REGIA AUTONOMA ADMINISTRATIA FLUVIALA A DUNARII DE JOS Galati

Declarație de aplicabilitate SoA AFDJ rev.0/2026

Controale de securitate a informatiilor					
Cerinta standard		**Aplicabil DA/NU**	**Justificare**	**Implementare**	**Statut implementare**
5	**Politica de securitate**				
5.1	Politici de securitate a informatiilor	**DA**	*Stabileste directia si demonstreazä angajamentul managementului de la cel mai inalt nivel pentru securitatea informatiilor*	*Politica de utilizare a Echipamentelor IT si a Internetului* -elaborata si aprobata de conducere -comunicata personalului regiei pentru instruire -publicata pe intranet. -revizuita in cazul in care apar modificari	*Implementat*
5.2	Roluri si responsabilitati in materie de securitate a informatiilor	**DA**	Este necesar sa fie definite responsabilitati pentru securitatea informatiilor protejarea resurselor individuale si pentru indeplinirea unor procese de Securitate specifice	-Proceduri documentate: *-PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice* *-PS 7.5.3-6 Activitatea de administrare a retelei de calculatoare* -Politica de utilizare a Echipamentelor IT si a Internetului -Decizii interne	*Implementat*
5.3	Segregarea-separarea atributiilor	**DA**	Sarcinile si domeniile de responsabilitate aflate in conflict trebuie separate pentru a reduce posibilitatea modificarilor neautorizate sau neintentionate sau utilizarea gresita a resurselor	-Fisa de post -Decizii	*Implementat*

5.4	Responsabilitatile conducerii	**DA**	Managementul are responsabilitatea de a se asigura ca intregul personal (angajati si contractori) cunosc, inteleg si aplica reglementarile privind securitatea informatiei in activitate, oferind resursele necesare, instruirea adecvata si canalele de raportare confidentiale	-*Politica de utilizare a Echipamentelor IT si a Internetului* aprobata de conducere si disponibila tuturor angajatilor -Proceduri specifice aprobate si disponibile angajatilor -Instruiri specifice	*Implementat*
5.5	Contactul cu autoritatile	**DA**	Pentru a indeplini reglemenatarile legale dar si pentru a solicita asistenta sau pentru informare trebuie mentinute contacte corespunzatoare cu autoritatile in functie de situatie: autoritati in domeniul legislativ, institutii cu atributii de protectie si paza, organizatia care elaboreaza regulamente si standarde	-Fiecare structura tine legatura cu autoritatile competente in domeniul specific de activitate (ex: DNSC-Directoratul National de Securitate Cibernetica, IPJ Galati pentru paza, ANCOM etc.)	*Implementat*
5.6	Contactul cu grupuri de interese speciale	**DA**	Pentru a fi mereu informat trebuie mentinute contacte corespunzatoare cu specialisti in securitatea informatiilor	Directoratul National de Securitate Cibernetica (DNSC)	*Implementat*
5.7	Informatii despre amenintari	**DA**	Informatiile legate de amenintarile la adresa securitatii informatiilor trebuie colectate si analizate pentru a genera informatii despre amenintari	Feed DNSC: https://www.dnsc.ro/feed Alerte de la solutiile de securitate (ex: Bitdefender)	*Implementat*

