UZINA DE CONSTRUCŢII MAŞINI HIDROENERGETICE S.R.L., cu Sediul social în strada Golului, nr. 1, cod 320053, localitatea Reşiţa, judeţul Caraş - Severin, înregistrată la Oficiul Registrului Comerţului sub nr. J2024000097110, Cod Unic de Înregistrare 49594720

Cont IBAN RO63BTRLRONCRT0682536501

Politica Uzinei de Construcții Mașini Hidroenergetice SRL privind Securitate a informației

CUPRINS

1. Preambul și Scop

Uzina de Construcții și Mașini Hidroenergetice Reșița S.R.L. (UCMH), în calitate de infrastructură națională în domeniul producției de echipamente pentru hidroenergie, își asumă responsabilitatea protejării tuturor informațiilor și sistemelor informatice. Prezenta politică are drept scop **asigurarea confidențialității, integrității și disponibilității** informațiilor UCMH, precum și menținerea unui nivel ridicat de securitate cibernetică, în condițiile unui risc acceptat de conducerea companiei. Politica stabilește cadrul general pentru guvernanța securității informației în UCMH, definind cerințele și măsurile necesare inițierii, implementării, menținerii și îmbunătățirii sistemului de management al securității informației.

Elaborare în conformitate cu legislația și standardele aplicabile: Această politică este elaborată în concordanță cu legislația națională și europeană, precum și cu standardele de securitate recunoscute, inclusiv, dar fără a se limita la:

- **Legea nr. 182/2002** privind protecția informațiilor clasificate și **H.G. nr. 585/2002** (Standardele naționale de protecție a informațiilor clasificate) – care reglementează clasificarea și protecția informațiilor de importanță pentru securitatea națională;

- **Ordonanţa de urgenţă nr. 155/2024** privind instituirea unui cadru pentru securitatea cibernetică a reţelelor şi sistemelor informatice din spaţiul cibernetic naţional civil (transpunerea Directivei NIS2), precum și **Legea nr. 58/2023** privind securitatea și apărarea cibernetică a României;

- **Ordinul SGG nr. 1323/2020** pentru aprobarea Normelor tehnice privind cerințele minime de securitate IT aplicabile operatorilor de servicii esențiale;

- **Regulamentul UE 2016/679 (GDPR)** privind protecția datelor cu caracter personal și **Legea nr. 190/2018** de aplicare a GDPR în România;

- Legislația privind protecția informațiilor comerciale nedivulgate (**OUG nr. 25/2019** privind protecția know-how-ului și a secretelor comerciale și Legea nr. 11/1991 privind combaterea concurenței neloiale);

- **Normele de guvernanță corporativă** aplicabile companiilor de stat (inclusiv OUG nr. 109/2011 privind guvernanța corporativă a întreprinderilor publice și reglementările interne Hidroelectrica în calitate de acționar);

- **Standardul internațional ISO/IEC 27001:2018** pentru sistemele de management al securității informației, precum și bunele practici recunoscute în domeniu.

Obiectivele politicii: UCMH urmărește, prin implementarea acestei politici, protejarea tuturor activelor informaționale și a rețelelor IT/OT (tehnologia informației și tehnologia operațională) folosite în activitatea sa de producere de echipamente hidroenergetice. Politica își propune prevenirea accesului neautorizat, a scurgerii de informații și a incidentelor de securitate, asigurând în același timp respectarea obligațiilor legale și continuitatea activităților esențiale. De asemenea, politica stabilește responsabilitățile personalului și mecanismele de control pentru a garanta că **riscurile de securitate sunt reduse la un nivel acceptabil**, iar cerințele operaționale, așteptările clienților și conformitatea legală sunt îndeplinite.

