Procedură Operaţională privind Administrarea sistemului informatic

COD: **PO-SECR-31**

Ediţia: **a II-a**, Revizia: **a II-a**, Data: **28.06.2023**,

Lista responsabililor cu elaborarea, verificarea şi aprobarea ediţiei

Nr. Crt	Elemente privind responsabilii/ operațiunea	Numele și prenumele	Funcția	Data	Semnătura
1.1	Elaborat	Cucu Cristina Mihaela	Secretar	28.06.2023	
1.2	Avizat	Bejenaru Mihaela	Presedinte Comisie Monitorizare	28.06.2023	
1.3	Aprobat	Cîmpanu Monica	Director	28.06.2023	

Situaţia ediţiilor şi a reviziilor în cadrul ediţiilor procedurii

Nr. Crt	Ediția sau, după caz, revizia în cadrul ediției	Componenta revizuită	Modalitatea reviziei	Data de la care se aplică prevederile ediției sau reviziei ediției
2.1	Ediția I	X	X	07.05.2018
2.2	Ediția a II-a	Documente de referintă; Descrierea activității sau procesului	Modificări legislative	31.10.2022
2.3	Revizia I	Documente de referintă; Descrierea activității sau procesului	Modificări legislative	17.03.2023
2.4	Revizia a II-a	Documente de referință	Modificări legislative	28.06.2023

Lista cuprinzând persoanele la care se difuzează ediţia sau, după caz, revizia din cadrul ediţiei procedurii

	Scopul difuzării	Exemplar nr.	Departament	Funcția	Numele și prenumele	Data primirii	Semnătura
3.1	Aplicare, Informare	1		Director	Cîmpanu Monica	28.06.2023	
3.2	Aplicare, Informare	2	Comisie Monitorizare	Presedinte Comisie Monitorizare	Bejenaru Mihaela	28.06.2023	
3.3	Aplicare, Evidență, Arhivare	3	Secretariat	Secretar	Cucu Cristina Mihaela	28.06.2023	

Scopul procedurii

1. Stabilește modul de realizare a activității, compartimentele și persoanele implicate

Procedura asigură implementarea unui set de reguli unitar la nivelul instituției publice ce reglementează condițiile și modul de funcționare a sistemului informatic și stabilirea regulilor, normelor și a măsurilor de siguranță și protecție a datelor și informațiilor din sistemul informatic integrat.

2. Dă asigurări cu privire la existența documentației adecvate derulării activității

Stabilirea responsabilităţilor privind întocmirea, avizarea şi aprobarea documentelor aferente acestei activităţi.

3. Asigură continuitatea activității, inclusiv în condiții de fluctuație a personalului

Prin procedură se urmărește asigurarea unui circuit corect, eficient, operativ și legal al documentelor.

4. Sprijină auditul și/sau alte organisme abilitate în acțiuni de auditare și/sau control, iar pe manager, în luarea deciziei

- Nu este cazul

5. Alte scopuri

- Nu este cazul

Domeniul de aplicare

1. Precizarea (definirea) activității la care se referă procedura operațională:

Procedura se referă la activitatea de administrare a sistemului informatic realizată de personalul din cadrul compartimentului Tehnologia Informației, stabilind totodată regulile, normele și măsurile de siguranță și protecție a datelor și informațiilor din sistemul informatic.

2. Delimitarea explicită a activității procedurate în cadrul portofoliului de activități desfășurate de entitatea publică:

Activitatea este relevantă ca importanță, fiind procedurată distinct în cadrul instituției.

3. Listarea principalelor activități de care depinde și/sau care depind de activitatea procedurată:

De activitatea procedurată depind toate celelalte activități din cadrul instituției, datorită rolului pe care această activitate îl are în cadrul derulării corecte și la timp a tuturor proceselor.

