

Ziemeļatlantijias Padome

# NATO NEKLASIFICĒTS

|  |  |
| --- | --- |
| 2013. gada 7. janvāris | AC/35-D/2000-REV7 |

**DROŠĪBAS JAUTĀJUMU KOMITEJAS**

**DIREKTĪVA PAR PERSONĀLA DROŠĪBU**

**Priekšsēdētāja paziņojums**

1. Pielikumā ir Direktīvas par personāla drošību septītais pārstrādātais izdevums, kas ir publicēts, lai nodrošinātu NATO Drošības politikas C-M(2002)49 īstenošanu. Tas savas būtības ir saistošs un obligāts NATO dalībvalstīm, pavēlniecībām un aģentūrām. Šis dokuments aizstāj AC/35-D/2000-REV6, kas ir jāiznīcina.
2. Šajā pārstrādātajā izdevumā ir atspoguļotas apstiprinātās izmaiņas attiecībā uz NATO *PSC* (*personnel security clearance* – personāla drošības pielaides) paraugiem, kas ietverti 1. un 2. papildinājumā.
3. Šo dokumentu Drošības jautājumu komiteja ir apstiprinājusi Drošības politikas formātā (sk. AC/35-DS(2012)0005-AS1 (SP) un AC/35-WP(2012)0004-REV1 (SP)), un tas tiks periodiski pārskatīts.

(Parakstījis) Stīvens F. Smits [*Stephen F. Smith*]

|  |  |
| --- | --- |
| Pielikums: 1 | Virsnieks-izpildītājs: Roberts Keils [*Robert Keil*], *NOS* (NATO *Office of Security* – NATO Drošības birojs) / *POB* (*post office box* – pasta kastīte), papildnumurs 4084Oriģināls: angļu valodā |



**NATO NEKLASIFICĒTS**

**DIREKTĪVA PAR PERSONĀLA DROŠĪBU**

**IEVADS**

1. Šo Personāla drošības direktīvu ir publicējusi Drošības jautājumu komiteja (AC/35), lai nodrošinātu NATO Drošības politikas (C-M(2002)49) "C" pielikuma īstenošanu. Šī direktīva ietver obligātos noteikumus, kā arī informāciju, kas izskaidro šo noteikumu nozīmi. Šajā direktīvā aplūkoti šādi aspekti:
	1. personāla drošības pielaides:
		1. pienākumi;
		2. prasības to amatu noteikšanai, kuriem nepieciešama attiecīga personāla drošības pielaide (*PSC*);
		3. kritēriji tiesību saņemt *PSC* izvērtēšanai;
		4. pārbaudes prasības drošības pielaidēm NATO KONFIDENCIĀLAJAI, NATO SLEPENAJAI un SEVIŠĶI SLEPENAJAI klasificētajai informācijai;
		5. prasības attiecībā uz *PSC* piešķiršanu NATO civilo un militāro institūciju darbiniekiem;
		6. prasības attiecībā uz *PSC* atkārtotu apstiprināšanu;
		7. procedūras rīcībai ar negatīvu informāciju par personu, kurai ir *PSC*; un
		8. prasības attiecībā uz personām piešķirto *PSC* uzskaiti;
	2. informētība drošības jautājumos un personu instruēšana;
	3. atļauju attiecībā uz piekļuvi NATO klasificētajai informācijai piešķiršana – pagaidu norīkošana, vienreizēja piekļuve, piekļuve ārkārtas gadījumos un piedalīšanās konferencēs un sanāksmēs;
	4. personāla drošības pielaides kurjeriem, apsargiem un pavadoņiem; un
	5. personu, kurām nav NATO dalībvalsts valstspiederības, piekļuve informācijai.

## PERSONĀLA DROŠĪBAS PIELAIDE (PSC)

1. Saskaņā ar NATO Drošības politikas prasībām ir jābūt saskaņotam uzticēšanās standartam attiecībā uz visu to personu lojalitāti, uzticību un uzticamību, kurām piešķirtas piekļuves tiesības NATO klasificētajai informācijai vai arī kurām saistībā ar to pienākumiem vai funkcijām ir nodrošināta piekļuve šādai informācijai. Lai to panāktu, personām, kurām ir atļauts piekļūt informācijai, kas klasificēta kā *NC* (NATO *CONFIDENTIAL* – NATO KONFIDENCIĀLĀ) vai kurai noteikta augstāka slepenības pakāpe, ir jābūt saņēmušām attiecīgu personāla drošības pielaidi (*PSC*), kas derīga uz sankcionētās piekļuves laiku, kā arī jābūt nepieciešamībai zināt šo informāciju. Proti:
	1. personām, ko tieši nolīgušas NATO civilās un militārās institūcijas, ir jābūt NATO personāla drošības pielaidei (*PSC*), ko piešķīrusi valsts drošības iestāde (*NSA*) (*National Security Authority* (*NSA*)) vai cita kompetenta attiecīgās personas valsts valdības iestāde;
	2. *NSA* vai citai kompetentai attiecīgās personas valsts valdības iestādei ir jāpiešķir NATO *PSC* arī personām, ko pieņēmusi darbā to valsts valdības militārā vai civilā institūcija un kuras tiek norīkotas amatā darbam NATO civilajā vai militārajā institūcijā;
	3. personām, ko pieņēmusi darbā dalībvalsts vai ko dalībvalsts iekļāvusi savas nacionālās delegācijas NATO *HQ* (*Headquarters* – Galvenajā mītnē) sastāvā, ir jābūt piešķirtai atbilstošai un derīgai nacionālajai un/vai NATO PSC; un
	4. valsts drošības iestādei (*NSA*) vai citai kompetentai iestādei personām, kas ir līgumdarbinieki, ir jāpiešķir NATO personāla drošības pielaide (*PSC*). Sīkāki norādījumi attiecībā uz līgumdarbiniekiem ir atrodami C-M(2002)49 "G" pielikumā un papildinošajā Direktīvā par industriālo drošību.