2. Domeniul de Aplicare și Categoriile de Informații

Domeniul de aplicare: Politica se aplică tuturor angajaților UCMH, personalului contractual, partenerilor și oricăror terțe părți care au acces la informațiile, sistemele sau rețelele UCMH, indiferent de forma acestora (electronică, pe hârtie sau verbală). Toate departamentele și filialele UCMH au obligația de a respecta prezenta politică. Politica acoperă atât informațiile **neclasificate** (inclusiv cele de interes public și cele cu caracter confidențial intern sau comercial), cât și **informațiile clasificate** (conform legislației privind informațiile clasificate). UCMH se angajează să comunice această politică întregului personal, documentul fiind disponibil intern; fiecare angajat cu funcție de conducere, precum și fiecare membru al conducerii, este obligat să ia la cunoștință prevederile politicii și să semneze de luare la cunoștință și conformare. De asemenea, orice persoană externă (ex.: angajați ai clienților, furnizori, colaboratori) care accesează informații **nepublice** aparținând UCMH, în formă scrisă sau electronică, trebuie să fie informată despre prevederile prezentei politici și să semneze acorduri de confidențialitate, asumându-și respectarea acestor reguli.

Categoriile de informații gestionate în cadrul UCMH se clasifică, în funcție de sensibilitate și regimul juridic aplicabil, după cum urmează:

- **Informații publice:** Date și informații destinate difuzării publice sau care, prin natura lor, nu necesită protecție specială. Conform legii, accesul la informațiile de interes public este garantat oricărui cetățean. Exemple: comunicate de presă, rapoarte anuale publice, informații publicate pe website-ul companiei.

- **Informații interne și comerciale confidențiale:** Date neclasificate, dar care aparțin UCMH și a căror divulgare neautorizată ar putea afecta interesele comerciale, financiare sau reputația companiei ori ar încălca obligațiile de confidențialitate față de parteneri. Acestea includ *secretele comerciale* (know-how, planuri de afaceri, date

tehnice proprietare, oferte, contracte, strategii etc.), protejate prin legislația comercială și clauze contractuale. Divulgarea, accesarea sau utilizarea ilegală a secretelor comerciale este interzisă și sancționată conform OUG 25/2019 și Legii 11/1991. Toate informațiile interne nepublice sunt tratate ca **„confidențiale – uz intern”** în absența unei clasificări superioare.

- **Informații cu caracter personal:** Date referitoare la o persoană fizică identificată sau identificabilă (angajați, clienți, parteneri) gestionate de UCMH în desfășurarea activității sale. Prelucrarea acestor date se va face în conformitate cu GDPR și Legea 190/2018, asigurând respectarea principiilor de legalitate, echitate, transparență, minimizare a datelor, integritate și confidențialitate. Vor fi aplicate măsuri tehnice și organizatorice adecvate pentru protecția datelor cu caracter personal (ex.: pseudonimizare, criptare, control de acces), iar angajații vor respecta procedurile interne privind protecția datelor. UCMH are desemnat un **Responsabil cu Protecția Datelor (DPO)**, conform art. 37 GDPR, care supraveghează conformitatea cu reglementările de protecție a datelor.

- **Informații clasificate:** Date și documente care, potrivit Legii 182/2002, sunt încadrate într-un nivel de secretizare deoarece dezvăluirea lor neautorizată ar putea aduce prejudicii securității naționale sau intereselor organizației. Conform legii, informațiile clasificate se împart în: **secrete de stat** și **secrete de serviciu**, în funcție de importanța pentru securitatea națională și consecințele divulgării. La rândul lor, secretele de stat sunt pe niveluri: *Strict Secret de Importanță Deosebită*, *Strict Secret* și *Secret*, echivalente cu nivelurile NATO “Top Secret”, “Secret” și “Confidential”. Informațiile *Secret de serviciu* (NATO “Restricted”) reprezintă date a căror divulgare neautorizată poate prejudicia interesele legale ale unei persoane juridice publice sau private. UCMH va clasifica și marca explicit orice informație proprie ce intră sub incidența acestor categorii, conform reglementărilor în vigoare, și va gestiona aceste informații cu un nivel sporit de securitate, conform cerințelor legale (vezi Secțiunea 5).

Notă: *În caz de dubiu privind categoria unei informații, persoanele trebuie să consulte Responsabilul cu Securitatea Informației sau structura de securitate desemnată, pentru a decide clasificarea corespunzătoare. În toate situațiile, se aplică principiul precauției – informațiile se tratează la cel mai înalt nivel de protecție aplicabil până la clarificarea regimului lor.*

3. Principii generale ale securității informației

UCMH aderă la un set de **principii fundamentale de securitate a informației**, care ghidează toate politicile și procedurile specifice:

- **Confidențialitate, Integritate, Disponibilitate (Triada CID):** Orice sistem sau proces implementat trebuie să asigure că informațiile sunt accesibile *doar persoanelor autorizate* (confidențialitate), sunt *corecte și complete* și nu au fost modificate neautorizat (integritate), și sunt *disponibile la timp* pentru utilizare de către persoanele autorizate atunci când este necesar (disponibilitate). Aceste obiective se aplică atât datelor stocate, cât și celor în tranzit sau prelucrate, și stau la baza tuturor celorlalte măsuri de securitate.

