Väljaandja:	Vabariigi Valitsus
Akti liik:	välisleping
Teksti liik:	algtekst
Jõustumise kp:	30.01.2002
Avaldamismärge:	RT II 2002, 7, 20

Eesti Vabariigi ja Rootsi Kuningriigi üldine salastatud teabe kaitse julgeolekukokkulepe

Vastu võetud 30.01.2002

«Eesti Vabariigi ja Rootsi Kuningriigi üldise salastatud teabe kaitse julgeolekukokkuleppe» eelnõu heakskiitmine ja volituste andmine

Välisministeeriumi teadaanne välislepingu jõustumise kohta

Eesti Vabariigi ja Rootsi Kuningriigi vahelise üldise salastatud teabe kaitse julgeolekukokkuleppe muutmise protokoll

S i s u k o r d

Eesti Vabariik ja Rootsi Kuningriik, edaspidi nimetatud «pooled», on oma riikliku julgeoleku huvides sõlminud käesoleva üldise julgeolekukokkuleppe eesmärgiga kaitsta heakskiidetud kanalite kaudu kahe maa vahel edastatavat salastatud teavet, mida edastatakse mõlema maa kaitsealase uurimistöö, tootmise ja hangete eesmärgil või kummagi maa äri- ja tööstusorganisatsioonide jaoks.

Käesolevat kokkulepet tõlgendatakse lähtuvalt riiklikest õigusaktidest.

Artikkel 1. Mõisted

1. Selguse huvides on defineeritud järgmised mõisted.

• «Salastatud teave» tähendab salastatud teavet, mis on edastatud kas suuliselt või nähtavana või elektrilisel või elektroonilisel teel, või materjali, mille avalikustamist peab riikliku julgeoleku huvides vältima ja mida peab lekke eest kaitsma.

• «Materjal» tähendab masina, varustuse või relva valmis või tootmisjärgus osist või dokumenti.

• «Dokument» tähendab jäädvustatud salastatud teavet, mis võib esineda kirja, noodi, protokolli, ettekande, memorandumi, leppemärgi või teate, toodetava eseme visandi, foto, filmi, kaardi, diagrammi, märkmiku, toodetava eseme šablooni, kopeerpaberi, kirjutusmasina lindi või disketi kujul või muus vormis (nt lindistus, magnetsalvestis, perfokaart, lint jms).

• «Lepingupartner» tähendab füüsilist või juriidilist isikut, kellel on õigus sõlmida lepingut.

• «Leping» tähendab kokkulepet ühe või mitme osapoole vahel, mis loob ja määratleb pooltevahelisi kehtivaid õigusi ja kohustusi.

• «Salastatud leping» tähendab lepingut, mis sisaldab salastatud teavet või mille sisu on sellega seotud.

• «Pädev asutus või määratud julgeolekuasutus» (viimasena nimetatu edaspidi «julgeolekuasutus») tähendab valitsusasutust, kes asjaomases riigis vastutab salastatud teabe kaitse eest.

• «Teavet edastav pool» tähendab pädeva asutuse või julgeolekuasutuse kaudu esindatavat lepingupoolt, kes salastatud teavet edastab.

• «Teavet vastuvõttev lepingupool» tähendab pädeva asutuse või julgeolekuasutuse kaudu esindatavat lepingupoolt, kellele salastatud teave edastatakse.

• «Salastatuse tasemed» ja nende ekvivalendid mõlemal maal on:

Eestis	**Rootsis**
TÄIESTI SALAJANE	KVALIFICERAT HEMLIG
SALAJANE	HEMLIG
KONFIDENTSIAALNE	HEMLIG

Rootsi salastatud teave, mida edastatakse Eesti Vabariiki, tuleb, kus iganes võimalik märgistada nii Rootsi salastatuse tasemega, kui ka sellele vastava Eesti salastatuse tasemega.

Vajadusel võib kumbki pool paluda teist poolt osutada teabele omistatud salastatuse tasemest kõrgemal tasemel kaitset. Madalamal tasemel kaitset ei saa osutada.

Artikkel 2. Pädevad asutused

Pädevad julgeolekuasutused, kes vastutavad kaitsealase julgeoleku eest mõlemal maal on:

Rootsis

Pädev asutus, kes Rootsis vastutab kaitsealase julgeoleku eest on:
Försvarsmakten(Rootsi relvajõud), Peakorter, Sõjaväeluure ja julgeolek (MUST), SE-107 86 Stockholm, Rootsi; telefon: 46 8 788 7500; faks: 46 8 788 8263.