## Pienākumi

1. *NSA* vai citas kompetentās valsts iestādes ir atbildīgas par:
	1. drošības izmeklēšanas veikšanu attiecībā uz saviem valstspiederīgajiem/pilsoņiem[[1]](#footnote-1) un citām savā jurisdikcijā esošajām personām, kurām ir nepieciešams piekļūt informācijai, kas klasificēta kā *NC* vai kurai noteikta augstāka slepenības pakāpe, kā arī pasākumiem, lai noteiktu to, vai *PSC* ir jāpiešķir, jāatsaka vai jāatņem. Izmeklēšanas standartiem ir jāatbilst NATO dalībvalstu nacionālajai izmeklēšanas praksei, taču nekādā gadījumā šie standarti nedrīkst būt zemāki par tiem, kas noteikti 7.-10. punktā;
	2. to, lai tiktu nodrošināts, ka *PSC* procedūras tiek veiktas ar izmeklējamās personas ziņu un piekrišanu valsts tiesību aktos noteiktajā kārtībā;
	3. *PSC* atkārtotu apstiprināšanu; un
	4. sadarbību ar citām *NSA* vai citām kompetentajām valsts iestādēm, veicot atbilstošās *PSC* procedūras.
2. NATO dalībvalstis un NATO civilo vai militāro institūciju vadītāji ir atbildīgi par:
	1. to amatu noteikšanu, kuru ieņemšanai nepieciešama PSC;
	2. atļauju piešķiršanu NATO klasificētajai informācijai savās atbildības jomās, tostarp situācijās, kas aprakstītas no 28.-37. punktam;
	3. to, lai tiktu nodrošināts, ka ievēro šeit izklāstītos personāla drošības standartus; un
	4. savu darbinieku pastāvīgu piekļuves tiesību izvērtēšanu NATO klasificētajai informācijai.

## To amatu noteikšana, kuriem nepieciešama personāla drošības pielaide (*PSC*),

1. Lai varētu izvērtēt to, vai amata ieņemšanai ir nepieciešama *PSC*, NATO dalībvalstis un NATO civilās un militārās institūcijas piesaista administratorus, kas visplašāk pārzina sava personāla darbu un piekļuves NATO klasificētajai informācijai līmeņus, kādi nepieciešami attiecīgajam amatam. Parasti tieši viņi vislabāk varēs noteikt to, kāds drošības pielaides līmenis ir nepieciešams attiecīgajā amatā.
2. Administratori ir arī atbildīgi par to, lai tiktu nodrošināts, ka viņu darbinieki atbilst savu darba pienākumu pildīšanai nepieciešamajam *PSC* līmenim, lai varētu piekļūt informācijai, un ka tiek piemērots nepieciešamības zināt princips. Kad ir jāveic regulārā personas *PSC* atkārtotā apstiprināšana, vai kad darbinieks mainās, attiecīgais administrators ir atbildīgs par to, lai tiktu izvērtēts, vai šim amatam attiecīgais *PSC* līmenis joprojām ir nepieciešams.

## Kritēriji, lai izvērtētu tiesības saņemt personāla drošības pielaides

1. Turpmākajos punktos ietverti galvenie kritēriji, pēc kuriem tiek vērtēta personas lojalitāte, uzticība un uzticamība, lai tai varētu piešķirt vai arī atstāt *PSC*. Šajos punktos aplūkoti aspekti, kuri saistīti ar personīgajām īpašībām un apstākļiem, kas var būt iespējamo drošības risku rašanās iemesls.
2. Lai gan šie kritēriji attiecas uz personu, attiecībā uz kuru tiek veikta pielaides procedūra, attiecīgos gadījumos saskaņā ar valsts tiesību aktiem būtiskas var būt arī laulātā, faktiskā dzīvesbiedra vai tuva ģimenes locekļa personīgās īpašības un uzvedība, kā arī apstākļi, kas ar viņu saistīti, un šie faktori ir jāņem vērā, izskatot jautājumu par personas tiesībām saņemt pielaidi.
3. Šie kritēriji ir jāpiemēro, lai noteiktu, vai persona vai tās laulātais, faktiskais dzīvesbiedrs, kā arī – attiecīgos gadījumos un saskaņā ar valsts tiesību aktiem – tuvs ģimenes loceklis:
	1. ir veicis vai mēģinājis veikt jebkādu spiegošanas darbību, terora aktu, sabotāžas, nodevības vai musināšanas darbību, kā arī iesaistījies sazvērestībā ar citu personu vai tai palīdzējis un atbalstījis to šādās darbībās (vai to mēģinājumā);
	2. ir vai ir bijis spiegu, teroristu, kaitnieku vai personu, par kurām ir pamatotas aizdomas, ka tās ir iepriekš minētie indivīdi, sabiedrotais vai arī tādu organizāciju vai ārvalstu pārstāvju, tostarp ārvalstu izlūkdienestu, partneris, kuras var apdraudēt NATO un/vai NATO dalībvalstu drošību, ja vien šī saistība nav bijusi atļauta dienesta pienākumu pildīšanas gaitā;
	3. ir vai ir bijis jebkādas tādas organizācijas dalībnieks, kura ar vardarbīgiem, graujošiem vai citiem pretlikumīgiem līdzekļiem cenšas gāzt dalībvalstu valdību vai izmainīt dalībvalstu pārvaldīšanas formu;
	4. ir vai pēdējā laikā ir bijis jebkuras tādas organizācijas atbalstītājs, kas aprakstīta c) apakšpunktā, vai arī ir vai pēdējā laikā ir bijis cieši saistīts ar šādu organizāciju dalībniekiem;
	5. ir tīši slēpis, sagrozījis vai falsificējis nozīmīgu informāciju, jo īpaši – informāciju drošības jomā, vai arī ir tīši melojis, aizpildot personāla drošības veidlapu, vai arī to darījis drošības intervijas laikā.
	6. ir atzīts par vainīgu noziedzīgā nodarījumā vai pārkāpumos, kas liecina par pastāvīgām noziedzīgām nosliecēm (vai arī viņam ir nopietnas finanšu grūtības vai neizskaidrojama turība; vai arī ir bijusi atkarība no alkohola, nelegālajām narkotikām un/vai atkarība, kas saistīta ar legālo narkotiku (medikamentu) ļaunprātīgu lietošanu);
	7. ir vai ir bijis iesaistīts nodarījumos, tostarp seksuāla rakstura pārkāpumos, kas var radīt risku, kas saistīts ar ietekmējamību, saskaroties ar šantāžu vai spiedienu;
	8. darbībās vai vārdos ir bijis negodīgs, nelojāls, neuzticams, neuzticīgs vai neapdomīgs;
	9. ir nopietni vai atkārtoti pārkāpis drošības noteikumus; vai arī ir mēģinājis vai spējis veikt nesankcionētas darbības pret sakaru un informācijas sistēmu (-ām);
	10. cieš vai ir cietis no jebkādas slimības vai arī garīgā vai emocionālā stāvokļa, kas var radīt ievērojamus traucējumus, kas ietekmē viņa saprātu vai uzticamību, vai arī var netīšām padarīt šo personu par potenciālu drošības risku. Visos šādos gadījumos ir jālūdz kompetenta medicīniska konsultācija; vai arī
	11. var būt pakļauts spiedienam tādu radinieku vai tuvu kolēģu dēļ, kuri var būt neaizsargāti pret ārvalstu izlūkdienestiem, teroristiskiem grupējumiem vai citām organizācijām vai personām, kas veic graujošu darbību un kuru intereses var apdraudēt NATO un/vai NATO dalībvalstu drošības intereses.

