APAVIL S.A.

ISO 9001
ISO 14001
ISO 45001
BUREAU VERITAS
Certification

Nr.Reg.Com. J 2004000522380
C.U.I.: RO 16468149
Site: www.apavil.ro

Str. CAROL I, nr. 3-5, Rm. Vâlcea, jud. Vâlcea Fax: 0250/738903
Nr 9540 / 27.03.2026 Tel: 0350/802161

APROBAT,
DIRECTOR GENERAL
Dr. Ing. Florescu Ion

S.A. RM. VÂLCEA JUD. VÂLCEA

POLITICA PRIVIND SECURITATEA INFORMAȚILOR

Exemplar controlat	DA	NU

Intocmit,

Responsabil Securitatea Rețelelor și Sistemelor Informatice,
Total Data Management SRL

Acest document este proprietatea APAVIL SA. Copierea, difuzarea sau utilizarea lui, chiar parţiala, in exteriorul APAVIL SA este interzisa daca nu exista acordul Conducerii APAVIL SA .

27.03.2026

1. SCOP

În activitățile desfășurate în cadrul APAVIL S.A. se creează, colectează, stochează și prelucrează cantități mari de date și informații. Informaţiile şi procesele, sistemele informatice şi reţelele asociate, precum şi personalul implicat în exploatarea, manipularea şi protecţia acestora sunt resurse importante pentru APAVIL S.A. şi, în consecinţă, necesită o protecţie adecvată împotriva diverselor amenințări și pericole.

Resursele sunt expuse atât ameninţărilor intenţionate, cât şi celor accidentale, iar procesele, sistemele informatice şi reţelele asociate, precum şi personalul pot prezenta vulnerabilităţi inerente. Schimbările intervenite în modul de desfășurare a activităților, în cadrul sistemelor utilizate sau alte schimbări externe (cum ar fi, legi, norme şi reglementări noi) pot crea noi riscuri de securitate a informaţiei. Prin urmare, dată fiind multitudinea de moduri în care ameninţările pot profita de vulnerabilități pentru a dăuna organizației, riscurile de securitate a informaţiei sunt întotdeauna prezente. O securitate eficace a informaţiei reduce aceste riscuri, prin protejarea organizației împotriva ameninţărilor şi vulnerabilităţilor şi, apoi, reduce impactul asupra resurselor ei.

Securitatea informaţiilor este obţinută prin implementarea unui set adecvat de măsuri și mijloace de control, incluzând politici, procese, proceduri, funcţii şi structuri organizatorice, precum și software şi hardware. Aceste măsuri și mijloace de control necesită să fie stabilite, implementate, supravegheate, revizuite şi îmbunătăţite, dacă este necesar, pentru a se asigura atingerea obiectivelor de securitate ale organizației.

Politica privind securitatea informațiilor are ca scop stabilirea cadrului necesar pentru elaborarea celorlalte politici, programe, planuri, norme, ghiduri, metodologii și proceduri privind securitatea informațiilor, în scopul asigurării integrităţii, confidenţialităţii şi disponibilităţii datelor și informaţiilor la nivelul APAVIL S.A.

Această politică face parte din setul de politici și proceduri de securitate a informațiilor, de protecție a datelor cu caracter personal și a rețelelor și sistemelor informatice și de comunicații care asigură furnizarea serviciilor și care vehiculează informații clasificate (secrete de serviciu, confidențiale, etc) și are menirea de a clarifica modul de organizare și desfășurare/ derulare a procesului de Management al Securității Informațiilor în APAVIL S.A.

Prezenta politică constituie baza pentru dezvoltarea unui Program de prevenire a scurgerii de informații clasificate (PPSIC), eficient, care să cuprindă și să descrie, în detaliu:

- cadrul organizatoric,
- prezentarea structurii și funcțiilor desemnate să îndeplinească atribuţii pe linia protecţiei activităţilor, datelor, informaţiilor şi documentelor clasificate, precum și atribuțiile specifice pentru managementul eficient al acestui domeniu,
- principalele obiective ale protecţiei informaţiilor clasificate,
- principiile avute în vedere în elaborarea şi aplicarea măsurilor şi procedurilor de securitate,
- listele cu informații clasificate,
- lista funcţiilor care necesită acces la informaţii clasificate, conform principiului "nevoii de a ști",
- locurile unde se concentrează, de regulă sau temporar, date, informaţii, documente clasificate sau se desfăşoară activităţi clasificate,
- măsurile de protecţie fizică a clădirilor, spaţiilor şi locurilor unde se păstrează sau se concentrează informaţii clasificate ori se dsfăşoară astfel de activităţi,

- măsurile procedurale de protecţie a datelor, informaţiilor, documentelor şi activităţilor clasificate,
- prezentarea „Sistemului Informatic și de Comunicații", destinat preluării, prelucrării, stocării şi transmiterii de date şi informații clasificate,
- modul de administrare și organizare a sistemului informatic și de comunicații clasificat,
- măsurile de protecţie împotriva observării şi ascultării (intenționate sau neintenționate),
- controalele, activităţile de analiză şi de evaluare a modului în care se respectă prevederile legale referitoare la protecţia informaţiilor clasificate,
- soluţionarea cazurilor de încălcare a reglementărilor privind protecţia informaţiilor clasificate
- măsurile de instruire, educație și conștientizare a persoanelor care au atribuţii pe linia protecţiei informaţiilor clasificate şi a celor care au acces la astfel de informaţii, precum și stabilirea unui Program de instruire, pregătire și conștientizare a personalului cu privire la cerințele legale de securitatea informațiilor aplicabile pentru fiecare loc de muncă sau activități desfășurate.