Määratud julgeolekuasutus Rootsis, kes vastutab kaitsealase materjaliga seotud riigikaitsealase julgeoleku eest on:
Försvarets Materielverk(Rootsi kaitsealaste materjalide administratsioon), Julgeolek, SE-115 88 Stockholm, Rootsi; telefon: 46 8 782 4000; faks: 46 8 660 2251.

Eestis

Pädev asutus Eestis, kes on vastutav riigikaitsealase julgeoleku eest:
Riigisaladuse kaitse osakond, Kaitseministeerium, Sakala 1, 15094 Tallinn, Eesti; telefon: 372 640 6030; faks: 372 640 6002.

Artikkel 3. Kasutamise ja avalikustamise piirangud

(1) Vastuvõtjad ei avalikusta ja ei kasuta salastatud teavet ning ei luba selle avalikustamist või kasutamist ilma eelnevate konsultatsioonideta, välja arvatud teavet edastava poole poolt näidatud eesmärkidel ja ulatuses.

(2) Teavet vastuvõttev pool ei anna edasi või ei avalikusta valitsusametnikule, lepingupartnerile või lepingupartneri töötajale või ükskõik millisele teisele isikule, kes on kolmanda maa kodanik või ükskõik millisele rahvusvahelisele organisatsioonile mitte mingisugust salastatud teavet, mis on vahetatud käesoleva lepingu kohaselt ega ei avalikusta üldsusele ilma edastava poolega konsulteerimata mingit osa salastatud teabest.

(3) Käesolev kokkulepe ei sisalda midagi, mis reguleeriks autoriõiguste loovutamist, kasutamist, vahetamist või avalikustamist või mida saaks võtta kui volitust selleks, kuni ei ole eelnevalt saadud spetsiaalset volitust nende õiguste omanikult, olenemata kas omanik on üks pooltest või on ta kolmas isik.

Artikkel 4. Salastatud teabe kaitse

(1) Teavet edastav pool peab kindlustama, et teavet vastuvõttev pool on informeeritud:
(a) teabe salastatuse tasemest ja ükskõik millistest täiendavatest tingimustest selle avalikustamisel või kasutamise piirangutest ja et dokumendid on sellisena märgistatud; ja
(b) igast hilisemast salastatuse taseme muutusest.

(2) Teavet vastuvõttev pool peab:

(a) võimaldama vastavuses oma riiklike õigusaktidega salastatud teabele samasuguse kaitse nagu teabe edastaja. Teavet vastuvõttev pool peab ükskõik millisel õiguslikult lubataval viisil hoidma edastatud salastatud teavet avalikustamise eest ükskõik millisel õiguslikul alusel; ja kumbki pool peab tagama arvestuse ja kontrolli protseduurid korraldamaks salastatud teabe jaotamist ja juurdepääsu sellele;
(b) tagama, et salastatud teave on märgistatud vastavuses artikliga 1; ja
(c) tagama, et salastatuse taset muudetakse ainult teavet edastanud poole või tema esindaja kirjalikul loal.

(3) Saavutamaks ja hoidmaks julgeoleku võrreldavaid standardeid peab iga pädev asutus / julgeolekuasutus esitama nõudmisel teisele informatsiooni oma julgeolekustandardite, protseduuride ja salastatud teabe kaitse praktika kohta ja sel eesmärgil võimaldama pädevate asutuste visiite.

Artikkel 5. Juurdepääs salastatud teabele

Salastatud teabele juurdepääsu võib lubada neile isikutele, kellel on «põhjendatud teadmisvajadus» ja kes on läbinud asjaomase pädeva asutuse / julgeolekuasutuse julgeolekukontrolli, mis on vastavuses tema riiklike standarditega ja vastab selle teabe tasemele, millele juurdepääsu võimaldatakse.

Artikkel 6. Salastatud teabe edastamine

(1) Salastatud teavet edastatakse kahe maa vahel vastavalt teavet edastava poole riiklikele julgeolekujuhenditele. Üks võimalus on teha seda ametlike valitsusvaheliste diplomaatiliste kanalite kaudu, aga võib kasutada ka teisi viise, nagu käsipost, turvatud teabeedastus (krüpteerimine), kui see on vastastikku vastuvõetav mõlemale poolele. Salastatud teavet vastuvõttev pool peab teabe vastuvõtmisest kirjalikult teatama.

(2) Lisaks sellele võib salastatud teavet edastada Rootsi äriühing ja Eesti omanduses olev äriühing Rootsi Kuningriigis või Eesti äriühing ja Rootsi omanduses olev äriühing Eesti Vabariigis, kasutades riiklike teabe edastamise juhiseid, mis on kasutusel ettevõtte asukohamaal. Edastamine võib aset leida ainult nende ettevõtete vahel, millel on asjakohased asutuse ja isikute riigisaladusele juurdepääsu load (vt artikkel 9(1)) ja kui on antud nõusolek selle teabe edastamiseks teise riiki.

