Declaratia de aplicabilitate

Declaratia de aplicabilitate			
A.5. Politici de securitate a informatiei			
A.5.1 Managementul directiei pentru securitatea informatiei			
Obiectiv de control: Determinarea directiilor de management si suport pentru securitatea informatiei in conformitate cu cerintele afacerii si cu legile si regulamentele relevante.			
Controale			
A.5.1.1	Politici pentru securitatea informatiei	Documentul de politica este aprobat de management, multiplicat si comunicat tuturor angajatilor.	DECLARATIE DE POLITICA PRIVIND SECURITATEA INFORMATIILOR
A.5.1.2	Revizuirea politicii de securitate a informatiei	Politica este analizata regulat in cadrul analizelor de management si, in cazul unor modificari cu influenta, se asigura ca aceasta ramane adecvata.	DECLARATIE DE POLITICA PRIVIND SECURITATEA INFORMATIILOR
A.6. Organizarea securitatii informatiei			
A.6.1. Organizarea interna			
Obiectiv: Administrarea securitatii informatiei in cadrul organizatiei			
A.6.1.1	Angajamentul echipei de management privind securitatea informatiei	Organizatia are personal dedicat gestionarii securitatii informatiei.. Totodata, Managerul de Sisteme IT din cadrul organizatiei este membru al departamentului de securitate. In acest mod, conducerea societatii s-a asigurat de existenta unei directii clare si a unui suport temeinic pentru initiativele privind securitatea informatiilor.	PO-SMSI-A6 Organizarea securitatii informatiei

Declaratia de aplicabilitate

A 6.1.2	Separarea responsabilitatilor	Accesul la sistemele informatice, aplicatii, intranet, servere si date se face in baza responsabilitatilor pe care le are fiecare angajat. Drepturi depline de acces au doar Presedintele societatii, managerul IT si managerii securitatii IT.	PO-SMSI-A6 Organizarea securitatii informatiei
A.6.1.3	Contactul cu autoritatile	Sunt mentinute contacte adecvate cu autoritatile legale, organismele de reglementare, furnizorii de servicii informationale si operatorii de telecomunicatii.	PO-SMSI-A6 Organizarea securitatii informatiei
A.6.1.4	Contactul cu grupuri specializate de interes	Contractele incheiate cu parteneri, furnizori si clienti sunt elaborate conform politicii de securitate a informatiei, iar accesul la resursele proprii este limitat. Toate contractele de acest tip contin reguli, obligatii, responsabilitati si drepturi referitoare la confidentialitatea, integritatea si disponibilitatea datelor accesate pe parcursul desfasurarii acestora.	PO-SMSI-A6 Organizarea securitatii informatiei
A.6.1.5	Securitatea informatiei in managementul de proiect	Toate proiectele gestionate de organizatie se desfasoara sub incidenta asigurarii securitatii informatiei.	PO-SMSI-A6.1.5 Informatie disponibila in mod public
A.6.2 Dispozitive mobile si lucrul la distanta			
Obiectiv: Asigurarea securitatii lucrului la telefon si a dispozitivelor mobile			
A.6.2.1	Politica dispozitivelor mobile	Utilizarea dispozitivelor mobile precum laptopuri, tablete, telefoane smart de catre angajatii societatii nu reprezinta un risc pentru societate, accesul la datele si echipamentele considerate critice nefiind afectat.	PO-SMSI-A8.3 Manipularea mediilor de stocare
A.6.2.2	Lucrul la distanta	Lucrul la distanta se face cu respectarea tuturor politicilor si procedurilor ce tin de Sistemul de management al securitatii informatiei.	PO-SMSI-A8.3 Manipularea mediilor de stocare
A.7 Securitatea resurselor umane			

Declaratia de aplicabilitate

A.7.1 Inaintea angajarii			
Obiectiv: Sa se asigure ca angajatii, contractantii si utilizatorii terti inteleg responsabilitatile care le revin si sunt corespunzatori pentru rolurile pentru care sunt alocati precum si sa reduca riscul de furt, frauda sau folosire necorespunzatoare a sistemelor			
A.7.1.1	Verificare	La angajarea personalului permanent, subcontractorilor sau personalelor care candideaza pentru un post in cadrul societatii, li se fac verificari.	PO-SMSI-7.2.2 Constinetizare,Instruire
A.7.1.2	Cerinte si conditii de angajare	Termenii si conditii de angajare stipuleaza responsabilitatile angajatului pentru securitatea informatiei.	PO-SMSI-7.2.2 Constinetizare,Instruire
A.7.2 In timpul perioadei de angajare			
Obiectiv: Sa asigure faptul ca toti angajatii, contractantii si utilizatorii terti sunt informati si isi indeplinesc responsabilitatile privind securitatea informatiei.			
A.7.2.1	Responsabilitatile managementului	Angajatii semneaza un acord de confidentialitate ca parte a conditiilor si contractului de angajare. (Contracte individuale de confidentialitate)	PO-SMSI-7.2.2 Constinetizare,Instruire
A.7.2.2	Informarea privind securitatea informatiei, instruirea si educarea	Toti angajatii organizatiei si, acolo unde este cazul, utilizatorii din partea tertilor, primesc la intervale regulate instruirea necesara privind politicile si procedurile organizatiei.	PO-SMSI-7.2.2 Constinetizare,Instruire
A.7.2.3	Procesul disciplinar	Incalcarea de catre angajati a politicilor de securitate este supusa unui proces disciplinar oficial. (ref: “Procedura de resurse umane”)	PO-SMSI-7.2.2 Constinetizare,Instruire
A.7.3 Incetarea contractului			
Obiectiv: Protejarea intereselor societatii ca parte a procesului de schimbare a locului de munca sau incetare a contractului			