Politica privind securitatea informațiilor permite:

- armonizarea proceselor de management al riscului din cadrul sistemelor de management;
- dezvoltarea unei culturi organizaționale în ceea ce privește securitatea informațiilor;
- armonizarea stilului de management funcție de riscurile interne și externe existente la adresa securității informațiilor;
- realizarea în condiții mai sigure, de eficacitate și eficiență, a obiectivelor APAVIL S.A.

2. DOMENIU APLICARE

Politica se aplică tuturor angajaților APAVIL S.A., colaboratorilor și angajaţilor furnizorilor de servicii care accesează resursele informaţionale ale APAVIL S.A.

Pentru a răspunde cerinţelor de securitate identificate prin analiza și determinarea riscului, managementul de la cel mai înalt nivel al APAVIL S.A. s-a angajat să dezvolte, să implementeze şi să menţină un Sistem de Management al Securităţii Informaţiei bazat pe implementarea obiectivelor şi măsurilor de securitate (conform legislației în vigoare), privind:

- Politica de securitate;
- Organizarea securităţii informaţiei;
- Managementul resurselor;
- Securitatea resurselor umane;
- Securitatea fizică şi a mediului de lucru;
- Managementul comunicaţiilor şi operaţiunilor;
- Controlul accesului;
- Achiziţionarea, dezvoltarea şi mentenanaţa sistemelor informatice;
- Managementul incidentelor de securitate a informaţiei;
- Managementul continuităţii afacerii;
- Conformitatea.

Politica de securitate se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a APAVIL S.A., respectiv:

- Angajaţi;
- Colaboratori;
- Furnizori;
- Clienţi;
- Alte persoane, entităţi sau organizaţii externe.

2.1. Precizarea (definirea) activității la care se referă politica

În activitățile desfășurate în cadrul APAVIL S.A. se creează, colectează, stochează și prelucrează cantități mari de date și informații. Toate aceste informații, alături de procesele, sistemele informatice şi reţelele asociate, precum și structurile şi personalul alocate pentru exploatarea, manipularea şi protecţia acestora reprezintă resurse strategice pentru APAVIL S.A. şi, în consecinţă, necesită o protecţie adecvată împotriva diverselor amenințări și pericole.

Compromiterea securității acestor resurse poate afecta capacitatea APAVIL S.A. de a oferi, fără întrerupere, servicii de calitate și poate conduce la fraude, la producerea de incidente legate de pierderea confidenţialităţii informațiilor, distrugerea informațiilor sau violarea unor clauze/ obligații contractuale, precum și la afectarea imaginii, prestigiului și credibilității organizației în faţa cetățenilor și partenerilor săi.

Resursele sunt expuse atât ameninţărilor intenţionate, cât şi celor accidentale, iar procesele, sistemele informatice şi reţelele asociate, precum şi personalul pot prezenta vulnerabilităţi inerente. Schimbările intervenite în modul de desfășurare a activităților, în cadrul sistemelor utilizate sau alte schimbări externe (cum ar fi, legi, norme şi reglementări noi) pot crea noi riscuri de securitate a informaţiei.

Riscurile de securitate la adresa informaţiei sunt întotdeauna prezente, dată fiind multitudinea de moduri în care ameninţările pot profita de vulnerabilităţi, pentru a dăuna organizației.

O securitate/ protecție eficace a datelor și informaţiilor reduce aceste riscuri prin protejarea organizației împotriva ameninţărilor şi vulnerabilităţilor şi apoi reduce impactul asupra resurselor ei, de orice natură (informaționale, umane, financiare, IT&C, etc).

Pe lângă bunele practici și normele interne, regulamentele și ghidurile stabilite la nivelul organizației, anumite categorii de date și informații pot intra sub incidența, atât a reglementărilor și legislației naţionale, cât și a celor UE sau NATO, devenind, astfel, vital ca întreg personalul să cunoască toate detaliile legate de modul de gestionare și manipulare datelor și informațiilor APAVIL S.A.

2.2. Delimitarea explicită a activității în cadrul portofoliului de activități desfășurate de societate

Securitatea informaţiilor, proprietate a APAVIL S.A., este obţinută prin aprobarea și implementarea unui set adecvat de măsuri și mijloace de control, incluzând politici, procese, proceduri, funcţii şi structuri organizatorice, precum și software şi hardware. Aceste măsuri și mijloace de control necesită să fie stabilite, implementate, monitorizate, revizuite şi îmbunătăţite (dacă este necesar), pentru a se asigura atingerea obiectivelor de securitate ale organizației.

