules apply and are outfitted with special security systems. These areas are classified into:

1. secure area I;
2. secure area II; and
3. administrative area.

 Secure areas I and II are specifically defined and access controlled. They shall be equipped with a burglar-alarm with electronic sensors connected to a security centre. Secure area I is monitored 24 hours a day and only individuals with a security clearance may have access, except by permission of the security officer. Secure areas I and II may be combined if special circumstances allow and provided that the keeping of classified information is not put at risk.

 Classified information designated by the security classification:

1. *"Top secret"* shall be stored in secure area I;
2. *"Secret"* and *"Confidential"* shall be stored in secure areas I or II; and
3. *"Restricted"* shall be stored in secure areas I or II or in administrative areas, provided the information is stored in locked storage units or in a locked office in an administrative area.

 An individual in possession of classified information shall, upon leaving his or her office or workspace, ensure that the information is stored in certified and locked storage units in secure areas, i.a.w. para. 1, according to its security classification.

### Article 8

### *Communication of Classified Information*

 The Ministry for Foreign Affairs is responsible for domestic communication of classified information, i.e. information received from abroad on the basis of international agreements, unless they stipulate otherwise. Before the classified information is communicated, a security clearance and/or approval shall have been issued for:

1. the individual concerned, who is to receive the information, stating that he or she satisfies the conditions for access to classified information;
2. the company or agency concerned, which is to receive the information, stating that it has the appropriate facilities, if applicable, for storing classified information and for controlling access thereto; and
3. equipment, such as information systems, to store the information or communicate it, stating that it is satisfactory with regard to information security, if applicable.

 Article 9

*Security, Designation and Transport of Classified Information*

 The security of classified information shall be ensured during its entire life-cycle.

 Classified information designated as *"Confidential"* and above shall be recorded in a register where its reception, handling, distribution and destruction are entered, cf. art. 13.

 When classified information is transported between locations, it shall be double wrapped in non-transparent packaging or envelopes. The inner packaging shall be sealed and designated by the security classification, receiver and sender. The outer packaging shall be sealed and only designated by the receiver and sender. Classified information designated as *"Restricted"* may be sent by conventional mail in this manner.

 Classified information designated as *"Confidential"* and above shall only be transported between locations in possession of a security cleared individual who shall have knowledge of the rules applicable to the transport of classified information.

 When classified information designated as *"Confidential"* and above is transported between countries, the individual holding a security clearance undertaking its transport shall be in possession of formal courier certificate for confirmation purposes issued by the sending agency. The courier certificate shall specify from where and to which destination the delivery shall be transported, the courier's route and the reference number for the delivery. Classified information transported from one state to another shall be exempt from customs searches at the border, provided the courier has the above mentioned agency-issued courier certificate in his or her possession.

Article 10

*Re-assessment and Validity Period of Classified Information*

 The security classification of classified information shall be re-assessed regularly or at least every five years. In principle, confidential documents designated as *"Top secret"* shall be declassified after 30 years, those designated as *"Secret"* after 15 years, and those designated as *"Confidential"* after 5 years.

Article 11

*Computer Security*

 It is not permitted to convert classified information, falling under this regulation, into electronic form or transfer such information by electronic means, except via approved information systems, cf. art. 22. Such classified information may not be sent by regular e-mail.

 Security cleared individuals shall, during their absence, shut down their computers, in which classified information is stored. They may never release their username and/or password to anyone.

 An agency or company, which has a security approved information system, shall set rules on access control to classified information stored therein, in order to ensure that individuals, who have access to the information, have received an adequate security clearance as laid down in this regulation and by other applicable rules in force.

Article 12

*Reproduction of Confidential Documents, Destruction and Declassification*

 Confidential documents may only be photocopied in approved photocopying machines which are not connected on-line and ink cartridges shall be destroyed according to rules applicable to confidential documents.

 If a document with the security classification *"Confidential"* or higher is reproduced, the number of copies and names of the recipients shall be recorded. Only the necessary number of copies shall be made.

 Copies of confidential documents shall be destroyed after use in an approved shredder or by burning.