Declaratia de aplicabilitate

A.7.3.1	Responsabilitatile privind terminarea contractului sau schimbarea locului de munca	Responsabilitatile privind incetarea contractului de munca sunt stabilite prin contractele de munca si de confidentialitate. Responsabilitatile privind schimbarea locului de munca sunt in mod clar definite si alocate.	PO-SMSI-7.2.2 Constinetizare,Instruire
A.8 Managementul resurselor			
A.8.1. Responsabilitatea pentru resurse			
Obiectiv: Identificarea resurselor organizatiei si definirea responsabilitatilor pentru utilizatorii acestora			
A.8.1.1.	Inventarul resurselor	A fost stabilit si este mentinut un inventar al tuturor resurselor importante asociate fiecarui sistem de informatii. (ref: “Inventarul resurselor”)	PO-SMSI-A8.1 Managementul resurselor informationale
A.8.1.2	Detinerea resurselor	Toate informatiile si resursele asociate cu sistemele de procesare a informatiei sunt detinute de o parte desemnata de catre organizatie	PO-SMSI-A8.1 Managementul resurselor informationale
A.8.1.3	Utilizarea in mod acceptabil a resurselor	Regulile pentru utilizarea informatiilor si resurselor asociate sistemelor de procesare a informatiilor sunt identificate si documentate.	PO-SMSI-A8.1 Managementul resurselor informationale
A.8.1.4	Returnarea resurselor	Procesul de incetare a angajarii este oficializat si include returnarea activelor.Cerintele privind returnarea activelor de catre contractanti sau terti sunt stipulate in acorduri / contracte.	PO-SMSI-A8.1 Managementul resurselor informationale
A.8.2. Clasificarea informatiei			
Obiectiv: Sa asigure faptul ca informatia beneficiaza de un nivel de protectie adecvat			
A.8.2.1	Indrumari de clasificare	Clasificarea si controalele de protectie asociate informatiei iau in considerare necesitatile afacerii de a permite sau restrictiona accesul la informatie si de impactul asupra	PO-SMSI-A8.2 Clasificarea si etichetarea informatiei SMSI

Declaratia de aplicabilitate

		afacerii aociat acestor necesitati. (ref “Coordonarea informatiilor si inregistrarilor”)	
A.8.2.2	Etichetarea si informatiei	Informatia este etichetata conform schemei de clasificare adoptata de organizatie. Suportului pe care se salveaza informatia ii este aplicata o eticheta ce contine gradul de clasificare al informatiei si regulile de disponibilitate a acesteia	PO-SMSI-A8.2 Clasificarea si etichetarea informatiei SMSI
A.8.2.3	Manevrarea resurselor	Manevrarea resurselor se face in conformitate cu politicile de securitate ale societatii.	PO-SMSI-A8.2 Clasificarea si etichetarea informatiei SMSI
A.8.3 Manipularea mediilor de stocare			
Obiectiv: sa previna divulgarea neautorizata, modificarea, indepartarea sau distrugerea resurselor si intreruperea activitatilor afacerii			
A.8.3.1	Managementul mediilor de stocare amovibile	In interiorul companiei este permisa utilizarea mediilor de stocare amovibile, precum CD-uri, flash memory stick-uri, etc. Citirea sau copierea datelor de pe mediile mobile pe statiile de lucru, se efectueaza dupa scanarea mediilor cu antivirusul stanard utilizat in organizatie.	PO-SMSI-A8.3 Manipularea mediilor de stocare
A.8.3.2	Distrugerea mediilor de stocare	Suporturile de stocare sunt eliminate in siguranta atunci cand nu mai sunt necesare.	PO-SMSI-A8.3 Manipularea mediilor de stocare
A.8.3.3	Mediile fizice de stocare in tranzit	Suporturile media aflate in tranzit sunt protejate la accesul neautorizat, utilizare incorecta sau deteriorare prin intermediul politicii de securitate IT.	PO-SMSI-A8.3 Manipularea mediilor de stocare
A.9 Controlul accesului			
A.9.1 Cerintele afacerii pentru controlul accesului			
Obiectiv: Sa controleze accesul la informatie			
A.9.1.1	Politica de control al accesului	Cerintele afacerii pentru controlul accesului sunt definite si	PO-SMSI-A9 Controlul accesului