Această politică este stabilită astfel încât:

- să fie în conformitate cu statutul, regulamentele, legile și alte documente oficiale în vigoare privind administrarea resurselor informaționale care asigură furnizarea de servicii;
- să stabilească practici prudente şi acceptabile privind utilizarea resursele informaționale ale APAVIL S.A.;
- să instruiască personalul care are acces autorizat la resursele informaționale precum și utilizatorii autorizați cu drepturi de acces la resursele sistemului informatic privind obligațiile și responsabilităţile asociate unui astfel de acces.

Fiecare angajat, colaborator sau angajat al furnizorilor de servicii este răspunzător pentru aplicarea întocmai, în activitatea sa, a politicilor şi procedurilor de securitate în vigoare, elaborate, aprobate şi implementate, conform legislaţiei/ reglementărilor specifice domeniului şi a normelor interne ale APAVIL S.A. și are obligaţia raportării oricărui incident de securitate sesizat.

3. DOCUMENTE DE REFERINŢĂ ŞI CONEXE

3.1. Reglementări internaţionale

- SR ISO/ CEI 27001: 2022 – Tehnologia informaţiei. Tehnici de securitate. Sisteme de management a securităţii informaţiei;
- SR EN ISO 9001:2015 – Sisteme de management al calităţii. Cerinţe;
- SR ISO/ CEI 27002: 2022 - Tehnologia informaţiei. Tehnici de securitate. Cod de bună practică pentru managementul securităţii informaţiei;
- Directiva (UE) 2022/ 2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de Securitate cibernetica in Uniune, de modificare a regulamentului UE nr 910/ 2014 si a Directivei (UE) 2018/1972 si de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2);
- Regulamentul (UE) 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).

3.2. Legislaţie primară

- OUG nr. 155 din 32 12 2024 privind instituirea unui cadru de Securitate cibernetica a retelelor si sistemelor informatice din spatiul cibernetic national 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 şi sistemelor informatice din spațiul cibernetic național civil;
- Legea 362/ 2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice;
- Legea nr.182/2003, din 12 aprilie 2003, privind securitatea informațiilor;
- HG nr. 585/2003 pentru aprobarea Standardelor naţionale de protecţie a informațiilor în România;
- HG nr. 781, din 25 iulie 2003 privind protecţia informaţiilor secrete de serviciu;
- Legea nr. 333, din 2003. privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor;
- Legea nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public;
- Legea nr. 190/ 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/ 679 al Parlamentului European și al Consiliului;

- Legislaţia aplicabilă în vigoare privind furnizarea serviciului public de alimentare cu apa si de canalizare in conditii de sustenabilitate.

3.3. Legislaţie secundară

- OSGG 600/ 2018 – privind aprobarea Codului controlului intern managerial al entităţilor publice;
- OSGG 1.323/ 2020 – de aprobare a Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale ;
- Ghidul pentru implementarea măsurilor minime de securitate aplicabile OSE – DNSC.

3.4. Alte documente, inclusiv reglementări interne ale societății

- Regulamentul intern (RI) al Apavil S.A.;
- Regulamentul de organizare şi funcţionare (ROF) al Apavil S.A.;
- Contract Colectiv/Individual de munca, Fisa postului, Decizii ale APAVIL S.A.

4. TERMINOLOGIE SI ABREVIERI

4.1. Terminologie

Nr. crt.	Termenul	Definiția și/ sau, dacă este cazul, actul care definește termenul
1.	Securitatea fizică	Domeniul securităţii care prezintă atât măsuri pentru prevenire cât şi pentru împiedicarea atacatorilor să aibă acces la obiective, resurse sau informaţii şi recomandări privind proiectarea infrastructurii pentru a opune rezistenţă la actele ostile.
2	Securitatea informaţiei	Păstrarea confidenţialităţii, integrităţii, disponibilităţii, autenticităţii şi a nerepudierii informaţiei.
3	Confidenţialitate	Proprietatea ca informaţia să nu fie făcută disponibilă sau divulgată unor persoane, entităţi, sau procese neautorizate.
4	Integritate	Proprietatea de a proteja acurateţea şi completitudinea resurselor.
5	Disponibilitate	Proprietatea de a fi accesibil şi utilizabil la cerere de către o entitate autorizată.
6	Autenticitate	Asigurarea identificării și/sau autentificării (de încredere) a informațiilor, persoanelor, dispozitivelor și serviciilor sistemului informatic
7	Nerepudiere	Asigurarea unei capacități corespunzătoare de a dovedi faptul că o acțiune sau un eveniment a avut loc, astfel încât, respectiva acțiune sau respectivul eveniment, să nu poată fi repudiate/negate ulterior.
8	Atac	Încercare de a distruge, a expune, a modifica, a dezactiva, a fura sau a obţine accesul neautorizat sau a utiliza în mod neautorizat o resursă.
9	Ameninţare	Cauză potenţială a unui incident nedorit care poate produce daune unui sistem sau organizaţii.
10	Vulnerabilitate	Slăbiciune a unei resurse sau a unui mijloc de control care poate fi exploatată de o ameninţare.
11	Eveniment privind securitatea informaţiei	Fapt identificat în legătură cu starea unui sistem, a unui serviciu, sau a unei reţele indicând o posibilă încălcare a politicii de securitate a informaţiei, un eşec al mijloacelor de control sau o