## Bipatrīdi

1. Izskatot jautājumu par tiesībām saņemt drošības pielaidi attiecībā uz personām, kurām ir dubultpilsonība, no kurām viena var nebūt NATO dalībvalsts pilsonība, ir jābūt īpaši uzmanīgiem. Ar nosacījumu, ka izcelsmes valsts *NSA*[[2]](#footnote-2), kas piešķir pielaidi, pieņem, ka nepastāv faktisks vai potenciāls lojalitātes konflikts, nav *prima facie* iemesla pielaidi atteikt.

## PĀRBAUDES PRASĪBAS PIELAIDĒM NATO KONFIDENCIĀLAJAI, NATO SLEPENAJAI UN SEVIŠĶI SLEPENAJAI KLASIFICĒTAJAI INFORMĀCIJAI

1. Sākotnējo drošības pielaidi attiecībā uz piekļuvi informācijai, kas klasificēta kā *NC* un *NS* (*NATO SECRET* – NATO SLEPENĀ) informācija, piešķir, pamatojoties uz izziņas darbībām, kas aptver vismaz pēdējos 5 gadus vai periodu no 18 gadu vecuma līdz pašreizējam brīdim (īsākajā no šiem periodiem); šīs izziņas darbības ir šādas:
	1. personāla drošības anketas (kas var būt vai nu NATO, vai nacionālā anketa) aizpildīšana;
	2. identitātes noskaidrošana / pilsonības / valstspiederības statusa pārbaude – pārliecinās par personas dzimšanas datumu un vietu, kā arī pārbauda tās identitāti. Noskaidro personas pašreizējo un agrāko pilsonību un/vai valstspiederību; tas ietver ietekmējamības ārvalstu avotu spiediena gadījumā novērtēšanu; piemēram, tā var būt ietekmējamība agrākās dzīvesvietas vai pagātnes saišu dēļ; un
	3. nacionālo un vietējo reģistru pārbaude – pārbauda valsts drošības un centrālos sodāmības reģistrus, ja pēdējie no iepriekš minētajiem eksistē, un/vai citus pielīdzināmos valdības un policijas reģistrus attiecībā uz oficiāli reģistrētām indikācijām par nelojalitāti vai neuzticamību. Pārbauda tiesībaizsardzības iestāžu reģistru, kuru jurisdikcijā vismaz sešus mēnešus bijusi personas dzīvesvieta vai darbavieta, informāciju.
2. Sākotnējo drošības pielaidi attiecībā uz piekļuvi informācijai, kas klasificēta kā *CTS* (*COSMIC TOP SECRET* – SEVIŠĶI SLEPENA) informācija, piešķir, pamatojoties uz izziņas darbībām, kas aptver vismaz pēdējos 10 gadus vai periodu no 18 gadu vecuma līdz pašreizējam brīdim (īsākajā no šiem periodiem). Ja intervijas tiek veiktas tā, kā tas norādīts e), i) un ii) apakšpunktā, izziņas darbības aptver vismaz 7 gadu periodu vai laiku no 18 gadu vecuma līdz pašreizējam brīdim (ņemot vērā īsāko no šiem periodiem). Lai varētu izvērtēt pielaides informācijai, kas klasificēta kā *CTS*, papildus prasībām, kas izklāstītas 11. punktā, nepieciešamas ir turpmāk norādītās ziņas; šie faktori var būt būtiski, izvērtējot arī *NC* un *NS* pielaides, ja tas atbilst valstu noteikumiem un tiesību aktiem:
	1. finanšu stāvoklis: pieprasa informāciju par personas finansēm, lai novērtētu ietekmējamību nopietnu finanšu grūtību dēļ ārvalstu vai vietējā spiediena gadījumā vai atklātu informāciju par neizskaidrojamu turību;
	2. izglītība: pieprasa informāciju par mācībām skolās, universitātēs un citās izglītības iestādēs kopš 18. dzimšanas dienas vai arī atbilstošā periodā saskaņā ar drošības iestādes, kas veic izmeklēšanu, vērtējumu;
	3. nodarbošanās: pieprasa informāciju par pašreizējo un agrāko nodarbošanos; informāciju sniedz, atsaucoties uz tādiem avotiem kā dati par nodarbošanos, pārskati par veikumu vai dienesta raksturojumi, kā arī darba devēji vai vadītāji;
	4. militārais dienests: attiecīgos gadījumos tiks pārbaudītas ziņas par personas dienestu bruņotajos spēkos un atvaļināšanās veids; un
	5. intervijas: ja to paredz un pieļauj nacionālie tiesību akti:
		1. veic arī interviju (-jas) ar personu – it īpaši, ja, veicot sākotnējās izziņas darbības, ir atklājusies potenciāli negatīva informācija; un
		2. veic arī intervijas ar personām, kurām ir iespējas sniegt objektīvu novērtējumu par personas sagatavotību, darbībām, lojalitāti, uzticīgumu un uzticamību. Gadījumos, kad saskaņā ar nacionālo praksi cilvēkam, attiecībā pret tiek veikta izmeklēšana, tiek lūgts sniegt papildu ziņas, tiek intervēti neatkarīgi eksperti, ja vien nav pamatota iemesla to nedarīt. Pietiekamā apjomā tiek veiktas papildu izziņas darbības, lai iegūtu visu pieejamo būtisko informāciju par personu un lai pamatotu vai atspēkotu negatīvo informāciju.
3. Ja kādā izmeklēšanas kategorijā informācija ir nepietiekama, to kompensē ar citiem izmeklēšanas līdzekļiem saskaņā ar tiesību aktiem nacionālās drošības jomā.

## Personāla drošības pielaides piešķiršana

1. *NSA* vai kompetentā valsts iestāde izskata visu pieejamo informāciju, lai varētu noteikt, vai *PSC* ir vai nav jāpiešķir. Jāpiezīmē, ka indikācijām par ietekmējamību iespējama spiediena gadījumā (piem., parādiem vai iespējamai laulātā / faktiskā dzīvesbiedra / tuva ģimenes locekļa iespējamo ietekmējamību) nevajadzētu būt pielaides atteikšanas iemeslam, ja cilvēka lojalitāte, uzticība un uzticamība ir neapstrīdama. Lai noteiktu, vai pielaidi drīkst piešķirt, *NSA* vai kompetentā valsts iestāde novērtē riskus, kas saistīti ar katru gadījumu.