 If the security classification of a document is lowered or if it is declassified, the document's security classification shall be crossed out and the date of the adjustment and the initials of the person making the decision written on it, cf. also art. 6. The adjustment shall also be entered into the register of classified information.

Article 13
*Registry and Depository Body*

An agency or a company, where classified information is handled by its employees according to this regulation, shall operate a special registry ensuring that such information is handled according to this regulation. The registry shall include a register of classified information covering its full life-cycle from its creation or reception until it is put in permanent storage or destroyed. Each agency or company shall register the reception, handling, the person responsible, distribution, storage and destruction of classified data. Access to the registry shall be restricted.

A registry shall be located in a secure area, i.a.w. art. 7, and its registrar shall be security cleared up to the highest security classification of documents stored there or up to the security classification held by the company in question. A registry shall be kept separate from an agency's or a company's general archive. Registries shall be subject to inspection by the National Commissioner of Police every two years. Agencies and companies shall adopt a storage policy and rules on the operation of their registries.

When there is no longer a need for classified information it shall be transferred to a special security archive of the Minister responsible for defence or be destroyed according to this regulation.

Any requests for access to classified information shall be submitted to its originator according to its designation.

CHAPTER III

**Authorisation for Access**

Article 14

*Grant of Authorisation for Access*

 The director of an agency or the managing director of a company is responsible for granting an individual authorisation for access, i.e. an individual whose duties require access to classified information according to the provisions of this regulation.

 It is not permitted to grant anyone authorisation for access to classified information, areas, buildings, structures, equipment or security agreements without prior confirmation by the National Commissioner of Police that the individual concerned has the appropriate security clearance.

 If urgent situations, such as an overriding public interest, requires that an individual be given access, even if he or she does not have a security clearance from the National Commissioner of Police, this may be allowed provided that the security of classified information is not put at risk. The National Commissioner of Police shall be notified immediately of such exemptions, if granted.

Article 15

*Access to Classified Information*

 Before an individual is given classified information, designated as *"Confidential"* or above, he or she shall have received the appropriate security clearance according to this regulation. A security clearance for an individual is given for a specific security classification which shall not be higher than necessary.

 Data designated by the security classification *"Confidential"* or higher shall only be handled by parties that have a security clearance for that classification or higher.

 Although a security clearance for an individual authorises access to specific data, such access shall be limited to data on a need-to-know basis.

Article 16

*Access to Areas*

 Before an individual is given access to areas where classified information is kept or handled he or she shall have received the appropriate security clearance according to this regulation unless special security measures have been taken for their concealment and he or she is accompanied by a security cleared individual. In other respects the director of an agency or the security officer concerned shall give authorisation for access to such areas.

 The names of guests of an agency that obtain access to areas where classified information is kept or handled shall be registered and their time of arrival and departure. They shall always be in the company of a security cleared individual.

 The security officer may grant an employee of an agency, who has not received a security clearance, access to areas where classified information is kept, e.g. for maintenance or cleaning purposes, provided appropriate measures have been taken to conceal the information or the employee is in the company of a security cleared individual at all times.

Article 17

*Withdrawal of Authorisation for Access*

 An authorisation for access expires when:

1. an individual terminates his or her employment for which the authorisation was required;
2. the authorisation is no longer required for other reasons; or
3. the individual concerned is no longer in possession of a valid security clearance according to this regulation.

 If information emerges calling into question the security competence of a cleared individual the director of the agency or the managing director of the company concerned shall withdraw the authorisation for access, restrict it or suspend it. Such decision shall be notified immediately to the National Commissioner of Police who determines whether the individual should keep his security clearance unchanged.

 If the National Commissioner of Police withdraws a security clearance i.a.w. art. 28, authorisations for access shall also be withdrawn under this Article.

 The decision of a director of an agency or managing director of a company on withdrawal of authorisation for access is final.

Article 18

*Access for the Highest Members of Government*

 The President of Iceland and ministers who have not received a security clearance according to this regulation may be granted access to classified information. Before such access is granted, they shall be made aware of their obligations and responsibilities for confidentiality in handling classified information according to this regulation. The aforementioned parties are required to maintain strict confidentiality of the information they receive on the basis of this authorisation.