4. Listarea compartimentelor furnizoare de date și/sau beneficiare de rezultate ale activității procedurate:

4.1 Compartimente furnizare de date

Toate structurile

4.2 Compartimente furnizoare de rezultate:

Toate structurile

4.3 Compartimente implicate în procesul activităţii:

Secretariat

Documente de referință

1. Reglementări internaționale:

- REGULAMENT nr. 679 din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)

2 Legislație primară:

- Legea nr. 506/2004, privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare
- Ordinul nr. 3097/2016 pentru aplicarea prevederilor art. 46 alin. (8) și art. 47 alin. (9) din Legea nr. 207/2015 privind Codul de procedură fiscală, Publicat în Monitorul Oficial, Partea I nr. 970 din 05 decembrie 2016
- Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cu modificările și completările ulterioare
- Ordinul nr. 1.323/2020 pentru aprobarea Normelor tehnice privind cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice aplicabile operatorilor de servicii esenţiale, cu modificările și completările ulterioare

3 Legislație secundară:

- Ordin nr. 600/2018 privind aprobarea Codului controlului intern managerial al entităţilor publice Publicat in Monitorul Oficial, Partea I nr. 387 din 07.05.2018
- Instrucţinea nr. 1/2018 din 16 mai 2018 privind aplicarea unitară la nivelul unităţilor de învăţământ preuniversitar a Standardului 9 - Proceduri prevăzut în Codul controlului intern managerial al entităţilor publice, aprobat prin Ordinul secretarului general al Guvernului nr. 600/2018

4 Alte documente, inclusiv reglementări interne ale entității publice:

- Programul de dezvoltare a SCIM
- Regulamentul de funcționare a CEAC
- Regulamentul de funcționare a Comisiei de Monitorizare
- Regulamentul de organizare şi funcționare al instituției
- Regulamentul Intern al Instituției
- Decizii ale Conducătorului Instituției
- Ordine și metodologii emise de ministerul educației
- Alte acte normative

Definiții și abrevieri

1. Definiții ale termenilor:

Nr. Crt.	Termenul	Definiția și / sau, dacă este cazul, actul care definește termenul
1.	Procedură documentată	Modul specific de realizare a unei activități sau a unui proces, editat pe suport de hârtie sau în format electronic; procedurile documentate pot fi proceduri de sistem şi proceduri operaţionale
2.	Procedură operaţională (procedură de lucru)	Procedură care descrie un proces sau o activitate care se desfăşoară la nivelul unuia sau mai multor compartimente dintr-o entitate, fără aplicabilitate la nivelul întregii entități publice
3.	Document	Act prin care se adevereşte, se constată sau se preconizează un fapt, se conferă un drept, se recunoaște o obligație respectiv text scris sau tipărit inscripție sau altă mărturie servind la cunoașterea unui fapt real actual sau din trecut
4.	Aprobare	Confirmarea scrisă, semnătura şi datarea acesteia, a autorităţii desemnate de a fi de acord cu aplicarea respectivului document în unitate.
5.	Verificare	Confirmare prin examinare şi furnizare de dovezi obiective de către autoritatea desemnată (verificator), a faptului că sunt satisfăcute cerinţele specificate, inclusiv cerinţele Comisiei de Monitorizare.
6.	Ediție procedură	Forma actuală a procedurii; Ediția unei proceduri se modifică atunci când deja au fost realizate 3 revizii ale respectivei proceduri sau atunci când modificările din structura procedurii depășesc 50% din conținutul reviziei anterioare;
7.	Revizie procedură	Acţiunea de modificare respectiv adăugare sau eliminare a unor informații, date, componente ale unei ediții a unei proceduri, modificări ce implică de regulă sub 50% din conținutul procedurii;.
8.	Sistem informatic	Prelucrarea automată a datelor din sistem (intrările) conform unor algoritmi prestabiliți, deteminați de regulile de gestiune proprii fiecărei instituții și în conformitate cu reglementările și legislația în vigoare.
9.	Intrări	Totalitatea datelor supuse prelucrărilor
10.	Prelucrări	Totalitatea operaţiilor efectuate asupra datelor pentru obţinerea informaţiilor care stau la baza deciziilor
11.	Ieşiri	Rezultatele prelucrărilor efectuate asupra datelor
12.	Hardware	Totalitatea sistemelor de calcul folosite pentru prelucrarea şi/sau evidenţa datelor
13.	Software	Totalitatea programelor folosite pentru prelucrarea şi/sau evidenţa datelor
14.	Colecţii organizate de date	Baza de date, reprezintă mulţimea datelor supuse prelucrărilor şi/sau evidenţei computerizate
15.	Programul antivirus	Este folosit în general pentru prevenirea şi eliminarea viruşilor de computer, viermilor şi cailor troieni
16.	Resurse umane	Personal tehnic, utilizatori.
17.	Program informatic	Reprezentarea sau implementarea unui algoritm într-un cod sursă
18.	Computer	Este o mijloc tehnic de prelucrat date şi informaţii, conform unei liste de instrucţiuni numită program
19.	Server	Este un program de aplicație care furnizează servicii altor aplicații
20.	Administrator de sistem	Persoana care proiectează, dezvoltă, implementează, întreţine în funcţiune soluţii IT ce includ lucrul în reţea şi accesul la Internet: pune cele mai convenabile soluţii la dispoziţia angajaţilor şi a conducerii, în funcţie de specificul activităţilor desfăşurate şi de rezultatele aşteptate
21.	Reţea locală	Reţea de calculatoare ce acoperă - în general - o arie locală, restrânsă: un birou, o clădire, un grup de clădiri alăturate
22.	Strategia de securitate	Se compune din totalitatea normelor, regulilor, procedurilor, îndrumarelor de bună practică care protejează bunurile organizației: echipamente hardware de orice fel, produse, aplicații, componente software de orice fel, date și orice alt fel de informații.
23.	Entitate publică	Autoritate publică, instituţie publică, companie/societate naţională, regie autonomă, societate la care statul sau o unitate administrativ-teritorială este acţionar majoritar, cu personalitate juridică, care utilizează /administrează fonduri publice şi/sau patrimoniu public
24.	Departament	Direcţie Generală, Direcţie, Serviciu, Birou, Compartiment
25.	Conducătorul departamentului (compartimentului)	Director general, director, şef serviciu, şef birou, şef compartiment

