CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

APSTIPRINU
LU aģentūras „Latvijas Universitātes Matemātikas un informātikas institūts"
direktors R.Balodis-Bolužs

Rīga, 2012.gada __.

Kārtība, kādā tiek sertificēta ES Regulai Nr. 211/2011 "par pilsoņu iniciatīvu" atbilstoša iniciatīvas atbalsta tiešsaistes vākšanas sistēma

Izdota saskaņā ar Latvijas Republikas likuma "Par tautas nobalsošanu, likumu ierosināšanu un Eiropas pilsoņu iniciatīvu" IV[1] nodaļas 25.[1] panta (2) punktu

I. Vispārīgie noteikumi

1. Instrukcija nosaka kārtību Informācijas tehnoloģiju drošības incidentu novēršanas institūcijā (CERT.LV), kādā:
   1.1. tiek pieņemts Organizatoru iesniegums Eiropas Parlamenta un Padomes (ES) 2011.gada 16.februāra Regulai Nr. 211/2011 "par pilsoņu iniciatīvu" atbilstošas vākšanas tiešsaistes sistēmas sertificēšanai;
   1.2. tiek veiktas izveidotās vākšanas tiešsaistes sistēmas un informācijas sistēmas atbilstības pārbaudes;
   1.3. tiek pieņemts lēmums par sertifikāta izsniegšanu vai par atteikumu izsniegt sertifikātu.
2. Eiropas pilsoņu iniciatīvas (turpmāk tekstā – Iniciatīva) izveides un sertifikācijas pārbaužu kārtība kā arī kompetento valsts iestāžu darbība ir noteikta šādos spēkā esošos normatīvajos dokumentos un standartos:
   2.1. Eiropas Parlamenta un Padomes (ES) 2011.gada 16.februāra Regula Nr. 211/2011 "par pilsoņu iniciatīvu" (turpmāk tekstā – Regula);
   2.2. Eiropas Komisijas īstenošanas Regula (ES) 2011.gada 17.novembra Regula Nr. 1179/2011 "ar ko nosaka tehniskās specifikācijas vākšanas tiešsaistes sistēmām saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 211/2011 par pilsoņu iniciatīvu " (turpmāk tekstā – Tehniskā specifikācija);
   2.3. Latvijas Republikas likums "Par tautas nobalsošanu, likumu ierosināšanu un Eiropas pilsoņu iniciatīvu" (turpmāk tekstā – Likums);
   2.4. Latvijas Republikas "Informācijas atklātības likums";
   2.5. Latvijas Republikas "Fizisko personu datu aizsardzības likums";
   2.6. Starptautiskās standartizācijas organizācijas un Starptautiskās elektrotehniskās komisijas standarti ISO/IEC 27001 un ISO/IEC 27002.
3. Par elektroniskās tiešsaistes vākšanas sistēmas sertificēšanu kompetentā iestāde (turpmāk tekstā – Sertificētājs) – Informācijas tehnoloģiju drošības incidentu novēršanas institūcija (turpmāk tekstā – CERT.LV), Adrese – Raiņa bulvāris 29, Rīga, LV1459, tālr.: +371 67085858, fakss: +371 67225072, elektroniskais pasts: eci@cert.lv.
4. Iniciatīvas Organizatori ir fiziskas personas, kuras veido pilsoņu komiteju, kura ir atbildīga par

pilsoņu iniciatīvas atbalsta tiešsaistes vākšanas sistēmas izveidi, ieviešanu, uzturēšanu, dokumentācijas sagatavošanu un pieteikšanu sertifikāta izsniegšanai atbilstoši Regulas un Tehniskās specifikācijas prasībām.

5. Iniciatīvas atbalsta tiešsaistes vākšanas sistēma (turpmāk tekstā – TVS) šīs instrukcijas izpratnē ir informācijas sistēma, kas sastāv no programmatūras, aparatūras, mitināšanas vides (*hosting*), darba procesiem un personāla, lai tiešsaistē vāktu paziņojumus par atbalstu. To izveido, uztur, sertificēšanai sagatavo un piesaka Organizatori atbilstoši visām Regulas prasībām.
6. Informācijas sistēma (turpmāk tekstā – IS) šīs instrukcijas izpratnē ir informācijas tehnoloģiju, programmatūras, mitināšanas vides, infrastruktūras drošības, darba procesu, sistēmu aprakstošas dokumentācijas un apkalpojošā personāla kopums.
7. TVS IS uzturētājs (turpmāk tekstā – Uzturētājs) šīs instrukcijas izpratnē ir fiziska vai juridiska persona, kurai Organizatori ir oficiāli deleģējuši pienākumu nodrošināt šādas IS uzturēšanu, uzraudzību, funkcionalitāti un drošību. Uzturētājam ir jāatbilst ISO/IEC 27001 sertifikācijai, bez pienākuma to formāli pārņemt, kas ir apliecināta ar standartam atbilstoši sagatavotu IS dokumentāciju.