5.8	Securitatea informatiilor in managementul de proiect	**DA**	Securitatea informatiilor trebuie luata in considerare in managementul proiectelor, indiferent de tipul proiectului. Este necesar un acord de confidentialitate care sa reflecte necesitatile de protectie a informatiilor la nivelul personalului	Declaratii de confidentialitate aferente proiectelor, semnate de membrii echipei de proiect si partenerii externi	*Implementat*
5.9	Inventarul informatiilor si al altor active asociate	**DA**	Exista un inventar al informatiilor si al altor active asociate, inclusiv al proprietarilor	-Evidenta inventarului software si hardware -Inventar MF (patrimoniu/contabilitate) -Log-uri de sistem	*Implementat*
5.10	Utilizarea acceptabila a informatiilor si a altor active asociate	**DA**	Normele privind utilizarea acceptabila si procedurile de gestionare a informatiilor si a altor active asociate vor fi identificate, documentate si puse in aplicare	Politica de utilizare a Echipamentelor IT si a Internetului	*Implementat*
5.11	Returnarea activelor	**DA**	Personalul si alte parti interesate, dupa caz, returneaza toate activele organizatiei aflate in posesia lor la schimbarea sau incetarea contractului de munca, a contractului sau a acordului	Fisa de lichidare	*Implementat*
5.12	Clasificarea informatiilor	**DA**	Informatiile sunt clasificate in functie de nevoile de securitate a informatiilor ale organizatiei pe baza confidentialitatii, integritatii, disponibilitatii si cerintelor relevante ale partilor in cauza	Proceduri documentate privind: *- PS 7.5.2-1 Managementu documentelor* *- PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice* -decizii interne -fise de post. Informatiile sunt clasificate in functie de nevoile de securitate a informatiilor pe baza confidentialitatii, integritatii, disponibilitatii si cerintelor relevante ale	*Implementat*

				partilor in cauza, cu acces limitat, functie de situatie(postare site, postare/modificare intranet Q, partitie structura)	
5.13	Etichetarea informatiilor	**DA**	Informatiile sunt clasificate in functie de nevoile de securitate a informatiilor ale organizatiei pe baza confidentialitatii, integritatii, disponibilitatii si cerintelor relevante ale partilor in cauza	- *PS 7.5.2-1 Managementul documentelor* – document ce reglementeaza informatiile clasificate -Decizia interna care reglementeaza informatiile clasificate	*Implementat*
5.14	Transferul de informatii	**DA**	Normele, procedurile sau acordurile de transfer de informatii ar trebui sa fie in vigoare pentru toate tipurile de facilitati de transfer din cadrul organizatiei precum si intre organizatie si alte parti	Administratia are implementate proceduri privind circuitul informatiilor in interiorul si in/din exterior: *-PS 7.5.2-1 Managementul documentelor,* *-PS 7.5-12 Implementare standard 12 Informare si comunicare*	*Implementat*
5.15	Controlul accesului	**DA**	Regulile de control al accesului fizic si logic la informatii si la alte active asociate vor fi stabilite si puse in aplicare pe baza cerintelor de securitate a informatiilor si a afacerii.	Protectie la accesul fizic prin cheie, gratii, etc. Protectie la accesul logic prin separarea drepturilor de acces la informatii	*Implementat*
5.16	Managementul identitatii	**DA**	Intregul ciclu de viata al identitatilor va fi gestionat	PS 7.5.3-6 Activitatea de administrare a retelei de calculatoare Windows Server prin Active Directory	*Implementat*
5.17	Informatii de autentificare	**DA**	Atribuirea si gestionarea informatiilor de autentificare sunt controlate de un proces de gestionare, inclusiv consilierea personalului cu privire la gestionarea corespunzatoare a informatiilor de autentificare	-Politica de utilizare a Echipamentelor IT si a Internetului -PS 7.5.3-6 Activitatea de administrare a retelei de calculatoare -Instruire personal IT pe probleme de Securitate (proceduri interne si Politica	*Implementat*