Nr. crt.	Termenul	Definiția și/ sau, dacă este cazul, actul care definește termenul
		situaţie ignorată anterior dar care poate fi relevantă din punct de vedere al securităţii.
12	Incident privind securitatea informaţiei	Unul sau o serie de evenimente privind securitatea informaţiei nedorite sau neprevăzute care au o probabilitate semnificativă de compromitere a operaţiunilor de business şi de ameninţare a securităţii informaţiei.
13	Date cu caracter personal	Orice informaţii privind o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.
14	Responsabil securitatea rețelelor și sistemelor informatice (RSRSI)	Responsabil securitatea rețelelor și sistemelor informatice colaborează cu Responsabilul IT&C și cu conducerea societății pentru a asigura cadrul general de politici, programe, planuri, norme, ghiduri, metodologii și proceduri privind securitatea cibernetică, în scopul asigurării integrităţii, confidenţialităţii şi disponibilităţii datelor și informaţiilor la nivelul Apavil S.A.
15	Responsabilul IT&C	Responsabilul IT&C administrează sistemele IT&C și aplică măsurile de securitate ce asigură securitatea rețelelor și sistemelor informatice din cadrul societății. Responsabilul IT&C este reprezentat de angajații din cadrul Compartimentului IT (ce își au sarcinile împărțite conform fișei de post). Aceștia planifică, implementează, verifică și inventariază soluțiile hardware si software utilizate în cadrul rețelelor și sistemelor informatice din societate, primesc și soluționează solicitări și tratează incidentele de securitate. Pentru îndeplinirea sarcinilor sale, Responsabilul IT&C colaborează cu Responsabilul cu Securitatea Retelelor si Sistemelor Informatice și cu furnizorii societății de soluții software, furnizorii de hardware, furnizorii de soluții de securitate cibernetică, furnizorii de soluții de monitorizare video, furnizorii de soluții web și de comunicare electronică, etc.
16	Responsabilul cu protecția datelor	Responsabilul cu protecția datelor este persoana desemnată de o organizație pentru a supraveghea respectarea legislației privind protecția datelor cu caracter personal, în special Regulamentul General privind Protecția Datelor (GDPR). Acesta are rolul de a consilia conducerea și angajații cu privire la obligațiile legale, de a monitoriza conformitatea internă și de a acționa ca punct de contact între organizație și Autoritatea de Supraveghere (ANSPDCP).

4.2. Abrevieri

Nr. Crt.	Abrevierea	Termenul abreviat
1.	GDPR	Regulamentul General pentru Protecția Datelor personale
2.	UE	Uniunea Europeană
3	ISO	Organizaţia Internaţională de Standardizare (în engleză - International Organization for Standardization)
4	SIC	Sistem Informatic și de Comunicații
5	IT&C	Tehnologia Informațiilor și Comunicațiilor
5	INFOSEC	Securitatea informaţiilor în Sistemele Informatice şi de Comunicaţii
6	PPSIC	Programul de Prevenire a Scurgerii de Informații Clasificate
7	RI	Regulamentul intern
8	ROF	Regulamentul de organizare și funcționare

5. REGULI SI RESPONSABILITATI

5.1. Responsabilitati

5.1.1. Directorul General Apavil S.A. are următoarele responsabilități:

- stabileşte și aprobă Politica de securitate a informaţiilor, politicile subsecvente și obiectivele de securitate a informațiilor;
- asigură disponibilitatea resurselor necesare pentru managementul securității informațiilor;
- comunică importanța unei gestionări eficiente a securității informației și a respectării cerințelor Sistemului de Management al Securității Informațiilor.

5.1.2. Responsabilul cu protecția datelor: (angajat al societății sau al unui furnizor de servicii de protecție a datelor cu caracter personal):

- informează și oferă consiliere personalului APAVIL S.A. și persoanelor împuternicite de organizaţie pentru prelucrarea datelor cu caracter personal care își desfășoară activitatea în temeiul GDPR și al altor dispoziții naționale sau ale Uniunii Europene privind protecția datelor,
- coordonează identificarea și evaluarea activităților de prelucrare a datelor desfășurate în organizaţie,
- participă la întâlniri cu conducerea organizaţiei, atunci când sunt concepute noi prelucrări, pentru a se asigura de respectarea principiului protecției datelor începând cu momentul conceperii, la toate nivelurile;
- menține evidențele activităților de prelucrare în conformitate cu articolul 30 din GDPR;
- monitorizează conformitatea cu GDPR, cu alte dispoziții naționale sau ale Uniunii Europene privind protecția datelor și cu politicile și procedurile APAVIL S.A. în ceea ce privește protecția datelor cu caracter personal, inclusiv atribuirea responsabilităților, conștientizarea și instruirea personalului implicat în operațiunile de prelucrare și auditurile aferente;
- oferă consiliere atunci când este solicitat în ceea ce privește evaluarea impactului asupra protecției datelor (DPIA) și monitorizează performanța sa în conformitate cu articolul 35;
- cooperează cu autoritatea de supraveghere;
- întocmește și actualizează politicile și procedurile interne de protecție a datelor;
- efectuează audituri pentru a determina conformitatea cu politicile și procedurile interne de protecție a datelor și necesitățile de îmbunătățire;