2. Abrevieri ale termenilor:

Nr. Crt.	Abrevierea	Termenul abreviat
1.	PO	Procedura operațională
2.	Ed.	Ediție
3.	Rev.	Revizie
4.	I.T.	Tehnologia Informației
5.	S.I.	ArhivareSistem informatic
6.	BD	Bază de date
7.	ADMIN	Administrator de sistem
8.	EP	Entitate Publică

Descrierea procedurii

1. Generalități:

Securitatea reţelelor şi a sistemelor informatice reprezintă capacitatea unei reţele şi a unui sistem informatic de a rezista, la un nivel de încredere dat, oricărei acţiuni care compromite disponibilitatea, autenticitatea, integritatea, confidenţialitatea sau nonrepudierea datelor stocate ori transmise sau prelucrate ori a serviciilor conexe oferite de reţeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora.

Operatorul ar trebui să ia toate măsurile rezonabile pentru a verifica identitatea unei persoane vizate care solicită acces la date, în special în contextul serviciilor online și al identificatorilor online. Un operator nu ar trebui să rețină datele cu caracter personal în scopul exclusiv de a fi în măsură să reacționeze la cereri potențiale.

Prelucrarea datelor cu caracter personal în măsura strict necesară și proporțională în scopul asigurării securității rețelelor și a informațiilor, și anume capacitatea unei rețele sau a unui sistem de informații de a face față, la un anumit nivel de încredere, evenimentelor accidentale sau acțiunilor ilegale sau rău intenționate care compromit disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor cu caracter personal stocate sau transmise, precum și securitatea serviciilor conexe oferite de aceste rețele și sisteme, sau accesibile prin intermediul acestora, de către autoritățile publice, echipele de intervenție în caz de urgență informatică, echipele de intervenție în cazul producerii unor incidente care afectează securitatea informatică, furnizorii de rețele și servicii de comunicații electronice, precum și de către furnizorii de servicii și tehnologii de securitate, constituie un interes legitim al operatorului de date în cauză. Acesta ar putea include, de exemplu, prevenirea accesului neautorizat la rețelele de comunicații electronice și a difuzării de coduri dăunătoare și oprirea atacurilor de „blocare a serviciului”, precum și prevenirea daunelor aduse calculatoarelor și sistemelor de comunicații electronice.