## NATO civilo un militāro institūciju darbinieku drošības pielaides apliecība

1. Kad *NSA* vai cita kompetentā valsts iestāde ir piešķīrusi *PSC* personai, kuru paredzēts pieņemt vai norīkot darbā NATO civilajā vai militārajā institūcijā, vai arī personai, kuru dalībvalsts iekļāvusi savas nacionālās delegācijas NATO *HQ* sastāvā, tās tieši vai pēc īpaša attiecīgās NATO institūcijas pieprasījuma iesniedz *PSC* apliecības kopiju NATO civilajai vai militārajai institūcijai, kurā šī persona ieņems amatu. Šīs apliecības paraugs ietverts 1. papildinājumā. Visos gadījumos uz personāla drošības pielaides apliecības norāda drošības pielaides piešķiršanas datumu, kā arī datumu, kad pielaide stājas spēkā.
2. Ja personas darba periods nesākas 12 mēnešu laikā no jaunas *PSC* piešķiršanas brīža, aizpildot amata vietu NATO civilajā vai militārajā institūcijā, vai arī personai ir 12 mēnešus ilgs darba pārtraukums, kura laikā tā netiek nodarbināta amatā NATO vai NATO dalībvalsts valdības civilajā vai militārajā institūcijā, attiecībā uz *PSC* ir jāgriežas personas vadošajā *NSA*, lai saņemtu apstiprinājumu par to, ka pielaide joprojām ir spēkā un ir nepieciešama.

## Drošības pielaides līgumdarbiniekiem, kas veic darbus NATO civilajās vai militārajās institūcijās

1. Noteikumi par personāla drošības pielaidēm vai par to apstiprināšanu līgumdarbiniekiem, kas veic darbus NATO telpās un kuriem ir nepieciešama personāla drošības pielaide, ir ietverti Direktīvā par industriālo drošību.

## Personāla drošības pielaides atkārtota apstiprināšana

1. Pēc *PSC* pirmreizējās piešķiršanas un ar nosacījumu, ka persona ir bez pārtraukumiem strādājusi NATO dalībvalsts vai NATO civilajā vai militārajā institūcijā un ka tai pastāvīgi ir nepieciešams piekļūt NATO klasificētajai informācijai, PSC tiek no jauna izskatīta, lai to varētu atkārtoti apstiprināt, ar intervāliem, kas nav ilgāki par 5 gadiem, *CTS* pielaidei, un intervāliem, kas nepārsniedz 10 gadus, *NS* un *NC* pielaidēm, stājoties spēkā no dienas, kad veikta pēdējā izmeklēšanas darbība, pamatojoties uz kuru tā ir piešķirta. Visas izmeklēšanas darbības, kas saistītas ar *PSC* pagarināšanu, attiecas uz periodu kopš iepriekšējām izmeklēšanas darbībām. PSC atkārtotas apstiprināšanas pieprasījumus iesniedz savlaicīgi saskaņā ar *NSA* prasībām.
2. *NC* un *NS* *PSC* atkārtotai apstiprināšanai veic vismaz turpmāk aprakstītās procedūras:
	1. attiecīgā persona aizpilda personāla drošības anketu (tā var būt NATO papildu personas datu veidlapa vai līdzīga valstu veidlapa, kuru nodrošina kompetentā valsts iestāde);
	2. attiecībā uz personām, ko nodarbina NATO civilā vai militārā institūcija, pārbauda personāla drošības anketas atbilstību NATO institūcijas drošības dokumentācijai un personālajām lietām;
	3. kad veikt atkārtotu apstiprināšanu attiecībā uz personām, ko nodarbina NATO institūcija, lūdz NATO civilā vai militārā institūcija, aizpildītu personāla drošības anketu, kas minēta a) apakšpunktā, un b) apakšpunktā noteiktās pārbaudes rezultātus nosūta personas vadošajai un uzņēmējvalsts *NSA*;
	4. valsts, kurā atrodas NATO institūcija, (t. i., uzņēmējvalsts) pēc personas vadošās *NSA* pieprasījuma no jauna izskata savu nacionālo dokumentāciju;
	5. jebkura cita NATO dalībvalsts, kurā uzturējies darbinieks, attiecīgos gadījumos veic (d) apakšpunktā norādītajai identisku otrreizēju izskatīšanu, ja to lūdz vadošā *NSA*; un
	6. kad kompetentā NATO civilā vai militārā institūcija lūdz personas vadošo *NSA* atkārtoti apstiprināt drošības pielaidi, tā arī nodod sīku personas drošības dokumentācijas informāciju, kas attiecas uz viņa/viņas darba laiku izvērtējuma periodā.
3. Tad vadošā *NSA* salīdzina visu informāciju, kas iegūta šīs dokumentācijas pārbaužu laikā, ar savā dokumentācijā ietverto informāciju un nosūta savu lēmumu NATO civilajai vai militārajai institūcijai, kas izteikusi lūgumu.
4. Veicot pielaides apstiprināšanu *CTS* līmenī, papildus parastajām otrreizējas izskatīšanas procedūrām, kas aprakstītas 19. punktā, var veikt arī interviju ar personu, un šajā gadījumā ir jāveic turpmāk norādītās darbības, kas attiecas uz 5 gadiem kopš iepriekšējām izmeklēšanas darbībām / pārbaudes:
	1. ja dalībvalstīm, kas ir nodrošinājušas savu personāla drošības anketu, ir nepieciešami personības raksturojumi, tos izskata, konsultējoties ar uzņēmējvalsts *NSA*;
	2. gadījumā, ja ir nepieciešama padziļināta izmeklēšana, jāveic intervijas vismaz ar divām personām, kurām ir iespējas sniegt objektīvu novērtējumu par personas sagatavotību, darbībām, lojalitāti, uzticīgumu un uzticamību;
	3. ja personas, kas strādā ārzemēs, *PSC* ir atkārtoti jāapstiprina vairāk nekā vienreiz nepārtrauktas ekspatriācijas laikā, jāizskata iespēja veikt padziļinātu izmeklēšanu, kas minēta b) apakšpunktā;
	4. ja nepieciešams, uzņēmējvalsts *NSA* izcelsmes valsts vārdā veic papildu izziņas darbības, kas izriet no informācijas, kas var atklāties jebkuras 19. punktā un 21. punkta a) līdz c) apakšpunktā (ieskaitot) minētās darbības rezultātā;
	5. uzņēmējvalsts un jebkuras citas dalībvalsts, kurā cilvēks ir uzturējies, *NSA* nosūta visu informāciju, kas iegūta saskaņā ar 19. punkta un 21. punkta a) līdz d) apakšpunkta (ieskaitot) noteikumiem, izcelsmes valsts *NSA*;
	6. vadošā *NSA* visu informāciju, kas tai nosūtīta saskaņā ar e) apakšpunkta noteikumiem, salīdzina ar savā dokumentācijā ietverto informāciju;
	7. vadošās *NSA* lēmumu attiecībā uz personāla drošības pielaides apliecības darbības termiņa pagarināšanu nosūta NATO civilajai vai militārajai institūcijai, kas iesniegusi pieprasījumu.
5. Ja NATO personāla drošības pielaide netiek atkārtoti apstiprināta pielaides darbības termiņā, atkārtotās apstiprināšanas pabeigšanai pieļaujams ir papildus atvēlēt 12 mēnešus ar noteikumu, ka *NSA* ir uzsākusi darbības, kas jāveic, lai atkārtoti apstiprinātu pielaidi. Ja šī 12 mēnešu papildu perioda beigās atkārtotas apstiprināšanas process joprojām nav pabeigts, persona tiek pārcelta amatā, kurā personāla drošības pielaide nav nepieciešama. Ja izņēmuma kārtā izziņas darbības nevar pabeigt šajā laika periodā un nav iegūta nekāda negatīva informācija, attiecīgā *NSA*/*DSA* var nodrošināt kompetentajai NATO civilajai vai militārajai institūcijai esošās drošības pielaides derīguma termiņa pagarināšanu, norādot datumu, kad ir sagaidāms galīgais lēmums par atkārtoto apstiprināšanu.