Artikkel 7. Visiidid

(1) Külastajate, kaasa arvatud teisest riigist teenistusse lähetatute suhtes, kellel on vajadus juurdepääsuks salastatud teabele või riigikaitseliste asutuste / salajasele koostööle kaasatud lepingupartneri territooriumile, on vajalik vastuvõtva riigi pädeva asutuse / julgeolekuasutuse nõusolek. Selliste visiitide taotlused esitatakse asjaomaste saatkondade kaudu.

(2) Visiiditaotlus peab sisaldama:
– külastaja perekonna- ja eesnime, andmeid sünnikoha ja -kuupäeva, kodakondsuse kohta ning passinumbrit;
– andmeid külastaja ametikoha kohta ning selle asutuse, ettevõtte või organisatsiooni nime, mida külastaja esindab või kuhu ta kuulub;
– tõendit, mis näitab külastaja juurdepääsuloa taset;
– külastatava asutuse, ettevõtte või organisatsiooni nime ning aadressi;
– külastatava(te) isiku(te) nime ja ametikohta, kui need on teada;
– visiidi eesmärki;
– saabumis- ja lahkumisaega ning visiidi kestvust. Korduvate visiitide korral peab näitama ajavahemiku, mille jooksul visiidid toimuvad.

(3) Kõik külastajad peavad järgima vastuvõtva riigi julgeolekunõudeid.

(4) Visiiditaotlused tuleb esitada vastuvõtvale poolele vastavalt vastuvõtva poole protseduuridele. Lühikese etteteatamistähtajaga visiite on võimalik korraldada edasilükkamatutel juhtudel eriliste vastastikku määratletud kokkulepete alusel.

(5) Eriprojekti või konkreetset lepingut puudutavatel juhtudel on võimalik kummagi poole heakskiidul luua korduvate külastajate nimekirju. Nimekirjad võivad algselt kehtida perioodi vältel, mis ei ületa kahteteist (12) kuud ja neid võib pikendada lisaperioodiks (mis ei tohi ületada kahteteist (12) kuud), pikendamine toimub pädeva asutuse eelneva nõusoleku alusel. Nimekirjad tuleb esitada vastavuses vastuvõtva poole protseduuridega. Kui nimekiri on heaks kiidetud, võivad need asutused ja äriühingud, kelle esindajad on selles nimekirjas, visiitide suhtes kokku leppida otse.

(6) Külastajad peavad käsitlema salastatud teavet, mida võidakse neile anda või mis võib neile teatavaks saada, nii, nagu oleks see teave edastatud vastavalt käesoleva kokkuleppe tingimustele.

Artikkel 8. Lepingud

(1) Kui tehakse ettepanek sõlmida või riik volitab lepingupartnerit sõlmima salastatud teavet puudutavat lepingut teises riigis asuva lepingupartneriga, siis teavet edastav pool peab saama eelneva kinnituse teise

riigi pädevalt asutuselt / julgeolekuasutuselt, et pakutav lepingupartner on läbinud asjakohasel tasemel julgeolekukontrolli ja tal on kasutusel asjakohased julgeolekumeetmed tagamaks salastatud teabele vajalikku kaitset. Juurdepääsuluba tähendab vastutust selle eest, et kontrollitud lepingupartner on korraldanud julgeoleku vastavuses riiklike julgeolekut reguleerivate seaduste ja määrustega ning ta on tema pädeva asutuse / julgeolekuasutuse järelevalve all.