II. Sertifikācijas process

8. Iniciatīvas TVS sertifikācijas process tiek uzsākts tikai pēc Organizatoru rakstiska lūguma un TVS sertifikācijas pieteikuma (pielikums Nr.1) saņemšanas un reģistrācijas brīža Latvijas Universitātes aģentūras "Latvijas Universitātes Matemātikas un informātikas institūts" (LU MII) Sevišķajā lietvedībā.
9. Sertifikācijas procesa diagramma parādīta instrukcijas pielikumā Nr.2.
10. Organizatori vienlaicīgi ar pieteikumu iesniedz visu Regulā un Tehniskajā specifikācijā minēto dokumentāciju un pierādījumus par izveidotās TVS IS atbilstību tai izvirzītajām prasībām, tajā skaitā:
    - 10.1. visas TVS IS **risku analīze**, kas sevī ietver vismaz šādus aspektus: izmantotās informācijas tehnoloģijas, apkārtējā vide, operējošā sistēma, servisu konfigurācija, infrastruktūras drošība, rezerves kopiju izveide, IS žurnāl-faili (*system log*), drošības kontroles, sistēmas monitorings un reakcija uz incidentiem;
    - 10.2. detalizēts **atbilstības novērtējums**, kas veikts, lai novērtētu TVS IS drošības atbilstību attiecībā pret Tehnisko specifikāciju un Standartu ISO/IEC 27001;
    - 10.3. detalizēta visas TVS IS **ievainojamību novērtējums un analīze**, kas tiek veikta pēc baltās-kastes/melnās-kastes (*white-box/black-box*) principa ar mērķi simulēt iekšējā/ārējā uzbrucēja ielaušanos;
    - 10.4. ieteicams veikt **ielaušanās testu**, lai novērtētu kā ievainojamības var tikt izmantotas un identificētu iespējamos ielaušanās ceļus. Ielaušanās testam ir jāsniedz risinājumi, kā šīs ievainojamības novērst, lai panāktu drošu sistēmu;
    - 10.5. ja Organizatori nav TVS IS vai visu tās elementu Uzturētājs, tad – **apstiprinātu līguma kopiju ar TVS vai tā elementu Uzturētāju**, kurā ir nepārprotami norādīts, ka tā sniegtais pakalpojums un infrastruktūras drošība atbilst Regulā un Tehniskajā specifikācijā noteiktajām prasībām;
    - 10.6. ja netiek lietots Eiropas Komisijas izstrādātais programmnodrošinājums – iniciatīvas TVS **izejas koda kopiju** (marķētā CD/DVD matricā).
11. Organizatori pieteikumu un pielikumos esošo dokumentāciju iesniedz Latviešu vai Angļu valodā.
12. Sertificētājs visu, Organizētāju iesniegto, dokumentāciju un informāciju marķē atbilstoši Latvijas Republikas "Informācijas atklātības likumam" kā ierobežotas pieejamības informāciju, un uzglabā

līdz TVS darbības beigām, bet ne mazāk kā 12 (divpadsmit) mēnešus no TVS sertifikācijas brīža.