CHAPTER IV

**Security Clearance and Approval**

Article 19

*General Provisions on Security Clearance and Approval*

 The Minister responsible for defence is responsible for the issuance of security clearances and approvals according to this regulation. The National Commissioner of Police issues security clearances and approvals, acting on behalf of the Minister responsible for defence, according to this regulation.

Article 20

*Personnel Security Clearance*

 Before an individual receives a security clearance he or she shall have passed a background check, signed a solemn declaration of confidentiality with regard to the classified information he or she receives during his or her employment and be briefed on the rules on handling classified information by the National Commissioner of Police. The duty for confidentiality shall be maintained after employment is terminated or an assignment is completed.

 Background checks by authorities in another state shall be accepted in this country upon request if substantiated by appropriate documentation. When deciding on a security clearance in such cases an evaluation shall be made of the background check made by the national security authority of the individual's home state in question.

The National Commissioner of Police may decide to run a background check on an individual even if he or she has been given a background check in another state before he or she receives a security clearance under this regulation.

 Each agency or company, that has security cleared individuals as their employees, shall keep an updated register of its security cleared employees. A record shall be kept of the validity period of a security clearance, the security classification, whether it has expired, been withdrawn, suspended or is being processed.

 The security officer is responsible for ensuring that employees requiring a valid security clearance have such clearance of the appropriate security classification at all times.

Article 21

*Company Security Clearance*

 A company, including suppliers, service providers, parties seeking tenders, contractors or exporters, whose employees have access to classified information or facilities, where classified information is kept or handled, shall be security cleared. Members of the board of directors and managers of such company shall, along with the security officer, pass a security clearance i.a.w. art. 20.

 The issuance of a security clearance for a company shall be based on a request from a procuring entity (buyer) purchasing goods or services from the company (contractor). A procuring entity's application for a company security clearance shall be submitted on a form for that purpose from the National Commissioner of Police. A security agreement shall also have been concluded between the procuring entity and company concerned, cf. art. 25. A procuring entity may submit a request for a new company security clearance and/or for the upgrading of the company's security classification.

 Before an employee of a company gains access to classified information up to the security classification *"Confidential"* or above, or if this is otherwise considered necessary, he or she shall be security cleared up to the appropriate security classification.

 A security clearance shall not be issued for a company if there is reasonable doubt about the security competence of the company or its employees. Only ties relevant to the competence of the company or its employees and their will to implement preventive security measures as provided for in this regulation shall be assessed. In making that assessment a background check shall be run on the members of the board of directors and managers of the company i.a.w. art. 30, cf. art. 31 and 32.

 A company shall provide all information considered necessary for assessing its security competence or that of its employees for the purpose of determining security clearances.

 The managing director of a company shall inform the National Commissioner of Police without delay of any:

1. changes in the appointment of the members of their board of directors and/or their managers;
2. transfer of ownership of the company to new parties;
3. transfer of operations or equipment;
4. changes to housing, facilities or equipment that has been security approved earlier;
5. authorisation for the company for a moratorium on payments, to seek forced debt relief, to obtain debt relief or undergo insolvency proceedings; or
6. other issues that may affect the security competence of the company according to this regulation.

 If circumstances arise within a company that might threaten security according to this regulation and the threat cannot be mitigated by preventive security measures, the National Commissioner of Police may withdraw the security clearance of the company concerned i.a.w. the provisions of art. 28.

 Classified information or equipment where such information is kept may not be transferred to new owners of a company unless the new owners have security clearances according to this regulation. Equipment may nevertheless be transferred to new owners provided that all classified information has been deleted from the equipment according to this regulation.

 The Minister may conclude security agreements with domestic parties (exporters) in need of a security clearance for international trade purposes. The provisions of this Article and of art. 25 shall apply to such agreements *mutatis mutandis.*

 A security clearance may not be issued for a company, including suppliers, service providers, contractors or exporters, unless its employees who are to handle classified information according to this regulation, have passed background checks in accordance with art. 30, cf. art. 31 and 32, and, where applicable, the company's facilities meet the conditions set by art. 7 and 23.