(2) Pädev asutus peab tagama, et lepingupartnerid, kes sõlmivad nende lepingueelsete uuringute tagajärjel lepingu, on teadlikud järgnevatest sätetest:
(a) salastatud teabe mõistest ja vastavuses käesoleva lepingu tingimustele kahe poole võrreldavatest salastatuse tasemetest;
(b) kummagi maa valitsusasutuste, kellel on volitused edastada ja koordineerida lepinguga seotud salastatud teabe kaitset, nimedest;
(c) valitsusasutuste ja/või lepingupartnerite vahel salastatud teabe edastamiseks kasutatavatest kanalitest;
(d) salastatud teabega seotud muudatuste tekkimisel neist teatamise protseduuridest ja mehhanismidest nii salastatuse tasemete muutmisel kui kaitsevajaduse äralangemisel;
(e) visiitide, juurdepääsu või ühe poole töötajate poolt teise poole ettevõtetesse tehtavate inspektsioonide heakskiitmise lepingus sisalduvatest protseduuridest;
(f) kohustusest, et lepingupartner avalikustab salastatud teavet ainult isikule, kes on eelnevalt läbinud julgeolekukontrolli, kellel on «põhjendatud teadmisvajadus» ja kes on töösuhetes või muul viisil seotud lepingu täitmisega;
(g) kohustusest, et lepingupartner ei avalikusta salastatud teavet või ei luba selle avalikustamist ühelegi isikule, kellele ei ole selgesõnaliselt kirjalikult lubanud sellist juurdepääsu lepingupartneri pädev asutus / julgeolekuasutus;
(h) kohustusest, et lepingupartner peab viivitamata teavitama lepingupartneri pädevat asutust / julgeolekuasutust igast toimunud või oletatavast julgeolekumeetmete rikkumisest või lepingus sisalduva salastatud teabe lekkest.

(3) Teavet edastava poole pädev asutus peab andma teavet vastuvõtva poole pädevale asutusele kaks koopiat salastatud lepingu asjassepuutuvatest osadest, võimaldamaks küllaldast julgeolekualast järelevalvet.

(4) Kõik lepingud peavad sisaldama julgeolekunõuete ja lepingu iga osa salastamise juhiseid. Rootsis antakse sellised juhised eraldi julgeolekukokkuleppega. Juhised peavad määratlema lepingu iga salastatud osa või salastatud osa, mis luuakse lepingu alusel, ja määrama sellele eraldi salastatuse taseme. Muudatustest nõudmistes või lepingu osades antakse teada igal ajal, kui see on vajalik ja teavet edastav pool peab teavitama teavet vastuvõtvat poolt, kui kogu see informatsioon kaotab oma salastatuse.

Artikkel 9. Vastastikused tööstusjulgeolekualased korraldused

(1) Iga pädev asutus / julgeolekuasutus peab teavitama teist poolt viimase nõudmisel oma riigis asuva äriühingu territooriumi julgeolekualasest staatusest. Iga pädev asutus / julgeolekuasutus peab samuti teatama iga oma kodaniku juurdepääsuloa tasemest, kui seda nõutakse. Need teated käsitletakse vastavalt asutuse juurdepääsuloana (FSC) ja üksikisiku juurdepääsuloana (PSC).

(2) Kui nõutakse, siis pädev asutus/julgeolekuasutus määrab kindlaks taotluses toodud äriühingu/üksikisiku juurdepääsuloa staatuse ja edastab juurdepääsuloa, kui äriühing/üksikisik on juba kontrollitud. Kui äriühing/ üksikisik ei oma juurdepääsuluba, või juurdepääsuluba on nõutavast madalama tasemega, tuleb saata teade, et juurdepääsuluba ei saa koheselt välja anda, aga taotluse rahuldamisega on asutud tegelema. Edukate järelepärimiste tulemusel väljastatakse juurdepääsuluba, mis võimaldab vastastikust juurdepääsulubade väljaandmist.

(3) Äriühing, mis oma asukohamaa pädeva asutuse / julgeolekuasutuse arvates on kolmanda riigi, mille eesmärgid on vastuolus asukohamaa huvidega, mõju all, ei vasta juurdepääsuloa saamise eeltingimustele ja sellest teavitatakse taotluse esitanud pädevat asutust / julgeolekuasutust.

(4) Kui kumbki pädev asutus / julgeolekuasutus saab ükskõik millist kahjustavat teavet isiku kohta, kellele on antud üksikisiku juurdepääsuluba, siis teavitab ta teist pädevat asutust / julgeolekuasutust informatsiooni iseloomust ja oma kavatsevast tegevusest või sellest, mida ta on ette võtnud. Põhjendatud taotluse korral võib kumbki pädev asutus/julgeolekuasutus nõuda teise pädeva asutuse / julgeolekuasutuse poolt iga eelnevalt väljastatud üksikisiku juurdepääsuloa ülevaatamist. Taotluse esitanud pädevat asutust / julgeolekuasutust teavitatakse ülevaatamise tulemustest ja igast sellele järgnenud tegevusest.

(5) Kui saadakse informatsiooni, mis tekitab kahtlusi vastastikku juurdepääsuloa saanud äriühingu sobivusse saada salastatud teabele jätkuvalt juurdepääsu teises riigis, siis antakse selle informatsiooni detailid koheselt pädevale asutusele / julgeolekuasutusele uurimise läbiviimiseks.