				de utilizare a Echipamentelor IT si a Internetului) Windows Server prin Active Directory	
5.18	Drepturi de acces	**DA**	Drepturile de acces la informatii si la alte active asociate trebuie sa fie furnizate, revizuite, modificate si sterse in conformitate cu politica si regulile specifice organizatiei de control al accesului	-Politica de utilizare a Echipamentelor IT si a Internetului -PS 7.5.3-6 Activitatea de administrare a retelei de calculatoare	*Implementat*
5.19	Securitatea informatiilor in relatiile cu furnizorii	**DA**	Procesele si procedurile trebuie definite si implementate pentru a gestiona riscurile de securitate a informatiilor asociate cu utilizarea produselor sau serviciilor furnizorului	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice	*Implementat*
5.20	Adresati-va securitatii informatiilor in acordurile cu furnizorii	**DA**	Cerintele relevante de securitate a informatiilor se stabilesc si se convin cu fiecare furnizor in functie de tipul relatiei cu furnizorul	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice	*Implementat*
5.21	Managementul securitatii informatii in cadrul lantului de aprovizionare cu tehnologia informatiei si comunicatiilor (TIC)	**DA**	Ar trebui definite si puse in aplicare procese si proceduri pentru a gestiona riscurile la adresa securitatii informatiilor asociate lantului de aprovizionare cu produse si servicii TIC	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice	*Implementat*
5.22	Monitorizarea, revizuirea si gestionarea schimbarii serviciilor furnizorilor	**DA**	Organizatia monitorizeaza periodic, revizuieste, evalueaza si gestioneaza modificarile practicilor de securitate a informatiilor ale furnizorului si ale furnizarii serviciilor	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice	*Implementat*
5.23	Securitatea informatiilor pentru utilizarea serviciilor cloud	**DA**	Procesele de achizitie, utilizare, gestionare si iesire a serviciilor cloud trebuie sa fie stabilite in conformitate cu cerintele de securitate a informatiilor ale organizatiei	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice	*Implementat*

5.24	Planificarea si pregatirea managementului incidentelor de securitate a informatiilor	**DA**	Organizatia trebuie sa planifice si sa se pregateasca pentru gestionarea incidentelor de securitate a informatiilor prin definirea, stabilirea si comunicarea proceselor, rolurilor si responsabilitatilor de gestionare a incidentelor de securitate a informatiilor	-Planul de continuitate a activitatii in domeniul securitatii retelelor si sistemelor informatice -Planul de recuperare in caz de dezastru in domeniul securitatii retelelor si sistemelor informatice	*Implementat*
5.25	Evaluarea si decizia privind **evenimentele de control** Securitatea informatiilor	**DA**	Organizatia trebuie sa evalueze evenimentele de securitate a informatiilor si sa decida daca acestea vor fi clasificate ca incidente de securitate a informatiilor	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice -Criptarea datelor de pe serverele regiei prin acces neautorizat (**PRORIS),** -Exfiltrarea neautorizata de informatii din reteaua regiei	*Implementat*
5.26	Raspunsul la incidentele de securitate a informatiilor	**DA**	La incidentele de securitate a informatiilor trebuie raspuns in conformitate cu procedurile documentate	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice	*Implementat*
5.27	Aflati din incidentele de securitate a informatiilor	**DA**	Cunostintele dobandite in urma incidentelor de securitate a informatiilor vor fi utilizate pentru a consolida si imbunatati controalele de securitate a informatiilor	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice - ***PRORAI*** Analiza post-incident	*Implementat*
5.28	Colectarea probelor	**DA**	Organizatia stabileste si pune in aplicare proceduri pentru identificarea, colectarea, dobandirea si pastrarea dovezilor legate de evenimentele de securitate a informatiilor	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice	*Implementat*
5.29	Securitatea informatiilor in timpul intreruperii	**DA**	Organizatia trebuie sa planifice cum sa mentina securitatea informatiilor la un nivel corespunzator in timpul intreruperii	Planul de continuitate a activitatii in domeniul securitatii retelelor si sistemelor informatice	*Implementat*
5.30	Disponibilitatea TIC pentru continuitatea afacerii	**DA**	Pregatirea in domeniul TIC trebuie planificata, pusa in aplicare, mentinuta si testata pe baza obiectivelor de continuitate a activitatii si a cerintelor de continuitate TIC	Planul de continuitate a activitatii in domeniul securitatii retelelor si sistemelor informatice	*Implementat*