 Article 22

*Security Approval of Information Systems and Equipment*

 Before classified information is handled, stored or communicated in a secure information system, the National Commissioner of Police shall approve the system up to the appropriate security classification.

 The National Commissioner of Police may entrust other parties, which have received appropriate clearances, to provide security service for information systems where classified information is handled.

 The National Commissioner of Police shall approve equipment, machinery and procedures for the destruction of classified information, cf. art. 12.

 Security approvals may not be issued for information systems or equipment unless they meet the security standards and requirements of the information system in question.

Article 23

*Facility Approval*

 The National Commissioner of Police shall issue facility approvals for housing, areas and facilities for use by those who handle and keep classified information according to this regulation. Such housing, areas and facilities shall meet the minimum security criteria and pass a security approval, cf. art. 7.

Article 24

*Validity Period of Security Clearances and Approvals*

 The validity period of a security clearance for an individual is as follows:

1. one year in case of an initial security clearance;
2. two to five years, as determined by the National Commissioner of Police, in case of a renewal; or
3. five years in case of a renewal of a security clearance for a permanently employed public servant who handles classified information on a regular basis.

 The validity period of a security clearance for a company shall be as follows:

1. two years in case of an initial security clearance; or
2. three to five years, as determined by the National Commissioner of Police, in case of a renewal.

 A different validity period for a security clearance from those stipulated in points (a) and (b) may be determined, according to the validity period of a security agreement.

 The validity period of security approvals for information systems and equipment shall be as follows:

1. of an interim approval to operate (IATO), maximum twelve months; or
2. of a security approval, maximum three years.

 The validity period of a facility approval shall be three years, unless it has been altered. Nevertheless, agencies may be given a facility approval for longer periods, even of unlimited duration, as the case may be, if justified for special reasons.

 The validity period of a security clearance and/or approval shall be clearly indicated at the time of issue.

 A security clearance expires when:

1. its validity period comes to an end;
2. a security agreement i.a.w. art. 25 expires or the validity period of an assignment comes to an end;
3. an individual, for whom a security clearance was required, terminates his or her employment;
4. the company in question is declared bankrupt or terminates its business activities; or
5. the need or prerequisite for a security clearance cease to exist for other reasons.

 A security approval expires when:

1. its validity period comes to an end;
2. information systems and equipment no longer meet the requirements of this regulation;
3. the facilities of a company or agency have been altered or they no longer meet the requirements of this regulation;
4. the company, where the equipment is kept, becomes bankrupt or terminates its business activities; or
5. the need for a security approval ceases to exist for other reasons.

Article 25

*Security Agreements*

 An agency, which keeps classified information according to this regulation, shall conclude a security agreement with those suppliers and service providers that, because of their business relations, need access to such information. Such agreements are a prerequisite for the National Commissioner of Police's security clearance of a company i.a.w. art. 21 to the appropriate security classification, if applicable.

 The National Commissioner of Police may decide that a security agreement i.a.w. para. 1 shall be concluded if a supplier or service provider needs access to a security approved computer system or storage place or if a security agreement is considered necessary for other reasons. A security agreement shall be concluded before suppliers or service providers are given access to classified information.

 A security agreement, which shall be in the form of an annex to a contract concerning the security classified purchase of goods or services or an invitation to tender, shall provide for responsibilities and obligations according to this regulation, including with regard to:

1. the security classification of the business relationship, specifically indicated for each part of the assignment;
2. the running of a background check on a supplier or service provider and other control to assess security factors and whether a supplier or service provider gives effect to the security provisions of the contract and meets other obligations according to this regulation;
3. the validity period of a security agreement, if applicable; and
4. the consequences of a violation of a security agreement, including contractual fines.

 Expenses or requirements incurred or undertaken by a supplier or service provider in complying with the provisions of this regulation or provisions related thereto and accepted in a security agreement are of no consequence to the procuring entity or the National Commissioner of Police, unless expressly so indicated in the security agreement.