- implementează un program de instruire cu privire la protecția datelor personale pentru personalul APAVIL S.A. implicat în activități de prelucrare;
- urmăreşte modificările aduse legislației și formulează recomandări pentru a asigura conformitatea cu aceste modificări;
- menține o evidență a încălcărilor vieții private în operațiunile de prelucrare desfășurate de organizaţie;
- oferă consiliere cu privire la modul de abordare a încălcărilor vieții private;
- se asigură că organizaţia răspunde solicitărilor persoanelor vizate în termenele legale;
- acționează ca punct de contact cu rezidenții din UE, autoritatea de supraveghere națională și autoritățile celorlalte țări ale Uniunii Europene și cu echipele interne în ceea ce privește aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la articolul 36 și consultă autoritatea de supraveghere națională, dacă este cazul, cu privire la orice altă chestiune;
- are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale.

În îndeplinirea atribuțiilor sale, Responsabilul cu protecția datelor are în vedere riscurile asociate operațiunilor de prelucrare, ținând seama de natura, de domeniul de aplicare, de contextul și de scopurile procesării.

5.1.3. Responsabil securitatea rețelelor și sistemelor informatice: (angajat al societății sau al unui furnizor de servicii IT&C):

- elaborează politicile și procedurile privind securitatea a sistemelor informatice și de comunicații si informaţiilor procesate, stocate și transmise în acestea;
- identifică nevoile de instruire, pregătire și de conștientizare privind securitatea informatică/ cibernetică şi instruieşte/ pregăteşte angajaţii în privinţa aplicării măsurilor preventive şi de limitare a ameninţărilor de securitate;
- ţine evidenţa riscurilor la care este supus sistemul informatic al organizaţiei, ce reies din următoarele surse: securitatea aplicaţiilor, rezultatele auditurilor interne şi externe şi din fişele de incidente de securitate informatică;
- realizează auditurile legate de aplicarea politicilor și procedurilor de securitate a informaţiilor prelucrate, stocate și transmise în sistemele informatice și de comunicații;
- propune planul anual de evaluare/ testare a utilizatorilor autorizați ai sistemului informatic și de comunicații;
- asigură monitorizarea tehnologică privind securitatea informaţiilor prelucrate, stocate și transmise în sistemele informatice și de comunicații (evaluând noile ameninţări, bunele practice, etc.).

5.1.4. Responsabilul IT&C/ Administratorul SIC (angajați ai societății sau ai unui furnizor de servicii IT&C) au următoarele responsabilități:

- propune modificări ale politicilor legate de IT&C și procedurilor aferente acesteia;
- tratează incidentele de securitate în scopul minimizării efectului distructiv al
- acestora asupra resurselor informatice și de comunicaţii;
- informează conducerea în caz de incidente, intervenție și rezolvarea incidentelor de securitate a informațiilor;
- asigură existenţa jurnalelor şi a traseelor auditării pentru orice tip de acces în sistem conform procedurilor asociate;
- planifică, implementează și verifică soluțiile de securitate a informațiilor: server antivirus, firewall, server de actualizări de securitate, backup, acces securizat la camera tehnică, asigurare aer condiționat, asigurare alimentare cu energie electrică/UPS;
- menține înregistrări privind configurația, aplicațiile și serviciile instalate, pentru a se putea reface sistemul în caz de dezastru;
- inventariază periodic aplicațiile și serviciile instalate și verifică dacă sunt autorizate;

- administrează sistemele IT&C și aplică măsurile de securitate și alte cerințe ale programului de securitate a informațiilor pentru sistemele informatice pentru care are atribuită responsabilitatea.

5.1.5. Șefii structurilor/ entităților organizatorice au următoarele responsabilități:

- implementarea politicilor si procedurile de securitate a informațiilor;
- instruirea personalului din subordine cu privire la cerințele legate de securitatea informațiilor aplicabile pentru fiecare loc de muncă;
- asigurarea că măsurile de securitate tehnice, fizice și procedurale adecvate sunt implementate în conformitate cu politicile și procedurile de securitate și sunt aplicate în mod corespunzător și de către tot personalul;
- asigurarea resurselor și efectuarea analizelor necesare pentru a se asigura că informațiile și activele informaționale sunt protejate în mod corespunzător în zona lor de responsabilitate;
- informarea persoanei desemnate cu managementul incidentelor de securitate despre încălcările reale sau presupuse ale politicilor de securitate care afectează securitatea informațiilor din zona lor de responsabilitate (incidentele de securitate a informațiilor);
- identificarea și clasificarea informațiilor și activelor informaționale semnificative din zona lor de responsabilitate și desemnarea deținătorilor (responsabililor) pentru acestea;
- informarea Responsabilului IT&C la schimbarea responsabililor de active informaționale.