5.31	Cerinte legale, statutare, de reglementare si contractuale	**DA**	Cerintele legale, statutare, de reglementare si contractuale relevante pentru securitatea informatiilor si abordarea organizatiei in ceea ce priveste indeplinirea acestor cerinte trebuie identificate, documentate si actualizate	Proceduri documentate revizuite in corelare cu actualizarea cerintelor legale: • Ordonanța de urgență a Guvernului nr. 155 din 30 decembrie 2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil; • Legea nr. 124 din 7 iulie 2025 pentru aprobarea Ordonanței de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil; • Lege nr.362*) din 28 decembrie 2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice - cu modificările și completările ulterioare; • Directiva NIS (Directiva (UE) 2016/1148); • Norme tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențial; • Legea nr.8/1996 privind drepturile de autor și drepturile conexe, republicată; • Norme tehnice de instalare a sistemelor de alarma si paza contractuale: SLA, acorduri de confidentialitate	*Implementat*
5.32	Drepturi de proprietate intelectuala	**NU**	Organizatia trebuie sa puna in aplicare obligatii/clauze adecvate pentru a proteja drepturile de proprietate intelectuala	Regia nu dezvolta produse software, nu creeaza proprietate intelectuala proprie si utilizeaza exclusiv solutii software comerciale. Riscurile asociate drepturilor de proprietate intelectuala au fost evaluate ca fiind inexistente pentru domeniul de aplicare al SMSI	

5.33	Protectia inregistrarilor	**DA**	Inregistrarile trebuie protejate impotriva pierderii, distrugerii, falsificarii, accesului neautorizat si publicarii neautorizate	Back-up, loguri, rapoarte de audit Protejate prin controlul accesului, Criptare cu parola	*Implementat*
5.34	Controlul confidentialitatii si protectiei informatiilor Informatii de identificare personala (PII)	**DA**	Organizatia identifica si respecta cerintele legate de pastrarea vietii private si de protectia PII in conformitate cu legile si reglementarile aplicabile si cu cerintele contractuale	Regulament privind protectia datelor cu caracter personal la nivelul AFDJ RA Galati	*Implementat*
5.35	Revizuirea independenta a securitatii informatiilor.	**DA**	Abordarea organizatiei in ceea ce priveste gestionarea securitatii informatiilor si implementarea acesteia, inclusiv a persoanelor, proceselor si tehnologiilor, va fi revizuita independent la intervale planificate sau atunci cand apar schimbari semnificative	Audit informatic extern in conformitate cu directiva NIS	*Implementat*
5.36	Respectarea politicilor, reglementarilor si standardelor de securitate a informatiilor	**DA**	Conformitatea cu politica de securitate a informatiilor a organizatiei, politicile, regulile si standardele specifice subiectului vor fi revizuite periodic	Politica de utilizare a Echipamentelor IT si a Internetului - revizuita/actualizata ori de cate ori e cazul	*Implementat*
5.37	Proceduri de operare documentate	**DA**	Procedurile de functionare a sistemelor de prelucrare a informatiilor ar trebui sa fie documentate si puse la dispozitia personalului aflat in dificultate	-Proceduri documentate postate pe serverul regiei, cu acces pentru intreg personalul -Instruire specifica	*Implementat*
6	**Controlul persoanelor**				
6.1	Verificări	**DA**	Verificarile antecedentelor tuturor candidatilor care urmeaza sa devina membri ai personalului vor fi efectuate inainte de aderarea la organizatie si in mod continuu, tinand seama de legile, reglementarile si etica aplicabile, si vor fi proportionale cu cerintele comerciale, clasificarea	Dosar personal conform procedurii, după caz: -cazier judiciar solicitat la angajare, -scrisoare recomandare.	*Implementat*