Article 26

 *Denial of a Personnel Security Clearance*

 An individual, for whom a security clearance has been requested, shall be notified of the results of the background check i.a.w. art. 30, cf. art. 31 and 32, as soon as possible. An individual may not be given a security clearance, who, in the view of the National Commissioner of Police, does not meet the criteria for determining his or her security clearance i.a.w. art. 31 and 32.

 A denial of a security clearance shall be subject to the procedures of the Administrative Procedures Act. Should the National Commissioner of Police decide to deny a security clearance for an individual on the basis of a background check, the National Commissioner of Police shall inform the individual concerned of the intended denial and justified reasons therefor. Nevertheless, the justification shall not include information that is essential to keep confidential because it:

1. is essential for, or may be detrimental to, the security of Iceland, states with which it has cooperation, relations with foreign governments or other essential security interests of the State;
2. is essential for the protection of sources of information;
3. concern the individual's relations with other individuals close to him or her that is not desirable he or she should know about;
4. concerns technical equipment, production information, business analysis or accounts, trade secrets or is of a kind that others may use in their activities; or
5. concern criminal matters or police investigations that concern the individual in some manner and cannot be revealed.

Before a denial of a security clearance is issued, the individual shall be given an opportunity to object, according to the provisions of the Public Administration Act.

If the National Commissioner of Police decides, after an individual has been given an opportunity to object, to deny a security clearance that decision shall be formally notified to that individual and to the requestor of the background check. The National Commissioner of Police's decision to deny a security clearance shall always be reasoned, albeit cf. para. 2, in accordance with the provisions of the Public Administration Act. Nevertheless, the requestor for the background check shall only be notified of the denial of the security clearance on the basis of this regulation, without further justification or explanation. The National Commissioner of Police's decision shall include guidance on how to appeal to the Minister responsible for defence, according to the provisions of the Public Administration Act.

 A party to a case may see documents and other information concerning the matter at hand according to the provisions of the Public Administration Act, with such exceptions as are contained therein. The National Commissioner of Police may also, in special circumstances, restrict a party's access to information if his interest in using the knowledge contained therein should give way to a greater public or private interest, cf. the provisions of the Public Administration Act. Such assessment shall i.a. take account of the items specified in para. 2. The merits of the case in question should be evaluated in each instance.

Article 27

*Denial of a Company Security Clearance*

 The director of an agency or the managing director of a company, for which a company security clearance has been requested, shall be notified of the check result i.a.w. art. 21 - 23, cf. art. 7, as soon as possible. A company or agency, facilities, information systems or equipment shall not be given a security clearance or approval if, in the view of the National Commissioner of Police, the criteria, i.a.w. art. 21 - 23, cf. art. 7, are not met.

 If a denial of company security clearance is foreseen, the procedures of the Administrative Procedures Act shall be applied with regard to parties' right to provide justification and objection before a final decision is made.

If the National Commissioner of Police determines that a company security clearance should be denied this decision shall be notified to the director of the agency or managing director of the company.

Article 28

*Withdrawal of a Security Clearance*

 The security officer shall immediately notify the National Commissioner of Police of the termination of employment of any individual who has received a security clearance according to this regulation or if the security clearance of an employee is no longer needed. The National Commissioner of Police shall immediately withdraw his security clearance.

 The security officer shall also without delay notify the National Commissioner of Police of any change in circumstances of a company, such as change of ownership, financial standing, housing, areas, employees or other issues of relevance that could affect the company's or its employees' security competence for a security clearance. The National Commissioner of Police shall then determine immediately whether the company's security clearance should be withdrawn, and if so, make such withdrawal according to the provisions of this Article, as appropriate.

 If the validity period of a security clearance expires the National Commissioner of Police shall notify the individual concerned and the security officer of the agency or company of the expiration of the security clearance.

 If information emerges that may have effect on the security competence of a security cleared individual the National Commissioner of Police shall be informed immediately who shall determine whether the individual's security clearance should be suspended or withdrawn and the case examined further.

 If the National Commissioner of Police decides to withdraw or suspend a security clearance this shall be notified to the individual concerned without delay and to the company or agency which applied for the security clearance for the individual concerned.