## Negatīva informācija

1. Nosaka procedūras, lai nodrošinātu, ka gadījumos, kad kļūst zināma negatīva informācija, kas attiecas uz personu, tās vadošā *NSA* pieņem lēmumu par to, vai tai saglabājama *PSC*. Gadījumos, kad tiek uzskatīts, ka personas rada nepieļaujamu drošības risku, *PSC* tām tiek atņemta un personām tiek liegta piekļuve NATO klasificētajai informācijai, un tās tiek atstādinātas no amatiem, kuros tās var apdraudēt drošību. Kad *PSC* tiek atņemta personai, kura norīkota darbā NATO civilajā vai militārajā institūcijā vai kuru šī institūcija ir tieši nolīgusi, vadošā *NSA* izdod NATO institūcijai apliecību, ar kuru *PSC* tiek atcelta.

## Personāla drošības pielaižu dokumentācija

1. NATO dalībvalstis un NATO civilā vai militārā institūcija - darba devējs glabā dokumentāciju par *PSC*, kas piešķirtas personām, kurām ir piekļuve NATO klasificētajai informācijai. Šī dokumentācija satur sīku informāciju par pielaides līmeni, piešķiršanas datumu un spēkā esamību.

## INFORMĒTĪBA DROŠĪBAS JAUTĀJUMOS UN PERSONU INSTRUĒŠANA

1. Visas personas, kas tiek nodarbinātas amatos, kur tām ir piekļuve *NR* (NATO *restricted* – NATO ierobežotas pieejamības) informācijai, vai kurām ir pielaide piekļuvei *NC* vai augstākas slepenības pakāpes informācijai, tiek instruētas par drošības procedūrām un to pienākumiem drošības jomā. Visas personas, kurām ir pielaide, apliecina, ka tās pilnībā izprot savus pienākumus un sekas, kas paredzētas saskaņā ar to valsts likumiem vai administratīvajiem vai izpildu rīkojumiem gadījumos, kad klasificēta informācija tīši vai nolaidības dēļ nonāk nepiederošu personu rokās. Apliecinājuma dokumentu glabā NATO dalībvalsts vai NATO civilā vai militārā institūcija, kas sankcionē piekļuvi NATO klasificētajai informācijai.
2. Visas personas, kurām atļauta piekļuve NATO klasificētajai informācijai vai kam ir jāstrādā ar šādu informāciju, sākumā tiek informētas (un tām tiek periodiski atgādināts) par drošības apdraudējumiem, kas rodas, neapdomīgi sarunājoties ar personām, kurām nav jāzina šī informācija; tāpat tās tiek informētas (un tām tiek atgādināts) par attiecībām ar plašsaziņas līdzekļiem un draudiem, ko rada izlūkdienestu darbības, kas vērstas pret NATO un tās dalībvalstīm. Personas tiek detalizēti instruētas par šiem draudiem, un tām ir nekavējoties jāziņo attiecīgajām drošības iestādēm par jebkādu tuvošanos vai viltīgu izturēšanos, ko tās uzskata par aizdomīgu vai neparastu.
3. Visas personas, kas pārtrauc strādāt amatā, kur nepieciešama pielaide NATO klasificētajai informācijai, tiek informētas par pienākumiem, kas saistīti ar turpmāku NATO klasificētās informācijas aizsargāšanu (un tās apliecina šos pienākumus).

## PIEKĻUVES NATO KLASIFICĒTAJAI INFORMĀCIJAI SANKCIONĒŠANA

1. Personai tiek atļauta piekļuve NATO klasificētajai informācijai tikai tad, kad tai ir piešķirta atbilstoša personāla drošības pielaide, ir ticis pieņemts lēmums par to, kādu informāciju tai ir nepieciešams zināt, un tā ir tikusi instruēta par NATO drošības procedūrām, kā arī ir sniegusi apliecinājumu par saviem pienākumiem drošības jomā.

## Izņēmuma apstākļi

## Iecelšana amatā uz laiku

1. Kad personu ir paredzēts iecelt amatā, kur nepieciešama *PSC*, kuras līmenis ir augstāks par to, kuram atbilst tās pašreizējais ieņemamais amats, amatā var iecelt pagaidu kārtā ar nosacījumu, ka:
	1. personai ir pašreiz spēkā esoša *PSC*;
	2. ir uzsāktas darbības tāda līmeņa *PSC* iegūšanai, kas nepieciešams šim amatam;
	3. personas iekārtošanu darbā ir apstiprinājusi atbildīgā *NSA* vai cita kompetentā iestāde; un
	4. ir veiktas pietiekamas pārbaudes, konstatējot, ka persona nav nopietni vai atkārtoti pārkāpusi drošības noteikumus.
2. Ieceļot amatā uz laiku, šis periods nav ilgāks par sešiem mēnešiem no dienas, kad persona stājas amatā. *NSA* var pagarināt laiku, uz kuru persona iecelta amatā, par vēl sešiem mēnešiem, ja ir uzsākta izmeklēšana un nav negatīvas informācijas.

## Vienreizēja piekļuve

1. Izņēmuma kārtā personām var tikt atļauts vienreiz piekļūt NATO informācijai, kas klasificēta kā tādam līmenim atbilstoša informācija, kas ir par vienu pakāpi augstāks nekā tas, kurā tām ir pielaide. Jāizpilda šādi kritēriji:
	1. personas vadītājam ir rakstiski jāpamato akūta vajadzība, kas saistīta ar uzdevumu, piekļūt informācijai;
	2. piekļuve tiek ierobežota, atļauju attiecinot tikai uz specifiskiem NATO klasificētās informācijas elementiem, lai varētu atbalstīt vadītāja aprakstītā uzdevuma izpildi;
	3. personai ir pašreiz spēkā esoša *PSC*;
	4. ir veiktas pietiekamas pārbaudes, konstatējot, ka persona nav nopietni vai atkārtoti pārkāpusi drošības noteikumus;
	5. atļauju var dod vienīgi *OF6* ("*one* *star* *general*" – brigādes ģenerālis) vai atbilstoša līmeņa civilā amatpersona pēc saskaņošanas ar attiecīgo drošības iestādi (-dēm); un
	6. dokumentu par izņēmuma piemērošanu, tostarp tās informācijas aprakstu, kurai tikusi apstiprināta piekļuve, glabā kompetentais drošības birojs.
2. Šī procedūra attiecībā uz piekļuvi NATO klasificētajai informācijai nav izmantojama vairākkārt. Ja tas ir nepieciešams vai ja piekļuve ir jānodrošina vairāk nekā 6 mēnešus, ir jāsaņem augstāka līmeņa personāla drošības pielaide.