5.1.6. Personalul societății:

- respectă toate politicile și procedurile privind securitatea informațiilor aplicabile pentru locurile lor de muncă;
- participă la instruirile legate de securitatea informațiilor;
- sunt responsabili pentru menținerea securității si confidenţialităţii tuturor informațiilor încredințate;
- informează șefii entităților organizatorice despre încălcările reale sau presupuse ale politicilor de securitate și confidenţialitate a datelor din zona lor de responsabilitate (incidente privind securitatea sau confidenţialitatea datelor).

5.1.7. Colaboratorii și angajații furnizorilor de servicii au următoarele responsabilități:

- respectă toate politicile și procedurile privind securitatea informațiilor și de protecție a datelor aplicabile pentru informațiile la care au acces;
- răspund direct de securitatea și conţinutul informaţiilor şi resursele informatice și de comunicații încredinţate direct sau indirect;
- informează persoanele de contact despre încălcările reale sau presupuse ale securităţii sau confidenţialităţii datelor;
- returnează informațiile încredințate în momentul încheierii relației contractuale sau în momentul solicitării returnării acestora de către organizaţie.

5.2. POLITICĂ

5.2.1. Declarație

Informațiile în format olografic, letric sau electronic utilizate în activitățile desfășurate în cadrul APAVIL S.A. sunt proprietatea acestuia și reprezintă bunuri strategice care trebuiesc administrate ca atare.

Compromiterea securității acestor resurse poate afecta capacitatea APAVIL S.A. privind furnizarea de servicii, de calitate, și poate conduce la producerea de fraude, incidente legate de confidenţialitatea informațiilor, distrugerea informațiilor, violarea unor clauze contractuale sau afectarea prestigiului și credibilității organizației în fața clienților, propriilor angajați, precum și în fața partenerilor și colaboratorilor săi.

5.2.2. Clasificarea informaţiilor

Clasificarea informaţiilor este necesară pentru a permite atât alocarea resurselor necesare protejării acestora, cât și pentru a determina pierderile potenţiale ca urmare a modificărilor, pierderii/ distrugerii sau divulgării acestora.

Informaţiile clasificate (definite de lege) sunt informaţiile, datele, documentele de interes pentru securitatea naţională, care, datorită nivelurilor de importanţă şi consecinţelor care s-ar produce ca urmare a dezvăluirii sau diseminării neautorizate, trebuie să fie protejate.

Informaţiile clasificate se împart în:

- Informaţii clasificate **secrete de stat** şi
- Informaţii clasificate **secrete de serviciu**.

Conform legii, conducătorii persoanelor juridice de drept public sau privat sunt abilitaţi să stabilească informaţiile care constituie secrete de serviciu, precum şi regulile de protecţie a acestora şi, totodată, să coordoneze şi să controleze măsurile privitoare la protecţia acestora, în conformitate cu normele stabilite prin Hotărâre a Guvernului.

Legea interzice clasificarea ca secrete de serviciu a informaţiilor care, prin natura sau conţinutul lor, sunt destinate să asigure informarea cetăţenilor asupra unor probleme de interes public sau personal, respectiv a celor de natură să favorizeze ori să acopere eludarea legii sau obstrucţionarea justiţiei.

În acest sens, managementul APAVIL S.A. este responsabil de evaluarea periodică a schemei de clasificare a informaţiilor, de stabilirea regulilor de protecţie, precum şi de coordonarea şi controlul măsurilor privitoare la protecţia acestora, în conformitate cu normele stabilite prin Hotărâre de Guvern.

Informaţiile clasificate **Secrete de serviciu** se referă la acele activităţi, date și informații care, fără a constitui, în înţelesul legii, secrete de stat, nu trebuie cunoscute decât pentru îndeplinirea atribuţiilor de serviciu, divulgarea lor putând prejudicia interesul societății.

Pentru informațiile clasificate **"Secrete de serviciu"** persoanele abilitate să atribuie informaţiilor această clasă, sunt conducătorii persoanelor juridice, precum şi alte persoane împuternicite de către aceştia.

5.2.2.1. Informaţiile clasificate deținute/ gestionate de APAVIL S.A.

Informațiile clasificate naționale (în înțelesul legii), deținute/ gestionate de APAVIL S.A. parțin următoarelor **clasele de secretizare**, respectiv:

- **Secret de serviciu**
- **Nesecret**
- **Confidențial** (conf. GDPR)

5.2.2.2. Informațiile SECRETE DE SERVICIU, deținute/gestionate de APAVIL S.A., sunt grupate în următoarele categorii:

- Informaţii puse la dispoziţie de către diverse instituții ale statului, precum și de către beneficiarii sau furnizorii/ subcontractorii, în cadru contractual, pe proiecte clasificate Secret de serviciu;
- Informaţii produse de APAVIL S.A. pentru diverse instituții ale statului, pentru beneficiarii sau furnizorii/subcontractorii, în cadru contractual, pe proiecte clasificate Secret de serviciu;
- Informaţii referitoare la sistemul de protecţie a informaţiilor secrete de serviciu deținute/gestionate de/în APAVIL S.A.;
- Informaţii referitoare la unele activităţi ale APAVIL S.A., stabilite de Conducerea societății, în acord cu H.G. nr.781/2002 şi Legea 544/2001.