			informatiilor care trebuie accesate si riscurile percepute		
6.2	Termeni si conditii de angajare	**DA**	Termenii si conditiile angajarii trebuie sa stabileasca in mod clar responsabilitatile angajatilor, contractorilor si utilizatorilor terta parte privind Securitatea informatiilor pentru a reduce riscul de furt, frauda si eroare de utilizare	-Regulament Intern (RI) -Contracte achizitii servicii -PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice	*Implementat*
6.3	Constientizarea, educatia si formarea in materie de securitate a informatiilor	**DA**	Toti angajatii organizatiei trebuie sa beneficieze de instruire pentru constientizarea corepunzatoare si actualizare periodica referitoare la politicile si procedurile organizatiei relevante pentru postul si functia loc, in domeniul securitatii informației	-Instruirea anagatilor cu privire la Politica de utilizare a Echipamentelor IT si a Internetului si proceduri -Cursuri perfectionare, dupa caz	*Implementat*
6.4	Procesul disciplinar	**DA**	Un proces disciplinar eficace formalizat si comunicat pentru a se lua masuri impotriva personalului si a altor parti interesate relevante care au comis o incalcare a politicii de securitate a informatiilor	-PS 10.2-1 Semnalarea neregulilor si protectia avertizorului -Regulament Intern (RI)	*Implementat*
6.5	Responsabilitati dupa incetarea sau schimbarea locului de munca	**DA**	Responsabilitatile si indatoririle in materie de securitate a informatiilor care raman valabile dupa incetarea sau schimbarea locului de munca trebuie sa fie definite, puse in aplicare si comunicate personalului relevant si altor parti interesate	-Regulament Intern (RI)	*Implementat*
6.6	Acorduri de confidentialitate sau de nedivulgare	**DA**	Acordurile de confidentialitate sau de nedivulgare care reflecta nevoile organizatiei de protectie a informatiilor ar trebui identificate, documentate, revizuite periodic si semnate de personal si de alte parti interesate relevante	-Regulament Intern (RI) -Contracte achizitii servicii	*Implementat*
6.7	Lucrul de la distanta	**DA**	Trebuie asigurata securitatea informatiilor prin procedura atunci cand se desfasoara activitati de tipul teleworking din mediile neprotejate	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice – care prevede accesul de la distanta prin VPN	*Implementat*

6.8	Rapoarte privind evenimentele de securitate a informatiilor	**DA**	Organizatia pune la dispozitie un mecanism prin care personalul sa raporteze in timp util evenimentele de securitate a informatiilor observate sau suspectate prin canale adecvate	-*Politica de utilizare a Echipamentelor IT si a Internetului* -adresa de email: *informatica@afdj.ro* -Platforma nationala pentru raportarea incidentelor de securitate cibernetica *https://pnrisc.dnsc.ro*	*Implementat*
7	**Controale fizice**				
7.1	Perimetre de securitate fizica	**DA**	Perimetrele de securitate vor fi definite si utilizate pentru a proteja zonele care contin informatii si alte active asociate	Zone cu acces fizic restrictionat	*Implementat*
7.2	Intrarea fizica	**DA**	Zonele securizate trebuie protejate prin controale de intrare si puncte de acces adecvate	-Camere video la fiecare nivel al cladirii -Acces securizat pe baza de cartela electronica pentru intrarea in unitate -Paza	*Implementat*
7.3	Birouri, camere si facilitati securizate	**DA**	Securitatea fizica a birourilor, camerelor si facilitatilor va fi proiectata si implementata	Intern - Camere video la fiecare nivel al cladirii Extern - Camere video	*Implementat*
7.4	Monitorizarea securitatii fizice	**DA**	Spatiile sunt monitorizate in permanenta pentru a asigura accesul fizic neautorizat	-Camere video la fiecare nivel al cladirii -Acces securizat pe baza de cartela electronica pentru intrarea in unitate -Paza	*Implementat*
7.5	Protectia impotriva amenintarilor fizice si de mediu	**DA**	Protectia impotriva amenintarilor fizice si de mediu, cum ar fi dezastrele naturale si alte amenintari fizice intentionate sau neintentionate la adresa infrastructurii, trebuie sa fie conceputa si pusa in aplicare	-Senzori fum -Sistem antiincendiu in camera server -Camere de supraveghere video	*Implementat*
7.6	Lucrul in zone sigure	**DA**	Masurile de siguranta sunt concepute si puse in aplicare pentru a functiona in zone sigure	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice - **PRASI**	*Implementat*
7.7	Birou curat si ecran protejat	**DA**	Reguli pentru birouri curate pentru documente si suporturi de stocare amovibile si regulile privind desktop curat pentru instalatiile de procesare a informatiilor trebuie sa fie definite si puse in aplicare in mod corespunzator	Politica de utilizare a Echipamentelor IT si a Internetului	*Implementat*