(6) Kui kumbki pädev asutus / julgeolekuasutus peatab teise maa kodanikule juurdepääsuloa alusel antud juurdepääsu lubamise või astub samme juurdepääsu tühistamiseks, teavitatakse teist poolt ja põhjendatakse sellist tegevust.

(7) Iga lepingupartneri pädev asutus / julgeolekuasutus võib nõuda, et teine kontrolliks ükskõik millise asutuse juurdepääsuloa, tagades, et taotlusele on lisatud sellise kontrolli nõude põhjendus. Sellise nõudmise täitmisel teavitatakse nõude esitanud ametiasutust kontrolli tulemustest ja otsustamise aluseks olnud faktidest.

(8) Kui teine pool nõuab, siis peab iga pädev asutus / julgeolekuasutus tegema üksikisiku juurdepääsuloa ja asutuse juurdepääsuloa ülevaatamise ja kontrolli alal koostööd.

Artikkel 10. Julgeolekumeetmete rakendamine

Julgeolekumeetmete rakendamist on võimalik edendada poolte julgeolekuesindajate vastastikuste visiitide kaudu. Vastavalt lubatakse poolte julgeoleku esindajatel pärast eelnevaid konsultatsioone külastada teist poolt, et arutada teise poole julgeolekusüsteemi.

Artikkel 11. Julgeolekumeetmete rikkumine või teabeleke

(1) Kui julgeolekumeetmete rikkumisega kaasnes salastatud materjali kaotsiminek või kahtlus, et salastatud teave on saanud teatavaks volitamata isikutele, peab teavet vastuvõtva poole pädev asutus / julgeolekuasutus teavet edastava poole pädevat asutust / julgeolekuasutust kirjalikult informeerima.

(2) Teavet vastuvõttev pool (kui nõutakse, siis teavet edastava poole abil) viib läbi viivitamatu uurimise vastavalt tema salastatud teabe kaitseks kehtivatele õigusaktidele ja juhenditele. Teavet vastuvõttev pool peab teavitama teavet edastavat poolt asjaoludest, tarvidusele võetud meetmetest ja uurimistulemusest, niipea kui võimalik.

Artikkel 12. Kulud

Kõik ühe poole poolt käesoleva lepingu nõuete täitmisel tehtud kulud katab seesama pool.

Artikkel 13. Muutmine

Kokkulepet võidakse poolte kirjalikul nõusolekul muuta või lisaga täiendada.

Artikkel 14. Erimeelsused

Kokkuleppe tõlgendamisest või rakendamisest tulenevad mistahes erimeelsused lahendatakse poolte vaheliste konsultatsioonide teel ja neid ei anta ühelegi riigisisesele või rahvusvahelisele kohtule või kolmandale poolele lahendamiseks.

Artikkel 15. Lõpetamine / ülevaatamine

(1) Kokkuleppe on jõus, kuni üks pool selle lõpetab, teavitades teist poolt kuus (6) kuud kirjalikult ette. Mõlemad pooled jäävad vastutavaks kogu käesoleva kokkuleppe sätete kohaselt vahetatud salastatud teabe kaitse eest peale lepingu lõpetamist.

(2) Sarnaselt kaitstakse kogu käesoleva kokkuleppe kohaselt vahetatud salastatud teavet, isegi kui selle edastamine leidis aset pärast ükskõik kumma poole poolt edastatud lõpetamise teatist.

(3) Lõpetamise korral otsitakse kõigile lahendamata probleemidele lahendeid poolte vaheliste konsultatsioonide kaudu.

(4) Pooled vaatavad kokkuleppe üle kümne (10) aasta jooksul pärast kehtima hakkamist või kui lepitakse kokku selle vajalikkuses.

Artikkel 16. Jõustumise kuupäev

Kokkulepe jõustub selle allakirjutamisel mõlema poole poolt.

Artikkel 17. Allkirjastamine

(1) Eelkirjutatu väljendab Eesti Vabariigi ja Rootsi Kuningriigi vahelisi kohustusi ülalpool viidatud küsimustes.

(2) Käesolev kokkulepe on koostatud kahes eksemplaris, eesti, rootsi ja inglise keeles, kusjuures kõik tekstid on võrdse jõuga. Käesoleva kokkuleppe erineva tõlgendamise korral võetakse aluseks inglisekeelne tekst.

Eesti Vabariigi nimel	**Rootsi Kuningriigi nimel**
Sven MIKSER	**Björn von SYDOW**

GENERAL SECURITY AGREEMENT BETWEEN THE REPUBLIC OF ESTONIA AND THE KINGDOM OF SWEDEN

List of Contents

Introduction

The Republic of Estonia and the Kingdom of Sweden, also referred to as the Parties, have in the interest of national security, established the following General Security Agreement, wishing to ensure the protection of Classified Information transferred between the two countries for the purposes of defense research, production and procurement or to commercial and industrial organisations in both countries, through approved channels.