Declaratia de aplicabilitate

		documentate iar accesul este restrictionat conform.	
A.9.1.2	Accesul la retele si serviciile de retea	Utilizatorii informatiilor societatii au acces limitat la retea si serviciile de retea, in conformitate cu rolul si responsabilitatiloe lor.	PO-SMSI-A9 Controlul accesului
A.9.2 Managementul accesului utilizatorului			
Obiectiv: sa asigure accesul autorizat si sa previna accesul neautorizat la sistemele de informatii			
A.9.2.1	Inregistrarea si stergerea utilizatorului	Inregistrarea utilizatorului, alocarea si eliminarea drepturilor de acces, la fel ca si stergerea datelor utilizatorului se fac de catre Managerul de Sisteme.	PO-SMSI-A9 Controlul accesului
A.9.2.2	Acordarea accesului utilizatorilor	Acolo unde aplicatiile si serviciile de sistem utilizate in cadrul societatii nu permit automatizarea procesului de acordare a accesului pentru utilizatori, in conformitate cu rolurile si responsabilitatile acestora, acesta se face de catre managerul de sisteme sau responsabilii de securitate IT.	PO-SMSI-A9 Controlul accesului
A.9.2.3	Managementul privilegiilor	Alocarea si utilizarea privilegiilor sunt restrictionate si controlate de catre administrator prin politica de securitate.(“Politica de securitate”)	PO-SMSI-A9 Controlul accesului
A.9.2.4	Managementul secretului privind autentificarea utilizatorilor	Alocarea parolelor este controlata prin politica de securitate a parolelor (“Politica de securitate”)	PO-SMSI-A9 Controlul accesului
A.9.2.5	Revizuirea drepturilor de acces ale utilizatorului	Periodic sunt revizuite drepturile de acces de catre Managerul de Sisteme, prin functiile de management ale Domain Controllerului si din panoul de administrare a aplicatiilor.	PO-SMSI-A9 Controlul accesului
A.9.2.6	Inlaturarea sau ajustarea drepturilor de acces	Drepturile de acces pentru utilizatorii sau partile terte sunt inlaturate o data cu incheierea contractelor in vigoare sau ajustate atunci cand responsabilitatile acestora se modifica.	PO-SMSI-A9 Controlul accesului
A.9.3. Responabilitatile utilizatorului			

Declaratia de aplicabilitate

Obiectiv: Responsabilizarea utilizatorilor vizavi de securizarea informatiei accesate			
A.9.3.1	Utilizarea secretului privind autentificarea	Este reglementata prin politica de securitate a parolelor. (“Politica de securitate”)	DECLARATIE DE POLITICA PRIVIND SECURITATEA INFORMATIILOR
A.9.4 Controlul accesului la sisteme si aplicatii			
Obiectiv: sa previna accesul neautorizat la sisteme si aplicatii			
A.9.4.1	Restrictionarea accesului la informatie	Accesul la sistemele si aplicatiile societatii se face in conformitate cu rolul si responsabilitatile utilizatorilor, asa cum este descris in politica de securitate.	PO-SMSI-A9 Controlul accesului
A.9.4.2	Proceduri de autentificare sigura	Autentificarea utilizatorilor la sistemele si aplicatiile societatii se face in conformitate cu politica de securitate, majoritatea fiind bazate pe utilizator si parola.	PO-SMSI-A9 Controlul accesului
A.9.4.3	Sistemul de management al parolelor	Acolo unde aplicatiile si sistemele permit, politica utilizarii parolelor este implementata automat. In restul cazurilor, angajatii sunt obligati sa urmeze procedurile de creare si gestionare a parolelor din cadrul politicii de securitate.	PO-SMSI-A9 Controlul accesului
A.9.4.4	Utilizarea programelor utilitare de sistem cu drepturi de administrator	Programele utilitare de sistem sunt rulate numai de catre managerul de sisteme si de responsabilii de securitate IT, ca urmare a restrictiilor impuse prin Politica de securitate.	PO-SMSI-A9 Controlul accesului
A.9.4.5	Controlul accesului la codul sursa al programelor	Accesul la codul sursa al programelor este oferit exclusiv programatorilor, managerului de sisteme si responsabililor de securitate.	PO-SMSI-A9 Controlul accesului
A.10 Criptografie			
Obiectiv: sa asigure utilizarea corectă și eficientă a criptografiei pentru a proteja confidențialitatea, autenticitatea și / sau integritatea informațiilor			