7.8	Amplasarea si protectia echipamentului	**DA**	Echipamentul va fi amplasat intr-un mod sigur	-Camera serverelor este izolata si protejata. -Copiatoare situate in zona de vizibilitate a camerelor de supraveghere	*Implementat*
7.9	Securitatea activelor din afara site-ului	**DA**	Activele din afara amplasamentului vor fi protejate.	Criptarea dispozitivelor mobile conform Politicii de utilizare a echipamentelor IT si a Internetului	*Implementat*
7.10	Medii de stocare	**DA**	Mediile de stocare trebuie gestionate pe tot parcursul ciclului lor de viata, de achizitie, utilizare, transport si eliminare, in conformitate cu sistemul de clasificare si cerintele de manipulare ale organizatiei	-Politica de utilizare a echipamentelor IT si a Internetului -PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice (Protectia datelor din cadrul sistemului informatic)	*Implementat*
7.11	Suport utilitati	**DA**	Sistmele de prelucrare a informatiilor trebuie sa fie protejate impotriva penelor de curent si a altor intreruperi cauzate de defectiuni	Folosire de UPS-uri	*Implementat*
7.12	Cablare de siguranta	**DA**	Cablurile care transporta energie electrica, date sau servicii de informatii justificative trebuie protejate impotriva interceptarii, interferentelor sau deteriorarii	Cabluri mascate	*Implementat*
7.13	Intretinerea echipamentelor	**DA**	Echipamentul va fi intretinut in mod corespunzator pentru a asigura disponibilitatea, integritatea si confidentialitatea informatiilor	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice	*Implementat*
	Eliminarea sau reutilizarea securizata a echipamentelor	**DA**	Componentele de tip suporturi de stocare vor fi verificate pentru a se asigura ca toate datele sensibile si software-ul licentiat au fost sterse sau suprascrise in siguranta inainte de stergere sau reutilizare	-PS 7.5.3-6 Activitatea de administrare a retelei de calculatoare -Politica de utilizare a Echipamentelor IT si a Internetului	*Implementat*
8	**Controlul tehnologiei**				
8.1	Dispozitive pentru statiile de lucru ale utilizatorilor	**DA**	Informatiile stocate, procesate sau accesibile prin intermediul dispozitivelor finale ale utilizatorului vor fi protejate	Politica de utilizare a Echipamentelor IT si a Internetului	*Implementat*
8.2	Drepturi de acces privilegiate	**DA**	Cesiunea si utilizarea drepturilor de acces	Politica de utilizare a Echipamentelor IT si a Internetului	*Implementat*