This Agreement is to be interpreted in accordance with national law.

Article 1. Definitions

The following terms are defined in the interests of clarity:

“Classified Information” means any classified item, be it an oral or visual communication of classified contents or the electrical or electronic transmission of a classified message, or be it material which must for the interest of national security be exempted from disclosure and must enjoy protection against compromise.

“Material” includes any item of machinery or equipment or weapons either manufactured or in the process of manufacture or document.

“Document” means any recording medium containing Classified Information, including but not limited to any letter, note, minute, report, memorandum, signal/message, sketch, photograph, film, map, chart, notebook, stencil, carbon, typewriter ribbon, diskette, etc or other form of recorded information (e.g. tape recording, magnetic recording, punched card, tape, etc).

“Contractor” means an individual or legal entity possessing the legal capacity to undertake contracts.

“Contract” means an agreement between two or more parties creating and defining enforceable rights and obligations between the Parties.

“Classified Contract” means a contract which contains or involves Classified Information.

“National Security Authority (NSA) / Designated Security Authority (DSA)” means the Government Authority responsible for Defense Security in each country.

“Originating Party” means the Party initiating the Classified Information as represented by the NSA/DSA.

“Recipient Party” means the Party to which the Classified Information is transmitted or transferred as represented by the NSA/DSA.

“Security Classifications” and their equivalents in the two countries are:

In Estonia	**In Sweden**
TÄIESTI SALAJANE	KVALIFICERAT HEMLIG
SALAJANE	HEMLIG
KONFIDENTSIAALNE	HEMLIG

Swedish classified information to be transmitted or transferred to the Republic of Estonia will, where possible, be marked both with the Swedish security classification and the corresponding Estonian classification.

On occasion either Party may ask the other to afford protection at a higher level but not at a lower level than the classification indicated.

Article 2. Competent Security Authorities

The Government Authorities responsible for Defense Security in each country are the following:

for Sweden

The NSA in Sweden responsible for Defense Security issues is:
Försvarsmakten (The Swedish Armed Forces), Headquarters, Military Intelligence and Security (MUST), SE-107 86 Stockholm, Sweden; Phone no: +46 8 788 7500; Fax no: +46 8 788 8263.

The DSA in Sweden responsible for Defense Security associated with defense materiel is:
Försvarets Materielverk (The Swedish Defense Material Administration), Security, SE-115 88 Stockholm, Sweden; Phone no: +46 8 782 4000; Fax no: +46 8 660 2251;

for Estonia

The NSA in Estonia responsible for Defense Security associated with Defense Security issues is:
Security Department, Ministry of Defense, Sakala 1, 15094 Tallinn, Estonia; Phone No +372 6406 030; Fax No +372 6406 002.

Article 3. Restrictions on Use and Disclosure

(1) Without prior consultation, recipients will not disclose or use, or permit the disclosure or use of, any Classified Information except for purposes and within the limitations stated by or on behalf of the Originating Party.

(2) The Recipient Party will not pass or disclose to a Government official, Contractor, Contractors employee or to any other person holding the nationality of any third country, or to any international organisation, any Classified Information, exchanged under the provisions of this Agreement, nor will it publicly disclose any Classified Information without the prior consultation of the Originating Party.

(3) Nothing in this Agreement will be taken as an authority for, or govern the release, use, exchange or disclosure of intellectual property rights until the specific written authorisation of the owner of these rights has first been obtained, whether the owner is one of the Parties or a third party.

Article 4. Protection of Classified Information

(1) The Originating Party will ensure that the Recipient Party is informed of:
(a) the classification of the information and of any additional conditions of release or limitations on its use, and that documents are so marked; and
(b) any subsequent change in classification.

(2) The Recipient Party will:
(a) in accordance with its national laws and regulations, afford the equivalent level of security protection to Classified Information as is afforded by the Originating Party. The Receiving Party will take all steps legally available to it to keep transmitted and transferred Classified Information free from disclosure under any legislative provision; and each Party will maintain accountability and control procedures to manage the dissemination of, and access to, Classified Information.
(b) ensure that Classified Information is marked in accordance with Article 1; and
(c) ensure that the classification is not altered, except as authorised in writing by or on behalf of the Originating Party.

(3) In order to achieve and maintain comparable standards of security, each NSA/DSA will, on request, provide to the other information about its security standards, procedures and practices for safeguarding Classified Information, and will for this purpose facilitate visits by the Competent Security Authorities.