2. Documente utilizate:

2.1. Lista și proveniența documentelor:

- Documentele utilizate în elaborarea prezentei proceduri sunt cele enumerate la Documentele de referință, precum și anexele dacă este cazul.

2.2. Conținutul și rolul documentelor:

- Documentele utilizate în elaborarea prezentei proceduri au rolul de a reglementa modalitatea de implementare a activității procedurate.
- Accesul, pentru fiecare Compartiment, la legislaţia aplicabilă, se face prin programul informatic la care au acces salariaţii entității.

2.3. Circuitul documentelor:

Pentru asigurarea condiţiilor necesare cunoaşterii și aplicării de către salariaţii entității a prevederilor legale care reglementează activitatea procedurată, elaboratorul va difuza procedura conform Formularului de distribuire/difuzare.

3. Resurse necesare:

3.1. Resurse materiale:

- Computer
- Imprimantă
- Copiator
- Consumabile (cerneală/toner)
- Hartie xerox
- Dosare

3.2. Resurse umane:

- Conducătorul Instituției
- Compartimentul de IT
- Utilizatori

3.3. Resurse financiare:

Conform bugetului unității școlare pentru anul în curs.

4. Modul de lucru:

4.1. Planificarea operațiunilor și acțiunilor activității:

Operațiunile și acțiunile privind activitatea procedurată se vor derula de către toate compartimentele, conform instrucțiunilor din prezenta procedură.

4.2. Derularea operațiunilor și acțiunilor activității:

Sistemele IT sprijină managementul adecvat al datelor, inclusiv administrarea bazelor de date şi asigurarea calităţii datelor. Sistemele de management al datelor şi procedurile de operare sunt în conformitate cu politica IT a entităţii, măsurile obligatorii de securitate şi regulile privind protecţia datelor personale.

Comunicarea prin e-mail a actelor administrative fiscale, actelor de executare și altor acte emise de organul fiscal local se realizează de către acesta la adresa de e-mail indicată de contribuabil.

Comunicarea se consideră realizată la data primirii unui e-mail de confirmare, de pe adresa de e-mail unde a fost transmis actul administrativ fiscal, actul de executare sau altor acte emise de organul fiscal local.

În cazul persoanelor juridice, e-mailul de confirmare trebuie să fie însoțit de semnătură electronică extinsă bazată pe un certificat calificat.

Confirmarea de primire trebuie comunicată de contribuabil în cel mult 3 zile lucrătoare de la primirea e-mailului. În cazul în care contribuabilul confirmă primirea, data comunicării este data transmiterii de către contribuabil a e-mailului de confirmare.

În cazul în care contribuabilul nu transmite e-mail-ul de confirmare a primirii în termenul prevăzut, actul administrativ fiscal, actul de executare sau alt act emis de organul fiscal local se consideră comunicat după expirarea unui termen de 15 zile calendaristice, calculat de la data comunicării e-mailului de către organul fiscal local.

În situația prevăzută organul fiscal local întocmește un proces-verbal de comunicare care se semnează cu semnătură electronică extinsă bazată pe un certificat calificat sau în format fizic, cu semnătură olografă.

Confirmarea de primire sau după caz respectiv procesul-verbal de comunicare se arhivează, electronic sau fizic, la dosarul contribuabilului.

O persoană vizată ar trebui să aibă dreptul la rectificarea datelor cu caracter personal care o privesc și „dreptul de a fi uitată”, în cazul în care păstrarea acestor date încalcă legea sau dreptul Uniunii sau dreptul intern sub incidența căruia intră operatorul. În special, persoanele vizate ar trebui să aibă dreptul ca datele lor cu caracter personal să fie șterse și să nu mai fie prelucrate, în cazul în care datele cu caracter personal nu mai sunt necesare pentru scopurile în care sunt colectate sau sunt prelucrate, în cazul în care persoanele vizate și-au retras consimțământul pentru prelucrare sau în cazul în care acestea se opun prelucrării datelor cu caracter personal care le privesc sau în cazul în care prelucrarea datelor cu caracter personal ale acestora nu este conformă cu legea.