			privilegiate sunt restrictionate si gestionate		
8.3	Restrictionarea accesului la informatii	**DA**	Accesul la informatii si la alte active asociate va fi restrictionat in conformitate cu politica specifica stabilita privind controlul accesului	Politica de utilizare a Echipamentelor IT si a Internetului	*Implementat*
8.4	Accesul la codul sursa	**NU**	Accesul la citirea si scrierea la codul sursa, instrumentele de dezvoltare si bibliotecile de software vor fi gestionate in mod corespunzator	Controlul nu este aplicabil deoarece Regia nu detine, nu dezvolta si nu gestioneaza cod sursa propriu, instrumente de dezvoltare sau biblioteci de software.	
8.5	Autentificare securizata	**DA**	Tehnologiile si procedurile de autentificare securizata vor fi implementate pe baza restrictiilor privind accesul la informatii si a politicii specifice privind controlul accesului	Politica de utilizare a Echipamentelor IT si a Internetului	*Implementat*
8.6	Managementul capacitatilor	**DA**	Utilizarea resurselor este monitorizata si ajustata in conformitate cu cerintele actuale si preconizate in materie de capacitate	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice	*Implementat*
8.7	Protectie impotriva programelor malware	**DA**	Protectia impotriva programelor malware va fi implementata si sustinuta de o constientizare adecvata a utilizatorilor	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice	*Implementat*
8.8	Managementul vulnerabilitatilor tehnice	**DA**	Ar trebui sa se obtina informatii cu privire la vulnerabilitatile tehnice ale sistemelor informatice utilizate, expunerea organizatiei la astfel de vulnerabilitati ar trebui evaluata si ar trebui luate masuri adecvate	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice	*Implementat*
8.9	Gestionarea configuratiei	**DA**	Configuratiile, inclusiv securitatea, hardware-ul, software-ul, serviciile si configuratiile de retea trebuie sa fie stabilite, documentate, implementate, monitorizate si revizuite	PS 7.5.3-6 Activitatea de administrare a retelei de calculatoare Software monitorizare retea - Omada - PRTG Monitorizare log-uri activitate sistem informatic cu Graylog Software protectie antimalware Bitdefender Sistem Firewall hardware	*Implementat*
8.10	Stergerea informatiilor	**DA**	Informatiile stocate in sisteme informatice, dispozitive sau orice alt suport de stocare vor	Politica de utilizare a Echipamentelor IT si a Internetului	*Implementat*

			fi sterse atunci cand nu mai sunt necesare		
8.11	Mascarea datelor	**DA**	Mascarea datelor ar trebui sa fie utilizata in conformitate cu politica specifica a organizatiei privind controlul accesului si cu alte politici legate de subiectul specific si cu cerintele de afaceri, tinand seama de legislatia aplicabila	*PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice* - Definirea si aprobarea cerintelor de securitate pentru aplicatii	*Implementat*
8.12	Prevenirea scurgerilor de date	**DA**	Masurile de prevenire a scurgerilor de date se aplica sistemelor, retelelor si oricaror alte dispozitive care prelucreaza, stocheaza sau transmit informatii sensibile	Auditarea accesului la fisiere	*Implementat*
8.13	Copierea de rezerva a informatiilor	**DA**	Copiile de rezerva ale informatiilor, software-ului si sistemelor vor fi intretinute si testate periodic in conformitate cu politica de backup specifica subiectului convenit	Procedura back-up periodic	*Implementat*
8.14	Redundanta instalatiilor de prelucrare a informatiilor	**DA**	Sistemele de prelucrare a informatiilor sunt instalate cu o redundanta suficienta pentru a indeplini cerintele de disponibilitate	Echipamente de rezerva	*Implementat*
8.15	Login	**DA**	Jurnalele care inregistreaza activitati, exceptii, defectiuni si alte evenimente relevante vor fi produse, stocate, protejate si analizate	Solutia GrayLog	*Implementat*
8.16	Activitati subsecvente	**DA**	Retelele, sistemele si aplicatiile sunt monitorizate pentru un comportament anormal si pentru a se lua masuri adecvate pentru a evalua potentialele incidente de securitate a informatiilor	Omada, Bitdefender EDR	*Implementat*
8.17	Sincronizarea ceasului	**DA**	Ceasurile sistemelor de procesare a informatiilor utilizate de organizatie trebuie sincronizate cu sursele de timp aprobate	NTP Server Local	*Implementat*
8.18	Folosirea utilitatilor privilegiate	**DA**	Folosirea utilitatilor care pot inlocui controalele sistemului si aplicatiilor trebuie restrictionata si controlata cu strictete	Utilizatori cu drepturi de acces limitate folosind AD la nivel de regie	*Implementat*