Article 5. Access to Classified Information

Access to Classified Information will be limited to those persons who have a “need to know” and who have been security cleared by the recipient NSA/DSA, in accordance with their national standards, to the level appropriate to the classification of the information to be accessed.

Article 6. Transmission of Classified Information

(1) Classified Information will be transmitted between the two countries in accordance with the national security regulations of the Originating Party. One route will be through official diplomatic Government to Government channels, but other Arrangements may be established, such as hand carriage, secure communications (encryption), if mutually acceptable to both Parties. The Party receiving Classified Information shall acknowledge its receipt in writing.

(2) Additionally, Classified Information may be transmitted or transferred between a Swedish company and a Estonian owned company in the Kingdom of Sweden or a Estonian company and a Swedish owned company in the Republic of Estonia using the national transmission or transfer regulations applicable in the country in which the companies are based. Releases may only take place between companies which hold the relevant facility and personnel security clearances (See article 9 (1)) and where the information has been approved for release to the other country.

Article 7. Visits

(1) The prior approval of the NSA/DSA of the host country will be required in respect of visitors, including those on detached duty from the other country, where access to Classified Information or to defense establishments / defense contractor premises engaged in classified work is necessary. Requests for such visits will be submitted through the respective Embassies.

(2) Requests will include the following information:
(a) surname and first name of proposed visitor, date and place of birth, nationality and passport number;
(b) official status of the visitor together with the name of the establishment, company or organisation which the visitor represents or to which the visitor belongs;
(c) certificate indicating the level of security clearance of the visitor;
(d) name and address of the establishment, company or organisation to be visited;
(e) name and status of the person(s) to be visited, if known;
(f) purpose of the visit; and
(g) date and duration of the visit. In cases of recurring visits the total period covered by the visits should be stated.

(3) All visitors will comply with the security regulations of the host country.

(4) Visit requests should be submitted to the Recipient Party in accordance with the normal procedures of the Recipient Party. Short notice visits can be arranged in urgent cases by special, mutually determined, arrangements.

(5) In cases involving a specific project or a particular contract it may, subject to the approval of both Parties, be possible to establish recurring visitors lists. These lists will be valid for an initial period not exceeding twelve (12) months and may be extended for a further period of time (not to exceed twelve (12) months) subject to the prior approval of the Competent Security Authority. They should be submitted in accordance with the normal procedures of the Recipient Party. Once a list has been approved, visit arrangements may be made direct between the establishments or companies involved in respect of listed individuals.

(6) Classified Information which may be provided to visiting personnel, or which may come to the notice of visiting personnel, will be treated by them as if such information had been furnished pursuant to the provisions of this Agreement.

Article 8. Contracts

(1) When proposing to place, or authorising a contractor in its country to place a Contract involving Classified Information with a Contractor in the other country the Originating Party will obtain prior clearance from the NSA/DSA of the other country that the proposed Contractor is security cleared to the appropriate level and also has appropriate security measures to provide adequate protection for Classified Information. The security clearance will carry a responsibility that the security conduct by the cleared Contractor will be in accordance with national security rules and regulations and monitored by his NSA/DSA.

(2) The Competent Security Authority will ensure that Contractors that receive Contracts placed as a consequence of these pre-contract enquiries are aware of the following provisions:
(a) the definition of the term Classified Information and of the equivalent levels of security classification of the two Parties in accordance with the provisions of this Agreement;
(b) the names of the Government Authority of each of the two countries 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 or transfer of the Classified Information between the Government Authorities and/or Contractors involved;
(d) the procedures and mechanisms for communicating the changes that may arise in respect of Classified Information either because of changes in its Security Classification or because protection is no longer necessary;
(e) the procedures for approval of visits, access or inspection by personnel of one country to companies of the other country are covered by the Contract;
(f) an obligation that the Contractor will disclose the Classified Information only to a person who has previously been cleared for access and who has a “need to know”, and is employed on or engaged in, the carrying out of the Contract;

(g) an obligation that the Contractor will not disclose the Classified Information or permit it to be disclosed to any person not expressly cleared in writing by the Contractor's NSA/DSA to have such access; and
(h) an obligation that the Contractor will immediately notify the Contractor's NSA/DSA or any actual or suspected breach or compromise of the Classified Information of this Contract.

(3) The Competent Security Authority of the Originating Party will pass two copies of the relevant parts of the Classified Contract to the Competent Security Authority of the Recipient Party, to allow adequate security monitoring.