 In case an individual's security clearance is withdrawn the procedures of art. 26 shall apply. The National Commissioner of Police may suspend a security clearance during an appeals procedure i.a.w. art. 38.

 The managing director of a company shall be notified of a planned withdrawal of a security clearance and of the reasons there for and shall be given opportunity to object according to the provisions of the Public Administration Act. The final decision of the National Commissioner of Police to withdraw a company's security clearance shall be reasoned according to the provisions of the Public Administration Act.

Article 29

*Withdrawal of Security Approvals*

 The security officer shall, without delay, notify the National Commissioner of Police of any changes made to an information system, equipment, facilities or space of a company or an agency, which has received a security approval according to this regulation or if there is no longer a need for a security approval. The National Commissioner of Police shall immediately withdraw the security approval in question, as appropriate.

 If the validity period of a security approval expires, the National Commissioner of Police shall immediately notify the security officer of the agency or company concerned.

 If information emerges that may have an effect on a security approval according to this regulation, the National Commissioner of Police shall be so informed without delay who shall determine whether the security approval should be suspended or withdrawn and the case examined further.

 If the National Commissioner of Police decides to withdraw or suspend a security approval, this shall be notified immediately to the security officer of the agency or company which applied for the approval.

 The director of an agency or the managing director of a company shall be notified of a planned withdrawal of a security approval and of the reasons there for and shall be given an opportunity to make use of his right to object, according to the provisions of the Public Administration Act. The final decision of the National Commissioner of Police to withdraw an agency's or a company's security approval shall be reasoned according to the provisions of the Public Administration Act.

CHAPTER V

**Background Check**

Article 30

*Running of a Background Check on an Individual*

The National Commissioner of Police runs a background check on an individual at the request of the party responsible for granting access according to Chapter III. The Minister decides which companies or agencies are competent to submit requests for security clearances according to this regulation.

A background check may i.a. include, for the individual concerned, an examination of police records, including police case lists, an examination of his or her judicial record, Interpol's information system, the SIS-information system, information from the national registry (Records Iceland), as appropriate, inquiries to foreign authorities, an examination of customs authorities' records, district courts records and other public records.

When issuing a security clearance up to the security classifications *“Confidential”* and *"Secret"* a background check should run at least five years back. When issuing a security clearance up to the security classification *"Top secret"* a background check should run at least ten years back.

A background check shall include an assessment of the information provided by the individual himself, of information held by the National Commissioner of Police and, as appropriate, found in public records, cf. para, 2. Agencies requested by the National Commissioner of Police for information in connection with a background check are required to release information from their records to the National Commissioner of Police. Information from records shall be released in writing or electronically. Background checks may include other sources as well, e.g. information from places of work, government agencies and from other sources, where applicable. Information collected in connection with a background check shall be submitted to the National Commissioner of Police free of charge.

A background checks shall not be run unless the individuals concerned has been informed of its necessity and from where information will be collected and unless formal consent has been given on a form from the National Commissioner of Police. By giving his or her consent the individual concerned agrees to provide complete and correct information, i.a. on any relationship that may affect the assessment of his or her security competence.

A background check shall be more complete as the security classification gets higher. A security clearance for the security classification *"Secret"* or above, or in other special cases, can cover individuals with family ties to the individual concerned or reside with him or her, provided those individuals have given their informed consent.

Information provided to the National Commissioner of Police in connection with a background check shall not be used for other purposes than a security clearance according to this regulation. Measures shall be taken to ensure that only employees working with security clearances have access to that information.