13. Ja Organizatori kopā ar pieteikumu nav iesnieguši pilnīgu nepieciešamo dokumentāciju un informāciju, tad Sertificētājs par to informē Organizatorus, un nosaka termiņu līdz kuram ir jāveic neatbilstību labojumi un jāiesniedz iztrūkstošā informācija. Ja Organizatori, viņiem noteiktajā termiņā, visu pieprasīto informāciju nesniedz, tad Sertificētājs pieņem lēmumu par atteikumu uzsākt sertifikāciju un izsniegt sertifikātu.
14. Sertifikācijas izpilde un sertifikācijai noteiktais termiņš (viens mēnesis) sākas no visas nepieciešamās pilnīgās informācijas saņemšanas no Organizatoriem brīža.
15. Sertificētājs saskaņā ar Regulu un Tehnisko specifikāciju, TVS IS sertifikāta izsniegšanas noteiktajā laika periodā, veic:
    15.1. Organizatoru iesniegtās dokumentācijas pārbaudi ar mērķi pārliecināties, ka izveidotā TVS IS ir atbilstoši dokumentēta, veikta pilnvērtīga IS risku analīze un ir noteiktas drošības kontroles;
    15.2. TVS IS elementu fiziskā izvietojuma un infrastruktūras drošības pārbaudi ar mērķi pārliecināties, ka tā atbilst iesniegtajā dokumentācijā aprakstītajam un Tehniskajā specifikācijā noteiktajam. Ja fiziskā izvietojuma pārbaudi nav iespējams veikt, tad tiek pārbaudīti atbilstošie nosacījumi Organizētāja ar Uzturētāju noslēgtajā līgumā;
    15.3. TVS IS atbilstības Tehniskajai specifikācijai pārbaudi ar mērķi pārliecināties, ka ir ieviestas un izpildītas visas Tehniskajā specifikācijā noteiktās prasības, par ko tiek aizpildīta Eiropas Komisijas (turpmāk tekstā – EK) sagatavotā TVS sertifikācijas pārbaudes lapa (*checklist*) (pielikums Nr.4);
    15.4. tiešsaistē esošas TVS funkcionalitātes pārbaudi ar mērķi pārliecināties par TVS funkcionālu, korektu un Tehniskajai specifikācijai atbilstošu darbību;
    15.5. tiešsaistē esošas TVS ievainojamību pārbaudi (*penetration test*) ar mērķi pārliecināties par tiešsaistē esošo TVS elementu drošību, veicot vismaz pārbaudes atbilstoši Atvērtā tīmekļa lietotņu drošības projekta (Open Web Application Security Project (OWASP)) 2010 Top 10 identificētajām ievainojamībām un apdraudējumiem;
    15.6. ja tiek uzskatīts par nepieciešamu, tad veic TVS programmnodrošinājuma izejas koda inspekciju ar mērķi pārliecināties par izstrādāta TVS koda kvalitāti un tā ievainojamībām.
16. Par pārbaudes procesā konstatētajām nepilnībām un kļūdām Sertificētājs informē Organizatorus, uzskaitot veiktās pārbaudes, konstatētās neatbilstības un ievainojamības un to novēršanas termiņus.
17. Ja pirmreizējās pārbaudes rezultātā tika konstatētas neatbilstības, tad noteiktajā laika periodā saņemot atbildes vēstuli no Organizatora par veiktajiem pasākumiem neatbilstību novēršanā, Sertificētājs veic atkārtotu pārbaudi ar mērķi pārliecināties, ka konstatētās neatbilstības ir novērstas.
18. Ja visu veikto pārbaužu rezultātā netiek konstatētas neatbilstības Regulas un Tehniskās specifikācijas prasībām, kā arī nav identificētas būtiskas ievainojamības, tad Sertificējis pieņem lēmumu par TVS sertificēšanu, izsniedzot Regulas IV pielikumam atbilstošu sertifikātu (pielikums Nr.3).
19. Ja veikto pārbaužu rezultātā ir konstatētas neatbilstības Regulas un Tehniskās specifikācijas prasībām, kā arī ir konstatētas būtiskas ievainojamības, kuras Organizētājs, tam noteiktajos termiņos, nav novērsis, tad Sertificētājs pieņem lēmumu par atteikumu izsniegt TVS sertifikātu.
20. Oficiālās sarakstes dokumentāciju sagatavo CERT.LV par Sertifikāciju atbildīgā amatpersona, to saskaņo CERT.LV vadītājs vai tā vietnieks un paraksta LU MII direktors vai izpilddirektors.

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

21. Sertificētājs informē Organizatoru par pārbaužu rezultātos konstatētajām neatbilstībām, TVS sertifikāta izsniegšanu vai lēmuma pieņemšanu par atteikumu izsniegt sertifikātu, kā arī citas būtiskas papildus informācijas pieprasīšanu vai apmaiņu, rakstiski nosūtot vēstuli un tās elektronisko kopiju ar elektroniskā pasta starpniecību uz Organizatora pieteikumā norādītajām saziņas adresēm. Pārējā sertifikācijas procesa laikā informācijas apmaiņa notiek ar elektroniskā pasta sarakstes starpniecību, Sertificētājam lietojot adresi – eci@cert.lv.