Declaratia de aplicabilitate

A.10.1.1	Politica privind controlul criptografic	existenta unei proceduri pentru criptografie	Nu se aplica
A.10.1.2	Key management	politica	Nu se aplica
A.11. Securitatea fizica si a mediului de lucru			
A.11.1. Zone de securitate			
Obiectiv: sa previna accesul fizic neautorizat, distrugerile si patrunderea in interiorul organizatiei precum si accesul la informatii			
A.11.1.1.	Perimetru fizic de securitate	Organizatia utilizeaza perimetre de securitate pentru a proteja amplasamentele echipamentelor tehnice de procesare a informatiei.	PO-SMSI-A11.1 Securitatea fizica
A.11.1.2.	Controlul accesului fizic	Zonele de securitate sunt protejate prin controale de intrare adecvate, pentru a sigura numai accesul persoanelor autorizate.	PO-SMSI-A11.1 Securitatea fizica
A.11.1.3	Securizarea birourilor, incaperilor si locatiilor	Zonele de securitate sunt create pentru a proteja birouri, incaperi sau echipamente pentru care sunt definite cerinte speciale de securitate.	PO-SMSI-A11.1 Securitatea fizica
A.11.1.4.	Protejarea impotriva amenintarilor externe si de mediu	Pregatirea pentru situatii de urgenta este documentata si capacitatea de raspuns este testata periodic.(ref: “Manual SMSI ”)	PO-SMSI-A11.1 Securitatea fizica
A.11.1.5.	Desfasurarea activitatii in zone de securitate	Sunt aplicate masuri pentru protectia fizica si pentru desfasurarea activitatii in zonele de securitate	PO-SMSI-A11.1 Securitatea fizica
A.9.11.6.	Zone de acces public, punctele de livrare si incarcare	Zonele de livrare si de incarcare sunt controlate si izolate de echipamentele pentru procesarea informatiilor pentru a se evita accesul neautorizat.	PO-SMSI-A11.1 Securitatea fizica
A.11.2. Echipamente			
Obiectiv: Prevenirea pierderii, avarierii, furtului sau compromiterii resurselor si a intreruperii operatiunilor societatii			

Declaratia de aplicabilitate

A.11.2.1	Amplasarea si protejarea echipamentelor	Echipamentele sunt amplasate si protejate astfel incat sa se reduca riscul la amenintari din mediul inconjurator si posibilitatea accesului neautorizat.	PO-SMSI-A11.2 Securitatea echipamentelor
A.11.2.2	Utilitatile suport	Echipamentele sunt protejate impotriva caderilor de tensiune sau a altor anomalii electrice prin conectarea lor la surse de curent neintrerupt – UPS si prin amplasarea unui Generator electric drept sursa alternativa de curent, in cazul penelor prelungite de curent. (ref: “Manual SMSI”)	PO-SMSI-A11.2 Securitatea echipamentelor
A.11.2.3	Securitatea retelelor de cablu	Cablurile de energie si pentru telecomunicatii care transmit date sau sustin servicii informatice sunt protejate impotriva interceptarilor sau a daunelor. (ref: “Manual SMSI”).	PO-SMSI-A11.2 Securitatea echipamentelor
A.11.2.4	Intretinerea echipamentelor	Echipamentele sunt intretinute corespunzator astfel incat sa poata fi asigurata permanent disponibilitatea si integritatea lor.	PO-SMSI-A11.2 Securitatea echipamentelor
A.11.2.5	Scoaterea bunurilor	Pentru scoaterea bunurilor in afara spatiului de lucru, se completeaza cererea mentionata la pct. A.11.2.6	PO-SMSI-A11.2 Securitatea echipamentelor
A.11.2.6	Securitatea echipamentului in afara locatiei	Scoaterea echipamentelor in afara locatiei presupune completarea unei cereri prin care se detaliaza justificarea actiunii, cerere care trebuie inmanata supervizorului. Masura a fost adoptata pentru gestionarea eficienta a echipamentelor societatii si pentru responsabilizarea persoanelor care imprumuta aceste echipamente. (ref: “Manual SMSI”).	PO-SMSI-A11.2 Securitatea echipamentelor
A.11.2.7	Scoaterea din uz sau reutilizarea in conditii de siguranta	Inainte de casarea sau refolosirea echipamentelor, informatia este stearsa de pe acestea.	PO-SMSI-A11.2 Securitatea echipamentelor
A.11.2.8	Echipament nesupravegheat	Este responsabilitatea utilizatorilor sa asigure securitatea echipamentelor nesupravegheate.	PO-SMSI-A11.2 Securitatea echipamentelor

Declaratia de aplicabilitate

A.11.2.9	Politica biroului curat si a ecranului protejat	Organizatia are o politica de birou curat si de protejare cu parola a sistemului pe durata pauzelor pentru reducerea riscului accesului neautorizat, pierderii si deteriorarii informatiei. (“Politica de securitate”)	PO-SMSI-A11.2 Securitatea echipamentelor
A.12 Securitatea operationala			
A.12.1. Proceduri operationale si responsabilitati			
Obiectvi: Sa asigure operarea corecta si in conditii de securitate a sistemelor de procesare a informatiei			
A.12.1.1	Proceduri de operare documentate	Procedurile operationale identificate in politica de securitate sunt documentate si mentinute.	PO-SMSI-A12.1.1 Procesarea corecta a datelor in cadrul aplicatiilor
A.12.1.2	Managementul schimbarilor	Orice modificari ale echipamentelor si sistemelor de procesare a informatiei se fac controlat. (“Manual SMSI”)	PO-SMSI-A12.1 Proceduri operationale si responsabilitati
A.12.1.3	Managementul capacitatilor	In cadrul societatii este monitorizat accesul resurselor astfel incat sa poata fi facute estimari corecte cu privire la necesarul echipamentelor si resurselor pentru asigurarea performantelor sistemelor.	PO-SMSI-A12.1 Proceduri operationale si responsabilitati
A.12.1.4	Separarea sistemelor de dezvoltare, testare si a sistemelor oprationale	Exista sisteme de test utilizate pentru testarea aplicatiilor si a programelor inainte ca acestea sa fie implementate in sistemele de productie. De asemenea, exista sisteme de test virtualizate, utilizate in cadrul diverselor proiecte ale societatii.	PO-SMSI-A12.1 Proceduri operationale si responsabilitati
A.12.2 Protectia impotriva malware			
Obiectiv: sa asigure protejarea informatiei si a sistemelor de procesare a informatiei impotriva malware-ului			
A.12.2.1	Masuri de securitate impotriva malware-ului	Impotriva amenintarilor de tip malware, organizatia utilizeaza antivirusul standard, updatat periodic	PO-SMSI-A12.2 Protectia impotriva codurilor mobile si daunatoare