Article 31

*Criteria for Deciding on a Personnel Security Clearance*

 A security clearance shall only be issued or renewed if the individual concerned passes a background check i.a.w. art. 30, cf. also the criteria established in this Article, cf. also art. 32. When assessing an individual's security competence to handle classified information the following factors shall be taken into account, as concerns reliability, integrity and judgement of the individual in question:

1. the fact that he or she has been linked to acts of sabotage, espionage or their planning, to attempted attacks or other such acts;
2. if he or she has committed a crime or a criminal offence or has abetted others in committing such acts;
3. if ties exist that that can lead the individual himself or a close relative to being threatened with loss of life, health, privacy or dignity and may force him or her to commit acts that could endanger the security of classified information;
4. if he or she has given false or incorrect information or has deliberately suppressed information that the individual should have known would influence the outcome of an assessment for issuing a security clearance;
5. if he or she has a history of abuse of alcohol or drugs;
6. if he or she has a medical condition requiring medication than can have an effect on reliability, integrity or judgement;
7. if he or she has been involved in compromising classified information, has broken security rules, has refused to provide personal information about him or herself, does not authorise the National Commissioner of Police to conduct examinations deemed essential and necessary for a background check, refuses to promise confidentiality, indicates that he or she does not wish to be subject to confidentiality requirements or refuses an interview summoned by the National Commissioner of Police;
8. if there are economic factors that can lead to dishonesty;
9. if he or she has ties with individuals or parties, such as associations, companies, societies or groups, domestically or abroad, that have illegal objectives, can threaten democratic society, are associated with the planning, preparation or commission of organised crime, drugs abuse, espionage, sabotage or terrorism;
10. if there are insufficient opportunities to run a background check;
11. if he or she has ties with foreign countries; and
12. if there are other factors present that can give rise to suspicion that the individual in question could engage in activities that might threaten security interests according to this regulation.

 A decision to issue or deny a security clearance, cf. art. 26, shall be based on an informed, clear, objective and individually-based, comprehensive assessment of available information. Political ties, including participation in legitimate political parties or entities or in any lawful societies shall not have effect on the individual's qualifications in connection with a security clearance. Negative information on a close relative shall only be taken into account if their ties are deemed to have an effect on the conduct and security competence of the individual to be given a security clearance.

 A security clearance shall not be issued until the individual concerned has received appropriate training by the national security authority. In special cases the National Commissioner of Police may set other objective conditions for issuing a security clearance.

### Article 32

#### Assessment of Criminal History

###  If a background check i.a.w. art. 30 and 31 reveals that an individual has broken the law, or if there is suspicion that the he has broken the law, the National Commissioner of Police may base his decision on whether or not to issue security clearance for the individual concerned on the criteria set out in this Article.

When deciding on whether to issue a security clearance for an individual his or her criminal records shall be examined. Such decision shall be based on information from the judicial record and as appropriate other police records on the individual concerned, cf. art. 30.

If an individual has been fined, domestically or abroad, or has been convicted or has pending cases against him or her in the criminal justice system, where he or she is suspected or accused of committing a criminal offence punishable under Icelandic law, the National Commissioner of Police shall deny him or her a security clearance, provided offence is serious or indicates that the security of the State and/or public interest may be compromised.

The National Commissioner of Police shall also deny a security clearance if an individual has been convicted of a serious offences, e.g. violations of the General Penal Code, use or distribution of narcotic drugs, illegal use or distribution of weapons, serious violations of the Customs Code, violations that have endangered someone's life, acts of violence, blackmail, violations that threaten State security, sexual offences or is or has been a member of illegal associations or alleged criminal associations.

The National Commissioner of Police may decide to deny a security clearance for an individual for other violations than those listed in this Article provided they are based on objective grounds.

Furthermore, the following circumstances may be taken into account:

1. the individual concerned has been indicted for a criminal offence assumed to carry imprisonment; or
2. an individual is wanted by the police, a warrant has been issued for his or her arrest or he or she is subject to a travel ban according to the provisions of the Criminal Judicial Proceedings Act No 88/2008.

If a background check i.a.w. art. 30 and 31 reveals that the police has repeatedly intervened over an individual because of his or her alleged violations, the National Commissioner of Police may deny him or her a security clearance.

 Article 33

*Repeat of a Background Check*

The National Commissioner of Police may repeat a background check for an individual, of his own accord or on application by a competent party and with the informed consent of the individual concerned. In such cases the National Commissioner of Police may use available data and information, as much as possible, and may also seek further data and information if needed.

The National Commissioner of Police may also, of his own accord or on application by a competent party, perform random checks on those individuals that have passed background checks as long as their security clearances are in effect.