Acest drept este relevant în special în cazul în care persoana vizată și-a dat consimțământul când era copil și nu cunoștea pe deplin riscurile pe care le implică prelucrarea, iar ulterior dorește să elimine astfel de date cu caracter personal, în special de pe internet. Persoana vizată ar trebui să aibă posibilitatea de a-și exercita acest drept în pofida faptului că nu mai este copil. Cu toate acestea, păstrarea în continuare a datelor cu caracter personal ar trebui să fie legală în cazul în care este necesară pentru exercitarea dreptului la libertatea de exprimare și de informare, pentru respectarea unei obligații legale, pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul, din motive de interes public în domeniul sănătății publice, în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice sau pentru constatarea, exercitarea sau apărarea unui drept în instanță.

În entitatea publică sunt implementate măsuri de securitate pentru protejarea documentelor împotriva distrugerii, furtului, pierderii, incendiului etc., precum şi măsuri de respectare a reglementărilor privind protecţia datelor cu caracter personal.

În vederea asigurării unui nivel ridicat de securitate, operatorii de servicii esenţiale se identifică şi se înscriu în Registrul operatorilor de servicii esenţiale.

Un serviciu este considerat esenţial dacă furnizarea lui îndeplineşte cumulativ următoarele condiţii:a) serviciul este esenţial în susţinerea unor activităţi societale şi/sau economice de cea mai mare importanţă;b) furnizarea sa depinde de o reţea sau de un sistem informatic;c) furnizarea serviciului este perturbată semnificativ în cazul producerii unui incident.

Evaluarea gradului de perturbare a furnizării serviciului esenţial se realizează în funcţie de următoarele criterii intersectoriale, fără a fi cumulative:

a) numărul de utilizatori care se bazează pe serviciul furnizat de entitatea în cauză;

b) dependenţa altor sectoare prevăzute în anexa la prezenta lege de serviciul furnizat de entitatea în cauză;

c) impactul pe care l-ar putea avea incidentele, în ceea ce priveşte intensitatea şi durata, asupra activităţilor economice şi societale sau asupra siguranţei publice;

d) cota de piaţă a entităţii în cauză;

e) distribuţia geografică în ceea ce priveşte zona care ar putea fi afectată de un incident;

f) importanţa entităţii pentru menţinerea unui nivel suficient al serviciului, ţinând cont de disponibilitatea unor mijloace alternative pentru furnizarea serviciului respectiv.

Furnizorul unui serviciu de comunicaţii electronice destinat publicului are obligaţia de a lua toate măsurile tehnice şi organizatorice adecvate în vederea garantarii securităţii serviciului. În ceea ce priveşte securitatea

reţelei, dacă este necesar, furnizorul serviciului de comunicaţii electronice va lua măsurile de securitate respective împreună cu furnizorul reţelei publice de comunicaţii electronice. Măsurile adoptate trebuie să garanteze un nivel de securitate proporţional cu riscul existent, având în vedere posibilităţile tehnice de ultima ora şi costurile implementarii acestor măsuri.

Confidenţialitatea comunicărilor transmise prin intermediul reţelelor publice de comunicaţii electronice şi a serviciilor de comunicaţii electronice destinate publicului, precum şi confidenţialitatea datelor de trafic aferente sunt garantate.

Utilizarea unei reţele de comunicaţii electronice în scopul stocării de informaţii în echipamentul terminal al unui abonat sau utilizator ori al obţinerii accesului la informaţia stocata în acest mod este permisă numai cu îndeplinirea, în mod cumulativ, a următoarelor condiţii:

a) abonatului sau utilizatorului în cauza i s-au furnizat informaţii clare şi complete, între altele cu privire la scopul în care se efectuează stocarea sau accesul la informaţia stocata;

b) abonatului sau utilizatorului în cauza i s-a oferit posibilitatea de a refuza stocarea sau accesul la informaţia stocata.