Izstrādāja:
CERT.LV Informācijas sistēmu drošības auditors
Bernhards Blumbergs

CERT.LV vadītāja
Baiba Kaškina

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Pielikums Nr.1
Kārtībai, kādā tiek sertificēta
ES Regulai Nr. 211/2011
"par pilsoņu iniciatīvu" atbilstoša
iniciatīvas atbalsta
tiešsaistes vākšanas sistēma

PILSOŅU INICIATĪVAS ATBALSTA TIEŠSAISTES VĀKŠANAS SISTĒMAS SERTIFIKĀCIJAS PIETEIKUMS

1. Informācija par atbalsta tiešsaistes vākšanas sistēmu (TVS):

_____
(ierosinātās pilsoņu iniciatīvas nosaukums)

_____ _____
(tīmekļa vietnes adrese) (tīmekļa vietnes IP adrese)

_____

_____
(TVS Informācijas sistēmas un tās elementu fiziskā izvietojuma vietas adrese)

TVS izmanto nemodificētu Eiropas Komisijas (EK) izstrādāto programmnodrošinājumu: ☐ Jā ☐ Nē

_____
(EK izstrādātas TVS versijas numurs)

_____ _____
(Serveru operējošā sistēma un versija) (Relāciju datubāzes vadības sistēma un versija)

2. TVS atbildīgās personas un kontaktinformācija:

No Organizatoru puses:

_____ _____ _____ _____
(vārds, uzvārds) (e-pasta adrese) (kontakttālrunis) (kontakttālrunis)

_____
(adrese)

No TVS Uzturētāja puses:

_____ _____ _____ _____
(vārds, uzvārds) (e-pasta adrese) (kontakttālrunis) (kontakttālrunis)

_____
(adrese)

No TVS programmnodrošinājuma izstrādātāju puses (ja netiek izmantota EK izstrādātā TVS):

_____ _____ _____ _____

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

(vārds, uzvārds) (e-pasta adrese) (kontakttālrunis) (kontakttālrunis)

(adrese)

3. Sertifikācijas pārbaužu pilnvarojums:
Mēs, uz visu sertifikācijas periodu, pilnvarojam Sertificētāju piešķirot tam tiesības piekļūt TVS informācijas sistēmai (IS), veikt TVS IS fiziskā izvietojuma un infrastruktūras drošības pārbaudi, izpildīt tiešsaistē esošas TVS funkcionalitātes pārbaudi un ievainojamību testēšanu.
Apliecinām, ka Sertificētājs nenes atbildību par iespējamiem TVS IS darbības traucējumiem, kas var rasties tā veikto funkcionalitātes un ievainojamību pārbaužu rezultātā.

4. Atbilstības apliecinājums:
Apliecinām, ka mūsu izveidotā un ieviestā TVS pilnībā atbilst visām Eiropas Parlamenta un Padomes (ES) 2011.gada 16.februāra Regulā Nr. 211/2011 "par pilsoņu iniciatīvu" un Komisijas īstenošanas Regulā (ES) 2011.gada 17.novembra Regula Nr. 1179/2011 "ar ko nosaka tehniskās specifikācijas vākšanas tiešsaistes sistēmām saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 211/2011 par pilsoņu iniciatīvu " noteiktajām prasībām.

5. Atbilstības informācijas pievienošana:
Mēs pievienojam un iesniedzam visu dokumentāciju un informāciju, kas pierāda izveidotās TVS atbilstību tai izvirzītajām prasībām. Apliecinām, ka visa iesniegtā informācija ir pilnīga un patiesa.

Nr.p.k.	Veids (dokuments vai elektronisks datu nesējs)	Nosaukums	Reģistrācijas numurs	Lapaspušu skaits (informācijas daudzums MB)

20___. gada ___._____

Organizatoru pilsoņu komitejas pārstāvis:

_____
(vārds, uzvārds, paraksts)

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Pielikums Nr.3
Kārtībai, kādā tiek sertificēta
ES Regulai Nr. 211/2011
"par pilsoņu iniciatīvu" atbilstoša
iniciatīvas atbalsta
tiešsaistes vākšanas sistēma

SERTIFIKĀTS, KAS APSTIPRINA VĀKŠANAS TIEŠSAISTES SISTĒMAS ATBILSTĪBU EIROPAS PARLAMENTA UN PADOMES 2011. GADA 16. FEBRUĀRA REGULAI (ES) Nr. 211/2011 PAR PILSOŅU INICIATĪVU

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija (CERT.LV) ar šo apliecina, ka vākšanas tiešsaistes sistēma

_____, ko izmanto paziņojumu par atbalstu
(tīmekļa vietnes adrese)

_____
(ierosinātās pilsoņu iniciatīvas nosaukums)

vākšanai, atbilst attiecīgajiem Regulas (ES) Nr. 211/2011 noteikumiem.