CHAPTER VI

**Miscellaneous Provisions**

Article 34

 *Individual's Obligation to Provide Information*

 An individual, who has received a security clearance according to this regulation, shall inform the security officer of everything that may affect his or her security competence. The security officer shall immediately inform the National Commissioner of Police thereof who shall assess if there are grounds for withdrawing the security clearance of the individual concerned i.a.w. art. 28.

Article 35

*Further Details on Implementation*

 In implementing this regulation, the following shall be taken into account *mutatis mutandis*:

1. North Atlantic Council Document No C-M(2002)49 of 17 June 2002 on security within the North Atlantic Treaty Organisation;
2. Council Decision (EU) No 2011/292/EU of 31 March 2011
on the security rules for protecting EU classified information; and
3. other international agreements and rules on their elaboration, as appropriate.

Article 36

*Confidentiality*

 Employees of the National Commissioner of Police shall maintain confidentiality with respect to all information obtained in the process of a background check that shall be kept confidential.

 Access of employees of the National Commissioner of Police to classified information i.a.w. para. 1 is determined by their role within the police force.

Individuals who, in the course of their work, obtain knowledge of the result of a background check on an individual run by the National Commissioner of Police shall maintain strict confidentiality with respect to its content.

Individuals, contractors or other parties who, in the course of their work, obtain access to classified information shall maintain strict confidentiality with respect to its content. They may not reveal to unauthorised parties what they learn in the course of their work that shall be kept confidential, otherwise they will remain answerable.

Confidentiality shall be maintained even after employment is terminated or a contract is completed.

Article 37

*Inspections by the National Commissioner of Police*

The National Commissioner of Police supervises security factors within agencies and companies regarding the implementation of this regulation, including whether they fulfil their obligations under laws and regulations, and prescribes improvements.

The National Commissioner of Police conducts regular inspections of facilities, areas, housing, installations, machinery, information systems or equipment and other items owned, used or otherwise controlled by an agency or a company, in order to assess whether unauthorised parties can, with or without technical means, see, hear or read classified information.

 The National Commissioner of Police shall have free access to any area where classified information or equipment for handling classified information is kept, in order to be able to conduct adequate inspections.

If it is revealed, by a security inspection by the National Commissioner of Police according to this Article, that an agency or company no longer meets obligations according to law or this regulation or faults are found with regard to specific issues the National Commissioner of Police shall send a report on the matter to the party in question as soon as possible after the inspection is concluded. The party shall be given a reasonable delay for improvements, in the view of the The National Commissioner of Police. If improvements are not brought about within the set time limit, the National Commissioner of Police can withdraw a security clearances and/or approval issued on the basis of this regulation and notify the international organisation concerned thereof, as appropriate.

 On average, inspections shall be conducted at 24 month intervals. The National Commissioner of Police shall issue operational rules for conducting security inspections according to this Article.

Article 38

*Filing of a Complaint*

 If a security clearance for an individual is denied on the basis of a background check, cf. art. 26, or a security clearances of an individual is withdrawn, cf. art. 28, a complaint may be filed with the Minister responsible for defence according to the provisions of the Administrative Procedures Act.

Article 39

*Penalties*

 Violations of this regulation shall be punishable according to the following provisions, unless more severe penalties apply pursuant to other laws:

1. chapters XIV and XVII of the General Penal Code No 19/1940;
2. art. 28 the Defence Act No 34/2008; and/or
3. art. 13 of the Act on control of services and items which may have strategic significance No 58/2010.

Article 40

*Entry into Force etc.*

 This regulation is adopted i.a.w. art. 24 and 27 of the Defence Act No 34/2008 and taking into account art. 15 and 18 of the Act on the rights and obligations of government employees No 70/1996.

 The provisions on security clearances for companies with relation to export interests are adopted i.a.w. art. 14 of the Act on control of services and items which may have strategic significance No 58/2010.

 This regulation enters into force immediately. Security clearances and/or approvals in force shall remain valid throughout their validity period or until new security clearances and/or approvals have been issued.

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*