8.19	Instalarea software-ului pe sistemele de operare	**DA**	Procedurile si masurile vor fi puse in aplicare pentru a gestiona in siguranta instalarea de software pe sistemele de operare	PS 7.5.3-6 Activitatea de administrare a retelei de calculatoare	*Implementat*
8.20	Securitatea retelei	**DA**	Retelele si dispozitivele de retea vor fi securizate, gestionate si controlate pentru a proteja informatiile din sisteme si aplicatii	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice	*Implementat*
8.21	Securitatea serviciilor de retea.	**DA**	Mecanismele de securitate, nivelurile serviciilor si cerintele de servicii ale serviciilor de retea sunt identificate, puse in aplicare si controlate	PS 7.5.3-6 Activitatea de administrare a retelei de calculatoare	*Implementat*
8.22	Segregarea retelei	**DA**	Grupurile de servicii de informatii, utilizatori si sisteme informatice ar trebui sa fie separate in retelele organizatiei	Prin configurari in echipamentul firewall	*Implementat*
8.23	Filtrare web	**DA**	Accesul la site-uri externe va fi gestionat pentru a reduce expunerea la continut rau intentionat	Prin configurari in echipamentul firewall	*Implementat*
8.24	Utilizarea criptografiei	**DA**	Trebuie definite si puse in aplicare norme pentru utilizarea eficienta a criptografiei, inclusiv gestionarea cheilor criptografice	Fisier cu gestionarea cheilor de criptare, RESME	*Implementat*
8.25	Ciclul de viata al dezvoltarii securizate	**DA**	Vor fi stabilite si puse in aplicare norme pentru dezvoltarea de software si sisteme securizate	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice	*Implementat*
8.26	Cerinte de securitate a aplicatiilor	**DA**	Cerintele de securitate a informatiilor trebuie identificate, specificate si aprobate la elaborarea sau achizitionarea de aplicatii	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice	*Implementat*
8.27	Principiile arhitecturii si ingineriei sistemelor securizate	**DA**	Principiile pentru ingineria sistemelor securizate ar trebui stabilite, documentate, mentinute si aplicate in orice activitate de dezvoltare a sistemelor informatice	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice – ***(PROFIT)***	*Implementat*
8.28	Criptare securizata	**NU**	Principiile codarii securizate se vor aplica dezvoltarii de software	Controlul nu este aplicabil deoarece Regia nu desfasoara activitati de programare sau dezvoltare interna de cod sursa.	
8.29	Testarea securitatii in dezvoltare si acceptare	**NU**	Procesele de testare a securitatii vor fi definite si implementate in ciclul de viata al dezvoltarii	Controlul nu este aplicabil deoarece Regia nu desfasoara activitati de programare sau dezvoltare interna de cod sursa	

8.30	Dezvoltare externalizata	**DA**	Organizatia conduce, monitorizeaza si revizuieste activitatile legate de dezvoltarea sistemelor externalizate	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice - Stabilirea relatiilor ecosistemului (***PROSRE)***	*Implementat*
8.31	Separarea mediilor de dezvoltare, testare si productie	**NU**	Mediile de dezvoltare, testare si productie trebuie sa fie separate si protejate	Controlul nu este aplicabil deoarece Regia nu detine si nu opereaza medii proprii de dezvoltare sau testare de software	
8.32	Managementul schimbarii	**DA**	Modificarile aduse instalatiilor de prelucrare a informatiilor si sistemelor informatice fac obiectul unor proceduri de gestionare a schimbarilor	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice - Mentinerea securitatii retelelor si sistemelor informatice (***PROMNIS)***	*Implementat*
8.33	Informatii de testare	**NU**	Informatiile de testare vor fi selectate, protejate si gestionate in mod corespunzator	Controlul nu este aplicabil deoarece Regia nu realizeaza teste de dezvoltare sau configurare de software care sa necesite utilizarea unor date sau informatii de test speciale	
8.34	Protectia sistemelor informatice in timpul testelor de audit	**DA**	Testele de audit si alte activitati de asigurare care implica evaluarea sistemelor de operare ar trebui planificate si convenite intre evaluator si conducerea corespunzatoare	PS 7.5.3-8 Asigurarea securitatii retelelor si sistemelor informatice - retelelor si sistemelor informatice	*Implementat*

DIRECTOR GENERAL
Angela Stela IVAN

Intocmit: CG, TR - SAITA, SM - CCM - 1.exemplar original/15 pagini