Declaratia de aplicabilitate

		cu semnaturile ultimilor virusi si worms si malware	
A.12.3 Backup			
Obiectiv: Protejarea impotriva pierderilor de date			
A.12.3.1	Back-upul informatiei	Se realizeaza in mod regulat copii de siguranta pentru informatia esentiala afacerii si pentru software.	PO-SMSI-A12.3 Copie de siguranta
A.12.4 Logarea si monitorizarea			
Obiectiv: Inregistrarea evenimentelor si generarea de jurnale de audit			
A.12.4.1	Jurnal de audit	Jurnalul de audit inregistreaza exceptiile si alte evenimente de securitate relevante si este pastrat pe perioada agreata in scopul oferirii de asistenta in investigatiile viitoare si in monitorizarea controlului accesului. (ref: „Manual SMSI”)	PO-SMSI-A12.4 Securitatea fisierelor de sistem
A.12.4.2	Protectia informatiilor din jurnale	Sistemele de inregistrare si jurnalele de informatii sunt protejate impotriva modificarilor si accesului neautorizat prin stabilirea accesului la acestea numai a administratorului de sistem.	PO-SMSI-A12.4 Securitatea fisierelor de sistem
A.12.4.3	Jurnalul activitatilor administratorului si operatorului	Personalul operational mentine jurnale ale activitatilor desfasurate. Acestea sunt subiect al verificarilor periodice efectuate de personal independent.	PO-SMSI-A12.4 Securitatea fisierelor de sistem
A.12.4.4	Sincronizarea ceasului	Pentru ca inregistrarile accesarii sistemelor si a fisierelor sa fie eficiente, este esential ca ceasurile tuturor sistemelor sa fie sincronizate, din motive de securitate. Investigarea unui eventual incident de securitate, care presupune analizarea inregistrarilor evenimentelor, ar fi compromisa daca orele sistemelor ar fi nesincronizate. Totodata, sincronizarea ceasurilor este foarte	PO-SMSI-A12.4.4 Monitorizare

Declaratia de aplicabilitate

		importanta si pentru crearea copiilor de back-up, care trebuie sa poarte data si ora exacta a crearii lor.	
A.12.5 Controlul softwareului operational			
Obiectiv: Asigurarea integritatii sistemelor operationale			
A.12.5.1	Instalarea softwareului pe sistemele operationale	Instalarea softwareului pe sistemele operationale se efectueaza in conformitate cu politica de securitate si cu nevoile utilizatorilor.	
A.12.6 Managementul vulnerabilitatilor tehnice			
Obiectiv: Prevenirea exploatarii vulnerabilitatilor tehnice			
A.12.6.1	Managementul vulnerabilitatilor tehnice	In cadrul organizatiei sunt identificate si evaluate vulnerabilitatile tehnice si sunt implementate masuri adecvate pentru reducerea riscului asociat acestor vulnerabilitati.	
A.12.6.2	Restrictii asupra instalarilor de software	Exista reguli care ingradesc accesul utilizatorilor la instalari neautorizate de sfotware.	
A.12.7 Consideratie fata de auditarea sistemelor informationale			
Obiectiv: Minimizarea impactului activitatilor de audit asupra sistemelor operationale			
A.12.7.1	Controale pentru auditarea sistemelor informationale	Auditarea sistemelor informationale se efectueaza tinand cont de necesitatea continuitatii proceselor de afaceri.	
A.13 Managementul securitatii retelei			

Declaratia de aplicabilitate

Obiectiv: Sa asigure protectia retelelor de informatii si protectia infrastructurii de suport			
A.13.1.1	Masuri de securitate a retelelor	Este implementata o gama de controale pentru realizarea si mentinerea securitatii in retelele de calculatoare.	PO-SMSI-A13 Managementul securitatii retelei
A.13.1.2	Securitatea serviciilor de retea	Serviciile de retea accesibile in cadrul organizatiei sunt: DHCP, DNS, Web service, E-mail, BGP, VPN, Firewall, etc. Accesul catre aceste servicii se face prin autentificare, utilizand nume de utilizator si parola. Verificarea jurnalelor de audit (logurilor) se face zilnic.	PO-SMSI-A13 Managementul securitatii retelei
A.13.1.3	Separarea in retele	In cadrul societatii exista mai multe retele, delimitate la nivel fizic si logic, astfel incat accesarea resurselor existente sa poata fi permisa numai utilizatorilor autorizati. Serverele de productie, cele de dezvoltare si echipamentele de backup se afla in locatii si retele diferite fata de reteaua folosita de utilizatorii societatii.	PO-SMSI-A13 Managementul securitatii retelei
A.13.2 Schimbul de informatii			
Obiectiv: Sa mentina securitatea schimbului de informatie in interiorul unei organizatii sau cu orice entitate externa			
A.13.2.1	Proceduri si politici pentru schimbul de informatii	Sunt aplicate politici care definesc modul in care informatiile trebuie protejate in momentul schimbului de informatii, de la expeditor la destinatar.	PO-SMSI-A13 Managementul securitatii retelei
A.13.2.2	Acorduri de schimb	Tertii care intra in posesia informatiilor ca urmare a schimului de informatii, trebuie sa se conformeze politicilor si directivelor care vizeaza securitatea informatiei in cadrul societatii.	PO-SMSI-A13 Managementul securitatii retelei