## Piekļuve izņēmuma apstākļos

1. Personām izņēmuma kārtā var atļaut piekļūt NATO *HQ* un NATO civilo vai militāro institūciju telpām, kā arī NATO klasificētajai informācijai ar nosacījumu, ka tiek izpildīti šādi kritēriji:
	1. personas ir NATO dalībvalsts valstspiederīgie;
	2. piekļuvi sankcionē NATO *HQ* nodaļas priekšnieks vai NATO civilā vai militārā institūcija, pamatojoties uz argumentētu rakstveida pamatojumu;
	3. piekļuve tiek ierobežota, atļauju attiecinot vienīgi uz specifiskiem tādas NATO informācijas elementiem, kura klasificēta kā NATO SLEPENĀ (vai zemākas slepenības pakāpes) informācija, ar mērķi atbalstīt NATO *HQ* nodaļas priekšnieka vai NATO civilās vai militārās institūcijas aprakstīta uzdevuma izpildi;
	4. piekļuve tiek atļauta vienreiz vai uz ierobežotu laika periodu, kas nekad nav ilgāks par sešiem mēnešiem;
	5. piekļuve tiek ierobežota, to nodrošinot tikai administratīvajās zonās vai 2. kategorijas drošības zonās;
	6. piekļuve *CIS* (*Communication and Information Systems* – sakaru un informācijas sistēmām), kas apstrādā NATO klasificēto informāciju, nav atļauta, izņemot gadījumus, kad *CIS* ir paredzētas vienīgi tādu darbību atbalstam, kurās attiecīgā persona ir iesaistīta;
	7. atbildīgā vadošā *NSA* ir saskaņā ar valsts tiesību aktiem piešķīrusi pagaidu *PSC* vai arī ir apliecinājusi, ka šīs personas drošības pielaides izskatīšanas process jau ir sācies un ka dokumentācijas iepriekšējajās pārbaudēs nav atklājusies negatīva informācija; un
	8. dokuments par izņēmuma piemērošanu, tostarp objekta un tās informācijas apraksts, kurai tikusi apstiprināta piekļuve, ir jāglabā atbildīgajam drošības birojam un periodiski jānosūta *NOS*.
2. Procedūru, kas aprakstīta 33. un 35. punktā, veic vienīgi uz šādos gadījumos:
	1. tādas personas īslaicīga nodarbināšana, kura ir neaizstājama, ņemot vērā tās spējas attiecīgās darbības jomā;
	2. tulku – gan no NATO dalībvalstīm, gan no valstīm, kas nav NATO dalībvalstis, nodarbināšana.

Šī procedūra attiecībā uz piekļuvi NATO telpām vai NATO klasificētajai informācijai nav izmantojama vairākkārt. Tādēļ *NOS* glabā dokumentāciju par izņēmumu piemērošanu un atbilstoši informē *NSC* (NATO *Security Committee* – Drošības jautājumu komiteju).

## To valstu tulku, kuras nav NATO dalībvalstis, nodarbināšana

1. Atļauju pieņemt darbā tādus tulkus, kas nav NATO dalībvalsts valstspiederīgie, var dod izņēmuma kārtā šādos gadījumos:
	1. lai varētu tulkot no attiecīgās valodas / attiecīgajā valodā, nepieciešama ir persona, kurai kāda no šīm valodām ir dzimtā un kura nav NATO dalībvalsts valstspiederīgā; un
	2. NATO klasificētā informācija, kas ir jāpārtulko, ir tikusi izvērtēta, un ir atļauta tās nodošana tulka izcelsmes valstij.

Piemēro 33. punkta b)-c)-f)-h) apakšpunkta noteikumus.

## Piekļuve ārkārtas gadījumos

1. Kara laikā, pieaugoša starptautiskā spiediena periodos, starptautisko operāciju, kas tiek veiktas īpašos apstākļos, vai miera laikā, spēku izvēršanas vai pēc izsaukuma veikto / mācību uzdevumu izpildes laikā, kad tas nepieciešams, lai veiktu ārkārtas pasākumus, dalībvalstis un NATO civilo un militāro institūciju vadītāji var izņēmuma apstākļos sankcionēt, dodot rakstisku atļauju, piekļuvi NATO klasificētajai informācijai personām, kurām nav vajadzīgās personāla drošības pielaides, ar nosacījumu, ka šāda atļauja ir absolūti nepieciešama un nav pamatotu šaubu par to, ka konkrētais indivīds ir lojāla un uzticama persona, uz kuru var paļauties. Tiek glabāts šīs atļaujas dokuments, kurā aprakstīta informācija, attiecībā uz kuru tika atļauta piekļuve.
2. Gadījumā, ja informācija ir klasificēta kā *CTS* informācija, šo piekļuvi ārkārtas gadījumos, kad vien iespējams, atļauj tikai tām personām, kurām ir atļauts piekļūt valsts SEVIŠĶI SLEPENAJAI informācijai vai tādai informācijai, kas klasificēta kā NS informācija.

## Personāla drošības pielaides augsta ranga valsts amatpersonām

1. Kārtība, kādā NATO klasificētajai informācijai var piekļūt augsta ranga valsts amatpersonas (piemēram, valstu un valdību vadītāji, valdības ministri, parlamenta locekļi un tiesneši), ir noteikta valstu tiesību aktos; šīs *SGO* (*Senior Government Officials* – augsta ranga valsts amatpersonas) ir jāinstruē par to pienākumiem drošības jomā attiecībā uz NATO klasificētās informācijas aizsardzību.

## Laulāto / apgādājamo personu piekļuve NATO klasificētajai informācijai

1. Laulātajiem vai apgādājamajām personām, kas pieņemtas darbā NATO civilajās un militārajās institūcijās un kurām ir jābūt nodrošinātai piekļuvei NATO klasificētajai informācijai saskaņā ar nepieciešamības zināt principu, tiek piešķirta drošības pielaide, un tās tiek instruētas par to pienākumiem drošības jomā attiecībā uz NATO klasificētās informācijas aizsardzību. Drošības pielaides izskatīšanas process ietver vismaz to prasību izpildi, kuras noteiktas attiecībā uz personāla drošības pielaidi un kas norādītas 11. un 13. punktā.