5.2.2.3. Informațiile NESECRETE, deținute/gestionate de APAVIL S.A., sunt grupate în următoarele categorii:

- Informaţii puse la dispoziţie de către diverse instituții ale statului, precum și de către beneficiarii sau furnizorii / subcontractorii, în cadru contractual;
- Informaţii produse de APAVIL S.A. pentru diverse instituții ale statului, sau pentru beneficiarii sau furnizorii/ subcontractorii, în cadru contractual;
- Informaţii schimbate cu diverşi parteneri, in cadru contractual sau în afara acestuia;
- Informaţii nedestinate publicităţii, referitoare la unele activităţi ale APAVIL S.A., stabilite de managementul societății, în acord cu Legea 544/2001, privind liberul acces la informații publice.
- Informaţii care pot fi făcute publice, referitoare la activităţile curente ale APAVIL S.A., dar numai cu avizul prealabil al Conducerii societății (directorului general sau al persoanei desemnate/ împuternicite de acesta, în acest sens).

5.2.2.4. Alte informații clasificate (*altele decât cele clasificate ca fiind informații secrete de stat sau* ***Secrete de serviciu*** *sau* ***Nesecrete***):

APAVIL S.A. mai poate deține/ gestiona și alte informații clasificate, dar clasificarea acestora se face fie conform cerințelor interne ale societății, fie cerințelor entităților emitente. Aceste informații se pot regăsi într-una din următoarele clase/ categorii:

- cu **Regim Special**,
- **Secrete Comerciale**,
- **Confidențiale** sau
- de **Uz intern**.

5.2.3. Securitatea fizică şi a mediului de lucru

Prelucrările/ generarea de date și informații, precum și echipamentele de prelucrare a datelor și informaţiilor, importante sau sensibile, trebuie desfășurate sau amplasate în zone sigure, protejate de un perimetru de securitate definit (și marcat/ semnalizat ca "ZONĂ

ADMINISTRATIVĂ"). Ele trebuie protejate fizic împotriva accesului neautorizat, deteriorărilor și intervenţiilor.

Protecţia fizică este realizată prin crearea uneia sau mai multor bariere fizice în jurul incintelor APAVIL S.A., în interiorul societății precum și în locația sistemelor de prelucrare a informaţiilor. Folosirea barierelor multiple oferă o protecţie suplimentară, în sensul că eşecul unei singure bariere nu înseamnă compromiterea imediată a securităţii.

APAVIL S.A. aplică măsuri de protecţie fizică și împotriva incendiilor, inundaţiilor și a oricăror alte forme de dezastre naturale sau produse de oameni.

Toate utilităţile suport, precum electricitatea, încălzirea/ ventilaţia sau aerul condiţionat sunt dimensionate corespunzător sistemelor pe care le servesc. Utilităţile suport sunt verificate şi testate, cu regularitate, pentru a se asigura buna lor funcţionare şi pentru a se reduce riscul funcţionărilor incorecte sau al defectărilor.

Informații suplimentare despre securitatea fizică şi a mediului de lucru pot fi găsite în Procedura privind securitatea fizică şi a mediului de lucru.

5.2.4. Securitatea resurselor umane

APAVIL S.A. trebuie să aplice măsuri astfel încât angajații, colaboratorii și angajații furnizorilor de servicii:

- să înţeleagă responsabilităţile care le revin și să fie corespunzători pentru rolurile alocate;
- să reducă riscul de furt, fraudă sau de folosire necorespunzătoare a activelor folosite la prelucrarea datelor;
- să fie pregătiţi să susţină și să aplice Politica de securitate a APAVIL S.A. pe durata contractului de muncă sau a contractului în baza căruia au acces la informații;
- să fie pregătiţi să susţină și să aplice politica de securitate a APAVIL S.A. pe durata contractului de muncă sau a contractului în baza căruia au acces la informații;
- să părăsească APAVIL S.A. sau să-și schimbe locul de muncă într-o manieră reglementată.

Detalii despre măsurile adoptate în cazul resurselor umane vor fi găsite în Procedura privind securitatea resurselor umane.

5.2.5. Securitatea documentelor utilizate

Angajații, colaboratorii și angajații furnizorilor de servicii care utilizează documente în format ograf, letric sau pe suport electronic conținând informații confidențiale (inclusiv date cu caracter personal) sau secrete aparţinând APAVIL S.A., trebuie să le protejeze în mod adecvat împotriva accesului neautorizat atunci când nu le utilizează sau le lăsă nesupravegheate.