Declaratia de aplicabilitate

A.13.2.3	Mesageria electronica	Utilizarea mesageriei electronice in cadrul organizatiei se face prin intermediul sistemelor de mail interne, administrate si mentinute de Managerul de Sisteme. Accesarea acestor sisteme se face in mod controlat.	PO-SMSI-A13 Managementul securitatii retelei
A.13.2.4	Acorduri privind confidentialitatea sau nedivulgarea	Obligatiile privitoarea la pastrarea confidentialitatii informatiilor accesate si la nedivulgarea acestora catre persoane neautorizate sunt specificate in toate tipurile de documente oficiale (ex:contracte) si in politicile interne referitoare la securitatea informatiei.	PO-SMSI-A13 Managementul securitatii retelei
A.14 Achizitionarea, dezvoltarea si mentenanta sistemelor informatice			
A.14.1. Cerinte de securitate pentru sistemele informationale			
Obiectiv: sa asigure faptul ca securitatea este parte integranta a sistemelor informatice			
A.14.1.1	Analiza si specificarea cerintelor de securitate	Cerintele pentru noile sisteme informatice si pentru imbunatatirea celor existente sunt analizate de catre Comisia de securitate.	PO-SMSI-A14.1 Planificarea si acceptanta sistemului
A.14.1.2	Securizarea serviciilor aplicatiilor in retelele publice	Informatiile accesate de catre utilizatorii anonimi sunt catalogate drept informatii publice, fara risc. Informatiile care trebuie protejate de accesul neautorizat sunt accesibile utilizatorilor legitimi numari prin folosirea mijloacelor de autentificare specifice, insemnand minim nume utilizator si parola (conform politicii de alcatuire a parolelor).	PO-SMSI-A14.1 Planificarea si acceptanta sistemului
A.14.1.3	Protejarea serviciilor aplicatiilor in tranzit	In cazul informatiilor transmise dinspre colaboratori/clienti catre societate si invers, in cadrul proceselor de afaceri gestionate de sisteme informationale complexe, exista masuri specifice implementate care sa asigure integritatea,	PO-SMSI-A14.1 Planificarea si acceptanta sistemului

Declaratia de aplicabilitate

		disponibilitatea si confidentialitatea informatiei.	
A.14.2 Securitatea in procesele de dezvoltare si de suport			
Obiectiv: Asigurarea elaborarii si implementarii securitatii informatiei in cadrul dezvoltarii ciclului de viata al sistemelor informationale			
A.14.2.1	Politica privind securitatea dezvoltarii	Exista reguli si politici privind securitatea dezvoltarii softwareului in cadrul societatii.	PO-SMSI-A14.1 Planificarea si acceptanta sistemului
A.14.2.2	Proceduri de control al verificarilor	Modificarile aduse software-ului operational din cadrul organizatiei vor fi efectuate conform procedurilor aplicabile	PO-SMSI-A14.1 Planificarea si acceptanta sistemului
A.14.2.3	Revizuirea tehnica a aplicatiilor dupa modificarile asupra pachetelor software	Dupa efectuare modificarilor aduse software-ului operational, se vor efectua teste corespunzatoare, inainte de implementarea modificarilor in mediul operational. (ref: „Politica de securitate”)	PO-SMSI-A14.1 Planificarea si acceptanta sistemului
A.14.2.4	Restrictii privind modificarile asupra pachetelor software	Modificarile asupra pachetelor software pot fi efectuate numai de personalul autorizat (dezvoltatori). Masurile de prevenire a modificarilor neautorizate sunt implementate prin acordarea drepturilor de accesare a sistemelor de dezvoltare, personalului dedicat.	PO-SMSI-A14.1 Planificarea si acceptanta sistemului
A.14.2.5	Principii privind securizarea construirii sistemelor	Construirea sistemelor utilizate se face in conformitate cu politicile si procedurile de securitate dezvoltate si implementate in cadrul societatii.	PO-SMSI-A14.1 Planificarea si acceptanta sistemului
A.14.2.5	Scurgerea de informatii	Personalul societatii si partenerii insarcinati cu dezvoltarea software si administrarea securitatii IT sunt informati cu privire la clasificarea informatiilor in cadrul organizatiei si au fost instruiti pentru aplicarea masurilor de securitate necesare pentru protejarea datelor. Totodata,	PO-SMSI-A14.1 Planificarea si acceptanta sistemului