## PIEDALĪŠANĀS KONFERENCĒS UN SANĀKSMĒS

1. Atļauja personai piedalīties konferencē, kursos, sanāksmē vai seminārā tiek dota, pamatojoties uz turpmāk minēto:
	1. ja nepieciešams, veic identitātes pārbaudi un apstiprina personai izsniegto atļauju un piešķirto drošības pielaidi:
	2. iesniedz personāla drošības pielaides apstiprinājumu, kā noteikts 2. papildinājumā;
	3. šo veidlapu izdod NATO civilās vai militārās institūcijas, *NSA* vai cita kompetentā valsts iestāde, un to pārsūta attiecīgajām iestādēm; izņēmuma kārtā tā var personīgi atrasties pie paša attiecīgā delegāta;
	4. attiecīgos gadījumos un ja ir vienojušās iestādes, kas saņem un pārsūta veidlapu, par pieņemamu tiek atzīts uzvārdu kopsaraksts, kurā ir ietverta sīkāka informācija, kas noteikta 2. papildinājumā;
	5. NATO objektos, kur ir valstu diplomātiskās vai militārās delegācijas/pārstāvniecības, NATO objekta Drošības birojs un valstu delegācijas/pārstāvji vienojas par īpašu kārtību, saskaņā ar kuru valstu delegācijas/pārstāvji, lūdzot izsniegt caurlaidi iekļūšanai objektā, iesniedz NATO objekta drošības birojam apliecinājumu par to, ka to valstspiederīgajam ir atbilstoša pielaide; un
	6. attiecībā uz NATO objektu vai iestāžu apmeklējumiem ar jebkādu mērķi, ko veic uzņēmuma pārstāvji, konsultanti vai līgumdarbinieki, ir jāievēro NATO Drošības politikas C-M(2002)49 "G" pielikuma un to papildinošās Direktīvas par industriālo drošību AC/35-D/2003 pēdējā redakcija.

## KURJERI / APSARGI / PAVADOŅI

1. Darbā pieņemtajiem kurjeriem un apsargiem, kuriem jāpārnēsā/jāpārvadā dokumenti, kas klasificēti kā *NC* vai kuriem noteikta augstāka slepenības pakāpe, viņu *NSA* piešķir vismaz NS līmeņa drošības pielaidi, ja vien netiek piemēroti īpaši tiesību akti nacionālās drošības jomā. Kurjerus, apsargus un pavadoņus instruē par NATO drošības procedūrām un viņu pienākumiem attiecībā uz viņiem uzticētās NATO klasificētās informācijas aizsargāšanu. Ja tādas personas kā apsargi un pavadoņi strādā apstākļos, kuros tie varētu nesankcionēti piekļūt klasificētajai informācijai, tām ir jāpiešķir drošības pielaide līmenī, ko par atbilstīgu uzskata kompetentā drošības iestāde.

## PIEKĻUVE INFORMĀCIJAI PERSONĀM, KURĀM NAV NATO DALĪBVALSTS VALSTSPIEDERĪBAS

1. Personām, kurām nav NATO dalībvalsts valstspiederības un kuras kā integrētas militārpersonas dienē NATO dalībvalstu bruņotajos spēkos, var tikt atļauta piekļuve klasificētai informācijai, kuras slepenības pakāpe ir līdz *CTS* (ieskaitot). Gadījumos, kas attiecas uz šādiem valstspiederīgajiem, NATO dalībvalsts *NSA* ir saistošs pienākums pārliecināties, ka tiek izpildīti nosacījumi attiecībā uz drošības pielaidi un piekļuvi informācijai, kas noteikti šajā direktīvā un NATO Drošības politikā.
2. Saskaņā ar vispārējajiem NATO Drošības politikas noteikumiem personām, kuras ir valstu, kas nav NATO dalībvalstis, valstspiederīgie[[3]](#footnote-3), vai arī kuras pārstāv starptautisku organizāciju, var tikt atļauta piekļuve NATO klasificētajai informācijai, katru konkrētu gadījumu izvērtējot atsevišķi, ar nosacījumu, ka:
	1. piekļuve ir nepieciešama, lai palīdzētu īstenot noteiktu NATO programmu, projektu, izpildīt līguma nosacījumus, operāciju vai saistīto uzdevumu;
	2. NATO personāla drošības pielaide (*PSC*) personai tiek piešķirta, pamatojoties uz pielaides izskatīšanas procedūras rezultātiem, kura nav mazāk stingra par to, kas noteikta attiecībā uz NATO valstspiederīgo saskaņā ar NATO drošības politiku un papildu direktīvām; jāpiezīmē, ka NATO *PSC* nav nepieciešama, lai varētu piekļūt *NR* informācijai;
	3. tiek saņemta iepriekšēja rakstiska piekrišana no NATO dalībvalsts vai NATO civilās vai militārās institūcijas, kas sagatavojusi informāciju; un
	4. attiecīgā persona, kas nav NATO dalībvalsts valstspiederīgais, ir skaidri sapratusi un apņemas, personīgi parakstot apliecinājumu par saviem pienākumiem, ka NATO informācija, kurai tā varētu piekļūt saistībā ar noteiktu NATO programmu, projektu, līgumu, operāciju vai saistīto uzdevumu, tiks noteikti izmantota vienīgi mērķiem, kas saistīti ar uzticēto uzdevumu, un netiks darīta zināma vai nodota trešajām personām, institūcijām, organizācijām vai valdībām.
3. Izņēmuma kārtā atkāpjoties no 43 c) apakšpunktā ietvertās prasības par kontroli, ko īsteno autors, NATO dalībvalstu *NSA* var piekrist, ka NATO klasificētajai informācijai drīkst piekļūt noteiktu valstu, kas nav NATO dalībvalstis, valstspiederīgie, kurus pieņēmušas darbā NATO civilās vai militārās institūcijas, NATO dalībvalsts valdība vai arī darbuzņēmējs, kas atrodas un ir reģistrēts NATO dalībvalstī, ar nosacījumu, ka papildus kritērijiem, kas norādīti 43(a), 43(b) un 43(d) apakšpunktā, tiek izpildīti visi turpmāk norādītie kritēriji:
	1. informāciju izpaust drīkst vienīgi personām, kas ir šādu valstu valstspiederīgie: Austrālija, Austrija, Jaunzēlande, Īrija, Somija, Šveice un Zviedrija. *NSA* var ierosināt veikt izmaiņas valstu sarakstā, iesniedzot priekšlikumus izskatīšanai *NSC*;
	2. piekļuve ir ierobežota un tiek nodrošināta vienīgi klasificētai informācijai, kuras slepenības pakāpe nav augstāka par *NS*, un atbilstoši izplatīšanas ierobežojumam vai administratīvajai norādei, kuru uzlicis autors. Netiek nodrošināta piekļuve *CTS* informācijai, *ATOMAL* (*documents containing United States atomic information – dokumenti, kas satur ASV ar atomieročiem saistītu informāciju*)vai citai īpašas kategorijas informācijai;
	3. personai, kurai nav NATO dalībvalsts valstspiederības, piešķir pielaidi NATO klasificētajai informācijai tikai uz laiku, kas nepieciešams, lai sniegtu noteikto atbalstu, īstenojot NATO projektu, programmu, līgumu, operāciju vai saistīto uzdevumu. Par piekļuves NATO klasificētajai informācijai kontroli pilnībā atbildīgs ir objekta vai organizācijas, kurā tiek nodrošināta piekļuve, drošības speciālists; drošības speciālists ir NATO dalībvalsts valstspiederīgais;
	4. piekļuves informācijai mērķis ir tāds, kā sākotnēji bija paredzēts, informāciju sniedzot NATO;
	5. ir noteikts informācijas drošības režīms vai vienošanās par drošības jautājumiem starp tās NATO dalībvalsts valdību, kas vēlas nodrošināt piekļuvi informācijai, un tās valsts valdību, kuras pilsonība ir personai, kurai nav NATO dalībvalsts valstspiederības. Turklāt NATO dalībvalsts, kas nodrošinās piekļuvi informācijai, saskaņā ar saviem nacionālajiem tiesību aktiem nodrošina, lai tai būtu pietiekama kontrole un jurisdikcija attiecībā uz personu, kurai nav NATO dalībvalsts valstspiederības, lai nodrošinātu iespēju šo personu saukt pie atbildības un noteikt, ka tā ir atbildīga par pienācīgu rīcību ar NATO klasificēto informāciju. Nepieciešamības gadījumā NATO dalībvalsts var rīkoties kā atbalstītājs attiecībā uz personām, kurām nav NATO dalībvalsts valstspiederības un kuras pieņemtas darbā NATO civilajās vai militārajās institūcijās; un
	6. NATO dalībvalsts, kas nodrošinās piekļuvi informācijai, vēlas valstij, kuras pilsonība ir personai, kurai nav NATO dalībvalsts valstspiederības, nodrošināt piekļuvi savai līdzīga veida un slepenības pakāpes klasificētajai informācijai.