Rīgā, 20___. gada ___._____

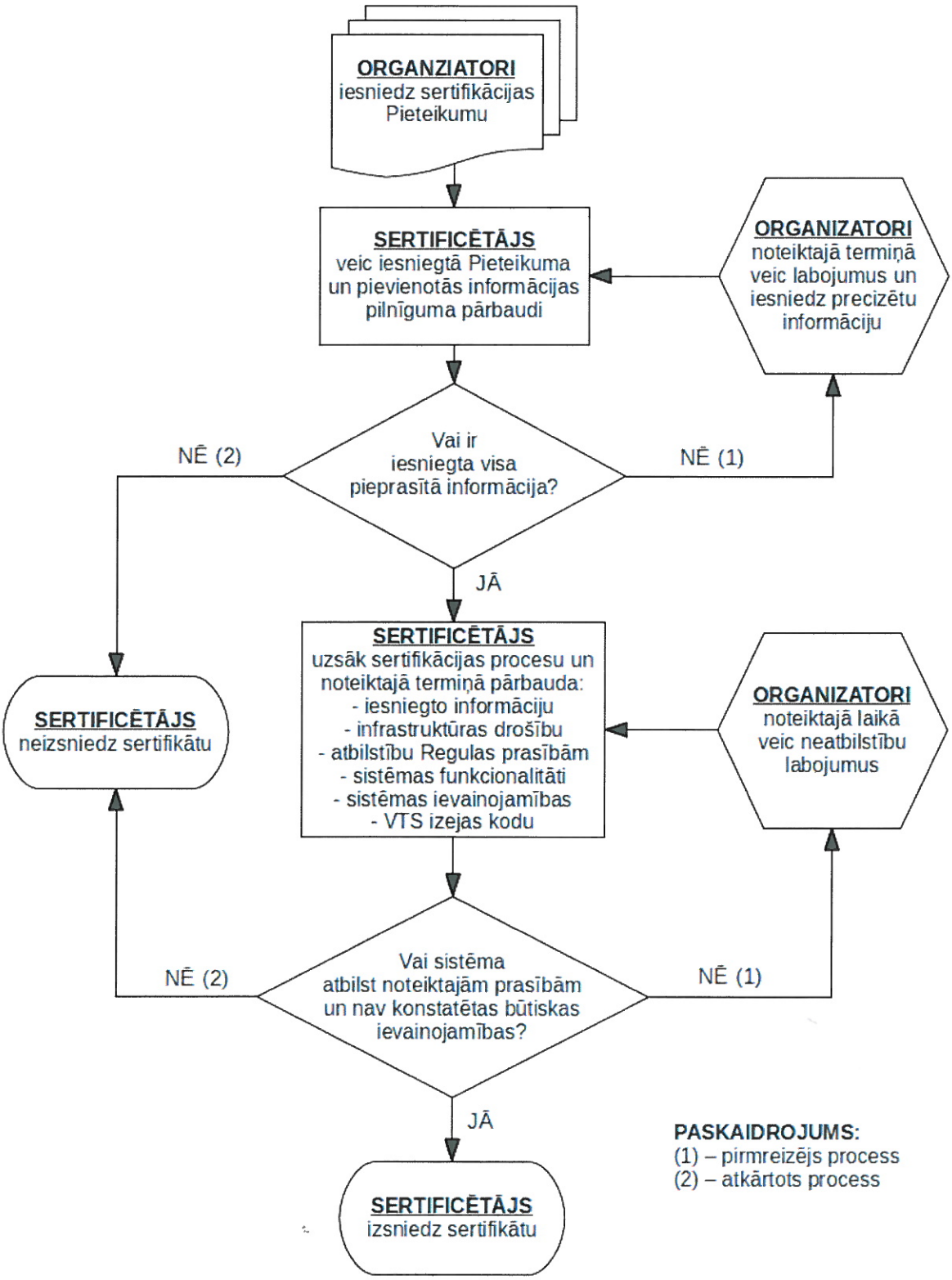
LU Matemātikas un informātikas institūts
Direktors Rihards Balodis-Bolužs

Iestādes oficiālais zīmogs:

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Pielikums Nr.2

Sertifikācijas procesa diagramma



PASKAIDROJUMS:
(1) – pirmreizējs process
(2) – atkārtots process

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Pielikums Nr.4
Kārtībai, kādā tiek sertificēta
ES Regulai Nr. 211/2011
"par pilsoņu iniciatīvu" atbilstoša
iniciatīvas atbalsta
tiešsaistes vākšanas sistēma

VĀKŠANAS TIEŠSAISTES SISTĒMAS SERTIFIKĀCIJAS PĀRBAUDES LAPA