Declaratia de aplicabilitate

		in contractele de munca, respectiv contractele de colaborare, sunt specificate cerinte de confidentialitate.	
A.14.2.6	Securitatea mediului de dezvoltare	Mediul de dezvoltare utilizat in cadrul societatii este construit si utilizat in conformitate cu regulile si politicile de securitate menite sa acopere toate etapele ciclului de dezvoltare.	PO-SMSI-A14.1 Planificarea si acceptanta sistemului
A.14.2.7	Externalizarea dezvoltarii de software	Procesul de dezvoltare software pentru organizatie de catre parteneri externi este controlat.	PO-SMSI-A14.1 Planificarea si acceptanta sistemului
A.14.2.8	Testarea securitatii sistemelor	Functionarea masurilor de securitate implementate intr-un sistem dezvoltat este testata in timpul procesului de dezvoltare.	PO-SMSI-A14.1 Planificarea si acceptanta sistemului
A.14.2.9	Testarea acceptantei sistemelor	Upgrade-ul sistemelor, instalarea sistemelor noi sau a versiunilor de sisteme noi se face conform criteriilor de securitate elaborate in politicile de securitate.	PO-SMSI-A14.1 Planificarea si acceptanta sistemului
A.15 Relatiile cu furnizorii			
A.15.1 Securitatea informatiei in relatia cu furnizorii			
Obiectiv: Asigurarea protectiei resurselor organizatiei accesate de furnizori			
A.15.1.1	Politica securitatii infromatiei in relatiile cu furnizorii	Furnizorii care prin natura serviciilor sau produselor livrate trebuie sa acceseze resursele informationale ale societatii se supun politicilor de securitate privind asigurarea confidentialitatii, integritatii, disponibilitatii si nedivulgarii informatiei pe care o acceseaza.	PO-SMSI-A15.1 Managementul serviciilor furnizate de terti
A.15.1.2.	Gestionarea securitatii in cadrul intelegerilor contractuale cu furnizorii	Masurile de securitate, definitiile serviciilor si parametrii de furnizare incluse in contracte sau acorduri de furnizare sunt implementate, operate	PO-SMSI-A15.1 Managementul serviciilor furnizate de terti

Declaratia de aplicabilitate

		si intretinute corepunzator de catre partea terta.	
A.15.1.3	Lantul de aprovizionare al tehnologiilor de comunicatii si informationale	Relatiile contractuale cu furnizorii includ preocuparea vizavi de riscurile securitatii informatiei asociate serviciilor de comunicatii si informationale si lantului de aprovizionare cu produse tehnologice.	PO-SMSI-A15.1 Managementul serviciilor furnizate de terti
A.15.2 Managementul livrarii serviciilor furnizorilor			
Obiectiv: Mentinerea unui nivel agreat al securitatii informatiei si livrarea serviciilor in conformitate cu intelegerile contractuale existente			
A.15.2.1	Monitorizarea si evaluarea serviciilor tertilor	Serviciile furnizate de terti sunt evaluate periodic.	PO-SMSI-A15.1 Managementul serviciilor furnizate de terti
A.15.2.2	Managementul modificarilor in cazul serviciilor tertilor	Modificarile privind furnizarea serviciilor se fac in mod controlat tinand cont de criticitatea sistemelor si sunt controlate prin prevederi contractuale.	PO-SMSI-A15.1 Managementul serviciilor furnizate de terti
A.16 Managementul incidentelor de securitate a informatiei			
A.16.1 Managementul incidenteleor de securitate a informatiei si imbunatatiri			
Obiectiv: Sa asigure faptul ca pentru managementul incidentelor de securitate a informatiei este aplicata o abordare consistenta si eficienta.			
A.16.1.1	Responsabilitati si proceduri	Sunt stabilite responsabilitati si proceduri de gestionare a incidentelor pentru a se asigura un raspuns rapid, efectiv si sistematizat incidentelor de securitate si pentru a colecta datele referitoare la incident, cum ar fi constatarile auditului si jurnale.	PO-SMSI-A16 Managementul incidentelor SMSI