## NATO NEKLASIFICĒTS[[4]](#footnote-4)\*

## 1. pielikums

## NATO PERSONĀLA DROŠĪBAS PIELAIDES APLIECĪBA

1. Ar šo tiek apliecināts, ka:

Pilns vārds, uzvārds:

Dzimšanas datums un vieta:

personāla drošības pielaidi ir piešķīrusi:

saskaņā ar spēkā esošajiem NATO noteikumiem, tostarp C-M(64)39 pielikumu par drošību *ATOMAL* informācijas gadījumā, un tādēļ tiek atzīts, ka ir izpildītas prasības, lai viņam varētu uzticēt informāciju, kuras slepenības pakāpe ir līdz (ieskaitot): [[5]](#footnote-5)

1. Šīs apliecības derīguma termiņš beigsies ne vēlāk kā: [[6]](#footnote-6)

Parakstījis:

Amats: Oficiāls valdības zīmogs

Izdošanas datums:

Izdevējiestādes kontaktinformācija (tālrunis, e-pasts, fakss):

## NATO NEKLASIFICĒTS[[7]](#footnote-7)\*

## 2. pielikums

## NATO PERSONĀLA DROŠĪBAS PIELAIDES APSTIPRINĀJUMS

1. Ar šo tiek apstiprināts, ka:

Pilns vārds, uzvārds:

Dzimšanas datums:

Dzimšanas vieta:

Valstspiederība:

Darbavieta:

Apmeklējuma mērķis un ilgums:

Pases / personas apliecības Nr.:

Izdota: Datums:

Militāra dienesta pakāpe un numurs (attiecīgos gadījumos)

 atļauta piekļuve NATO klasificētajai informācijai, kuras slepenības pakāpe ir līdz (ieskaitot)

saskaņā ar NATO drošības noteikumiem, tostarp C-M(64)39 pielikumam par drošību *ATOMAL* informācijas gadījumā, un viņu ir atbilstoši instruējis

Parakstījis:

Amats: Oficiālais zīmogs

Izdošanas datums:

1. Šī apstiprinājuma derīguma termiņš beigsies ne vēlāk kā:

3. Izdevusi

(Dalībvalsts vai NATO civilā vai militārā institūcija)

Izdošanas datums un vieta:

Izdevējiestādes kontaktinformācija (tālrunis, e-pasts, fakss):

1. Industriālās drošības kontekstā ir noteikums (Sk. Direktīvas par industriālo drošību 43. un 44. punktu), ka *NSA/DSA* (*Designated State* *Authority* – pilnvarotajai valsts iestādei) ir jāpiešķir *PSC* personai, kurai ir citas NATO dalībvalsts valstspiederība/pilsonība. [↑](#footnote-ref-1)
2. Industriālās drošības kontekstā ir noteikums (Sk. Direktīvas par industriālo drošību 43. un 44. punktu), ka *NSA/DSA* ir jāpiešķir *PSC* personai, kurai ir citas NATO dalībvalsts valstspiederība/pilsonība. [↑](#footnote-ref-2)
3. Valstu, kas nav NATO dalībvalstis, valstspiederīgie ir "karalistes pavalstnieki", "valsts pilsoņi" un "pastāvīgie iedzīvotāji Kanādā". "Pastāvīgie iedzīvotāji Kanādā" ir personas, attiecībā uz kurām ir veikts pārbaužu process, tostarp dzīvesvietas pārbaudes, ziņu par sodāmību un drošības pārbaudes un kuras gatavojas saņemt likumīgi izsniegtu atļauju, lai varētu iekārtot pastāvīgu dzīves vietu valstī. [↑](#footnote-ref-3)
4. \* Apzīmējums nav parauga daļa. [↑](#footnote-ref-4)
5. Attiecīgos gadījumos ieraksiet vienu vai vairākus no turpmāk minētajiem:

|  |  |  |  |
| --- | --- | --- | --- |
| (a) | SEVIŠĶI SLEPENI | (d) | SEVIŠĶI SLEPENI *ATOMAL* |
| (b) | NATO SLEPENI | (e) | NATO SLEPENI *ATOMAL* |
| (c) | NATO KONFIDENCIĀLI | (f) | NATO KONFIDENCIĀLI *ATOMAL* |

 [↑](#footnote-ref-5)
6. Termiņa beigu datums atbilst Direktīvas par personāla drošību 18. punkta noteikumiem. [↑](#footnote-ref-6)
7. \* Apzīmējums nav parauga daļa. [↑](#footnote-ref-7)