Prelucrarea datelor de localizare, altele decât datele de trafic, referitoare la utilizatorii sau abonatii reţelelor publice de comunicaţii electronice sau ai serviciilor de comunicaţii electronice destinate publicului, atunci când este posibila, este permisă numai în unul dintre următoarele cazuri:

a) datele în cauza sunt transformate în date anonime;

b) cu consimţământul expres prealabil al utilizatorului sau abonatului la care se referă datele respective, în măsura şi pentru durata necesare furnizarii unui serviciu cu valoare adăugată;

c) atunci când serviciul cu valoare adăugată cu funcţie de localizare are ca scop transmiterea unidirectionala şi nediferentiata a unor informaţii către utilizatori.

Furnizorul serviciului de comunicaţii electronice destinat publicului are obligaţia de a pune la dispoziţie utilizatorului sau abonatului, anterior obţinerii consimţământului acestuia, informaţii referitoare la:

a) tipul de date de localizare, altele decât datele de trafic, care vor fi prelucrate;

b) scopurile şi durata prelucrării acestor date;

c) eventuala transmitere a datelor către un terţ, în scopul furnizarii serviciului cu valoare adăugată.

Utilizatorii sau abonatii care îşi dau consimţământul în vederea prelucrării datelor în conformitate cu prevederile lit. b) au dreptul de a-şi retrage oricând consimţământul exprimat cu privire la prelucrarea datelor sau de a refuza temporar prelucrarea datelor în cauza pentru fiecare conectare la reţea sau pentru fiecare transmitere a unei comunicări.

Furnizorul serviciului de comunicaţii electronice destinat publicului are obligaţia de a pune la dispoziţie utilizatorilor sau abonatilor un procedeu simplu şi gratuit pentru exercitarea acestor drepturi.

Prelucrarea datelor de localizare, altele decât datele de trafic, poate fi efectuată numai de către persoanele care acţionează sub autoritatea furnizorului reţelei publice de comunicaţii electronice sau al serviciului de comunicaţii electronice destinat publicului ori a terţului furnizor de servicii cu valoare adăugată şi trebuie să se limiteze numai la ceea ce este necesar pentru furnizarea serviciului cu valoare adăugată.

4.3. Valorificarea rezultatelor activității:

Rezultatele activității vor fi valorificate de către toate comisiile și compartimentele din Instituție.

Responsabilități

Conducătorul instituției
- Aprobă procedura
- Asigură implementarea și menținerea procedurii
- Monitorizează prezenta procedură

Compartimentul IT
- Realizează activitățile descrise în prezenta procedură
- Asigură implementarea și menținerea procedurii
- Monitorizează prezenta procedură

Formular de evidenţă a modificărilor

Nr. Crt	Numărul ediţiei / reviziei	Data ediţiei / reviziei	Componenta revizuită	Descrierea modificării	Avizul conducătorului compartimentului
1	Ediția I	07.05.2018	X	X	
2	Ediția a II-a	31.10.2022	Documente de referintă; Descrierea activității sau procesului	Modificări legislative	
3	Revizia I	17.03.2023	Documente de referintă; Descrierea activității sau procesului	Modificări legislative	
4	Revizia a II-a	28.06.2023	Documente de referință	Modificări legislative	Favorabil

Formular de analiză a procedurii

Nr. Crt	Compartiment	Nume şi prenume conducător compartiment	Aviz	Data	Observaţii	Semnătura

Lista de difuzare a procedurii

Nr. ex.	Compartiment	Nume și prenume	Data primirii	Data retragerii	Data intrării în vigoare	Semnătura
1		Cîmpanu Monica	28.06.2023	28.06.2023	28.06.2023	
2	Comisie Monitorizare	Bejenaru Mihaela	28.06.2023	28.06.2023	28.06.2023	
3	Secretariat	Cucu Cristina Mihaela	28.06.2023	28.06.2023	28.06.2023	

Anexe

Nr. Crt	Denumirea anexei	Elaborator	Aproba	Numar de exemplare	Arhivare

Precizări

- Toate documentele şi dovezile pe baza cărora se realizează activitatea procedurată se află în dosarele Comisiei SCIM şi în documentele echipei manageriale.
- Analiza şi revizuirea procedurii se face anual, sau ori de câte ori apar modificări ale reglementărilor legale cu caracter general şi intern pe baza cărora se desfăşoară activitatea care face obiectul acestei proceduri.

Cuprins