Detalii despre măsurile de securitate aplicate în cazul documentelor utilizate pot fi găsite în **Normele interne privind Managementul și Protecția documentelor clasificate.**

5.2.6. Securitatea IT&C

O mare parte din datele create, colectate sau stocate se bazează pe utilizarea resurselor informatice și de comunicații ale APAVIL S.A. Organizația investește substanţial în resursele sale umane și echipamentele IT&C pentru a putea asigura integritatea, confidenţialitatea şi disponibilitatea informațiilor și a sistemelor informatice și de aceea aceste resurse trebuie utilizate și administrate corespunzător.

Integritatea, confidenţialitatea şi disponibilitatea acestor resurse este obţinută prin implementarea unui set adecvat de mijloace de control, incluzând politici, proceduri, procese, aplicații software şi echipamente hardware.Astfel, sunt aplicate măsuri în vederea:

- administrării conturilor de acces la date, sistemelor informatice și site-urilor web;
- administrării accesului administrativ la sistemele informatice și la reţeaua de comunicaţii;
- gestionării aplicaţiilor ce se pot utiliza în cadrul societății;
- configurării sistemelor informatice ce accesează reţeaua de comunicaţii;
- securizării serverelor și a dispozitivelor de stocare a datelor;
- gestionării back-up-urilor şi arhivelor;
- utilizării corespunzătoare a echipamentelor;
- detectării accesului neautorizat;
- gestionării modificărilor efectuate echipamentelor;
- asigurării securităţii echipamentelor și resurselor scoase în afara societății;
- utilizării echipamentelor proprietate personală;
- utilizării corespunzătoare a reţelelor Intranet și Internet;
- gestionării mijloacelor de comunicaţie puse la dispoziţia angajaţilor și colaboratorilor;
- gestionării site-urilor web aparţinând APAVIL S.A.;
- detectării virușilor;
- asigurării securităţii în cazul accesului de la distanță;
- asigurării managementului incidentelor de securitate.

Detalii despre măsurile de securitate aplicate resurselor IT&C vor fi găsite în **Politica IT&C** și în procedurile aferente acesteia.

5.2.7. Protecția datelor cu caracter personal

Protecția datelor personale este o componentă importantă a oricărei activități, astfel că toate informațiile trebuie să fie prelucrate în siguranță și în conformitate cu politica stabilită în acest sens. Pe lângă bunele practici stabilite la nivelul societății, anumite categorii de date sunt supuse şi reglementărilor legislației naţionale și este vital ca personalul să recunoască toate detaliile legate de manipularea informațiilor și datelor APAVIL S.A.

Respectarea cerințelor legate de protecția datelor cu caracter personal este responsabilitatea tuturor membrilor APAVIL S.A. Orice încălcare deliberată a acestei politici poate conduce la măsuri disciplinare, la retragerea accesului la resursele informaționale ale APAVIL S.A. sau chiar la urmărirea penală.

Informații suplimentare despre protecția datelor cu caracter personal pot fi găsite în **Politica privind protecția datelor cu caracter personal** și în procedurile aferente acesteia.

5.2.8. Conștientizare și instruire cu privire la securitatea informației

Toți angajații APAVIL S.A., colaboratorii sau angajații furnizorilor de servicii trebuie să fie conștientizați sau instruiți cu privire a politicile și procedurile organizaționale corespunzătoare fiecarui loc de muncă sau activități desfășurate.

În acest scop, șefii entităților organizatorice trebuie să stabilească un **Program de instruire, pregătire și conștientizare a personalului** din subordine cu privire la cerințele legate de securitatea informațiilor aplicabile pentru fiecare loc de muncă sau activități desfășurate.

Detalii suplimentare în **Procedura privind pregătirea, instruirea și conștientizarea utilizatorilor SIC.**

5.2.9. Relațiile cu furnizorii

Unele din activităţile desfășurate în cadrul APAVIL S.A. sunt realizate de către furnizori de servicii. În acest caz, APAVIL S.A. recurge doar la furnizori de servicii care oferă garanții suficiente pentru punerea în aplicare a măsurilor tehnice şi organizatorice prevăzute de politica de securitate și de politicile și procedurile asociate acesteia.

Activitatea desfășurată de către un furnizor de servicii trebuie reglementată printr-un contract sau alt act juridic (conform legislației în vigoare, o **Anexă de securitate** la **Contract**) care are caracter obligatoriu pentru furnizorul de servicii şi care trebuie să stabilească cel puţin durata desfășurării activităţilor, natura activităţilor desfășurate şi măsurile de securitate, tehnice şi organizatorice ce trebuie implementate de furnizor sau respectate de către angajaţii furnizorului de servicii.

Detalii despre măsurile de securitate aplicate în cazul relaţiilor cu furnizorii vor fi găsite în Procedura privind Relațiile cu furnizorii.

5.2.10. Măsuri disciplinare

Toți angajații APAVIL S.A., colaboratorii sau angajații furnizorilor de servicii sunt obligați să respecte această politică de securitate a informațiilor precum și politicile și procedurile asociate acesteia.

Încălcarea prevederilor politicii de securitate a informațiilor sau a politicilor și procedurilor asociate acesteia poate face obiectul unor măsuri disciplinare, civile, contravenţionale ori penale, în raport cu gravitatea faptei săvârșite.