(4) Each contract will contain guidance on the security requirements and on the classification of each aspect / elements of the Contract. In Sweden this guidance will be set out in separate security agreements. The guidance must identify each classified aspect of the Contract, or any classified aspect which is to be generated by the contract, and allocate to it a specific security classification. Changes in the requirements or to the aspects/ elements will be notified as and when necessary and the Originating Party will notify the Recipient Party when all the information has been declassified.

Article 9. Reciprocal Industrial Security Arrangements

(1) Each NSA/DSA will notify the security status of a company's premises in its country when requested by the other Party. Each NSA/DSA will also notify the security clearance status of one of its nationals when so requested. These notifications will be known as Facility security clearance (FSC) and Personnel security clearance (PSC) respectively.

(2) When requested the NSA/DSA will establish the security clearance status of the company/individual which is the subject of the inquiry and forward a security clearance if the company/individual is already cleared. If the company/individual does not have a security clearance, or the security clearance is at a lower security level than that which has been requested, notification will be sent that the security clearance cannot be issued immediately but that action is being taken to process the request. Following successful enquires a security clearance will be provided which will then permit a reciprocal security clearance to be issued.

(3) A company which is deemed by the NSA/DSA, in the country in which it is registered, to be under the ownership, control or influence of a third country whose aims are not compatible with those of the host Government is not eligible for a security clearance and the requesting NSA/DSA will be notified.

(4) If either NSA/DSA learns of any derogatory information about an individual for whom a PSC has been issued, it will notify the other NSA/DSA of the nature of the information and the action it intends to take, or has taken. Either NSA/DSA may request a review of any PSC which has been furnished earlier by the other NSA/ DSA, provided that the request is accompanied by a reason. The requesting NSA/DSA will be notified of the results of the review and any subsequent action.

(5) If information becomes available which raises doubts about the suitability of a reciprocally cleared company to continue to have access to Classified Information in the other country then details of this information will be promptly given to the NSA/DSA to allow an investigation to be carried out.

(6) If either NSA/DSA suspends or takes action to revoke access which is granted to a national of the other country based upon a security clearance, the other Party will be notified and given the reasons for such an action.

(7) Each NSA/DSA may request the other to review any FSC, provided that their request is accompanied by the reasons for seeking such a review. Following this review, the requesting authority will be notified of the results and will be provided with facts supporting any decisions taken.

(8) If required by the other Party each NSA/DSA will cooperate in reviews and investigations concerning FSC and PSC.

Article 10. Implementation of Security Requirements

Implementation of security requirements can be advanced through reciprocal visits by security representatives of the Parties. Accordingly, security representatives of the Parties, after prior consultation, will be permitted to visit the other Party, to discuss the security system of the other Party.

Article 11. Breach or Compromise

(1) In the event of a security breach involving loss of Classified Material or suspicion that Classified Information has been disclosed to unauthorised persons, the NSA/DSA of the Recipient Party will immediately inform the NSA/DSA of the Originating Party in writing.

(2) An immediate investigation will be carried out by the Recipient Party (with assistance from the Originating Party if required) in accordance with the laws and regulations in force in that country for the protection of Classified Information. The Recipient Party will inform the Originating Party about the circumstances, measures adopted and outcome of the investigations as soon as possible.

Article 12. Costs

All costs incurred by one Party in the application of the obligations in this Agreement shall be borne by that Party.

Article 13. Amendments

This Agreement may be amended or supplemented in an annex after written consent by the Parties.

Article 14. Disputes

Any dispute regarding the interpretation or application of this Agreement will be resolved by consultation between the Parties and will not be referred to any national or international tribunal or third party for settlement.

Article 15. Termination / Review

(1) This Agreement will remain in force until terminated by either Party giving the other Party six (6) months written notice of termination. Both Parties will remain responsible after termination for the safeguarding of all Classified Information exchanged under the provisions of this Agreement.

(2) Similarly, all Classified Information which is exchanged under this Agreement will be safeguarded, even though its transfer may occur after notice by either of the Parties to terminate.

(3) In the event of termination, solutions to any outstanding problems will be sought by consultations between the Parties.

(4) This Agreement will be reviewed by the Parties within ten (10) years after its effective date or as agreed when necessary.

Article 16. Effective Date

This Agreement will enter into force upon signature of both Parties.

Article 17. Signatures

(1) The foregoing represents the undertakings between the Republic of Estonia and the Kingdom of Sweden upon matters referred to therein.

(2) This Agreement is signed in two originals in the Estonian, Swedish and English language, all three texts equally authentic. In case of different interpretation of this Agreement the English text will prevail.

Tallinn, 30.01.2002.

For the Republic of Estonia **Sven MIKSER**	**For the Kingdom of Sweden** **Björn von SYDOW**