Declaratia de aplicabilitate

A.16.1.2	Raportarea evenimentelor de securitate a informatiei	Incidentele de securitate sunt raportate prin canalele de management adecvate cat mai repede posibil.	PO-SMSI-A16 Managementul incidentelor SMSI
A.16.1.3	Raportarea slabiciunilor de securitate	Se cere utilizatorilor serviciilor informatice sa noteze si sa raporteze orice slabiciune observata sau suspectata a securitatii sistemelor sau serviciilor. (ref: „Manual SMSI")	PO-SMSI-A16 Managementul incidentelor SMSI
A.16.1.4	Evaluarea si deciziile privind evenimentele ce vizeaza securitatea informatiei	Evenimentele care vizeaza securitatea informatiei sunt evaluate si catalogate ca atare.	PO-SMSI-A16 Managementul incidentelor SMSI
A.16.1.5	Actionarea in cazul incidentelor de securitate	In functie de tipul de incident de securitate intalnit, se va actiona conform procedurilor si politicilor existente.	PO-SMSI-A16 Managementul incidentelor SMSI
A.16.1..6	Invatarea din incidentele de securitate a informatiei	Sunt utilizate mecanisme care sa cuantifice si sa monitorizeze tipul, gravitatea si costurile incidentelor si erorilor de functionare. (ref: "Manual SMSI")	PO-SMSI-A16 Managementul incidentelor SMSI
A.16.1.7	Colectarea probelor	Atunci cand este necesara actionarea in instanta, civila sau penala, a unei persoane sau organizatii, dovezile prezentate trebuie sa se conformeze regulilor de efectuare a probei sau regulilor specifice instantei careia i se expune cazul. Aceasta include respectarea oricarui standard sau cod de practica pentru colectarea dovezilor admisibile in instanta.	PO-SMSI-A16 Managementul incidentelor SMSI
A.17 Aspecte de securitate a informatiei a managementului continuitatii afacerii			
A.17.1. Continuitatea securitatii informatiei			
Obiectiv: Continuitatea securitatii informatiei va fi inclusa in sistemele de continuitate a afacerii ale organizatiei.			
A.17.1.1	Planificarea securitatii informatiei	Pentru dezvoltarea si mentinerea continuitatii afacerii organizatiei este desfasurat un proces de management. (PCA)	PO-SMSI-A17 Managementul continuitatii afacerii

Declaratia de aplicabilitate

A.17.12	Implementarea continuitatii securitatii informatiei	Pentru dezvoltarea si mentinerea continuitatii securitatii informatiei este desfasurat un proces de management. (PCA)	PO-SMSI-A17 Managementul continuitatii afacerii
A.17.1.3	Verificarea, revizuirea si evaluarea continuitatii securitatii informatiei	Sunt asigurate masurile necesare pentru verificarea validitatii si eficientei controalelor imeplementate menite sa asigure continuitatea securitatii informatiei.	PO-SMSI-A17 Managementul continuitatii afacerii
A.17.2 Redundanta			
Obiectiv: asigurarea disponibilitatii facilitatilor de procesare a informatiei			
A.17.2.1	Disponibilitatea facilitatilor de procesare a informatiei	Facilitatile de procesare a informatiei sunt implementate astfel incat criteriile de disponibilitate ale societatii sa fie intrunite.	PO-SMSI-A17 Managementul continuitatii afacerii
A.18 Conformitatea			
A.18.1 Conformitatea cu cerintele legale si obligatiile contractuale			
Obiectiv: Sa evite incalcarea oricarei legi, obligatii statuare, de reglementare sau contractuale sau a oricarei cerinte de securitate.			
A.18.1.1	Identificarea legislatiei aplicabile si a cerintelor contractuale	Toate cerintele relevante statutare, de reglementare sau contractuale sunt explicit definite si sunt documentate pentru fiecare sistem informatic si pentru organizatie in ansamblu	PO-SMSI-A18 Conformitatea cu cerintele legale
A.18.1.2.	Drepturile de proprietate intelectuala	Sunt implementate proceduri corespunzatoare pentru a asigura conformitatea cu cerintele legislative, de reglementare si contractuale cu privire la utilizarea materialelor pentru care pot exista drepturi de proprietate intelectuala si cu privire la utilizarea produselor software proprietate.	PO-SMSI-A18 Conformitatea cu cerintele legale

Declaratia de aplicabilitate

A.18.1.3	Protejarea inregistrarilor din cadrul organizatiei	Inregistrarile sunt protejate imptoriva pierderii, distrugerii si falsificarii acestora in conformitate cu cerintele statutare, de reglementare, contractuale si de afaceri (ref: “Politica de securitate”)	PO-SMSI-A18 Conformitatea cu cerintele legale
A.18.1.4	Protectia datelor cu caracter personal si confidentialitatea informatiilor personale	Protectia datelor cu caracter personal si confidentialitatea acestora este asigurata asa cum este specificat in legislatia, regulamentele aplicabile si, acolo unde este cazul, in clauzele contractuale.	PO-SMSI-A18 Conformitatea cu cerintele legale
A.18.1.6	Reglementari privind masurile criptografice	Excludere! Organizatia nu utilizeaza masuri criptografice.	PO-SMSI-A18 Conformitatea cu cerintele legale
A.18.2 Revizuirea securitatii informatiei			
Obiectiv: Sa asigure conformitatea securitatii informatiei cu standardele si politicile de securitate organizationale.			
A.18.2.1	Revizuirea independenta a securitatii informatiei	Securitatea informatiei este revizuita de catre terti de fiecare data cand au loc schimbari majore in cadrul sistemelor societatii.	
A.18.2.2	Conformitatea cu standardele si politicile de securitate	Managerii intreprind actiuni care sa asigure ca in zona lor de responsabilitate sunt corect aplicate toate procedurile de securitate si ca toate zonele din cadrul organizatiei sunt periodic analizate pentru a se asigura conformitatea cu politicile si standardele de securitate. (ref: “Politica de securitate”)	
A.18.2.3	Verificarea conformitatii tehnice	Sistemele informatice sunt periodic analizate pentru conformitatea cu politicile si standardele de securitate.	