- **Respectarea cadrului legal și contractual:** Securitatea informației se realizează cu stricta respectare a legilor aplicabile (enumerate în Preambul) și a obligațiilor contractuale asumate de UCMH față de parteneri sau autorități. Nicio prevedere din această politică nu va fi interpretată într-un mod care să limiteze accesul legal la informațiile de interes public sau să contravină drepturilor și libertăților fundamentale. De asemenea, UCMH asigură conformitatea cu cerințele impuse operatorilor de servicii esențiale (conform legislației NIS2) și cu standardele corporative stabilite de acționariat.

- **Responsabilitatea și *need-to-know*:** Accesul la informații și sisteme este acordat exclusiv în baza necesității de a cunoaște, raportat la sarcinile de serviciu. Fiecare angajat are responsabilitatea de a proteja informațiile pe care le gestionează și de a respecta măsurile de securitate. Conducerea companiei asigură suportul necesar (resurse, training, structură organizatorică) pentru implementarea politicii, iar *cultura de securitate* este promovată la toate nivelurile. Orice încălcare a politicii sau incident de securitate va fi raportat fără întârziere și tratat cu maximă seriozitate.

- **Abordarea bazată pe risc:** Măsurile de securitate sunt implementate proporțional cu nivelul de risc și valoarea informațiilor protejate. UCMH aplică un proces continuu de evaluare a riscurilor de securitate, identificând amenințările și vulnerabilitățile relevante, și tratează riscurile prin măsuri de prevenire, detectare, răspuns și recuperare adecvate. Se urmărește reducerea riscurilor la un nivel acceptabil pentru organizație, în conformitate cu apetitului la risc stabilit de management.

- **Îmbunătățire continuă și *compliance*:** Sistemul de management al securității informației este supus unui proces de monitorizare, audit intern și revizuire periodică (vezi Secțiunea 11), pentru a asigura eficacitatea sa și adaptarea la evoluția amenințărilor, a tehnologiei sau a cerințelor de reglementare. UCMH se angajează să actualizeze anual prezenta politică și procedurile aferente, sau ori de câte ori intervin

schimbări semnificative de risc ori legislative. Orice neconformitate sau deficiență identificată va fi corectată prompt, iar lecțiile învățate din incidente vor conduce la îmbunătățirea măsurilor existente.

4. Niveluri de clasificare și tratament al informațiilor

Pentru a implementa în practică principiile de confidențialitate, integritate și disponibilitate, UCMH folosește un **sistem de clasificare internă a informațiilor și sistemelor** bazat pe niveluri de impact (denumit *CIS 1–5*). Fiecărei informații sau aplicații i se evaluează cerințele de securitate pe dimensiunile confidențialitate, integritate și disponibilitate, pe o scară de la **1 (impact minim/neglijabil)** până la **5 (impact foarte mare/catastrofal)**. Astfel, clasificarea *CIS 1–5* reflectă gradul de sensibilitate și criticitate al informației:

- **CIS 1 (Nivel Nesemnificativ):** Informații publice sau non-critice, a căror compromitere nu ar produce niciun prejudiciu organizației. Confidențialitatea nu este necesară (date publice), integritatea și disponibilitatea nu sunt critice. *Exemplu:* date de pe site-ul public, anunțuri deja făcute publice.

- **CIS 2 (Nivel Scăzut):** Informații interne curente, a căror divulgare ar avea un impact redus. Integritatea și disponibilitatea sunt importante dar o întrerupere pe termen scurt este tolerabilă. *Exemplu:* comunicări interne generale, proceduri de lucru non-sensibile.

- **CIS 3 (Nivel Moderat):** Informații confidențiale de afaceri sau sisteme de importanță medie. Necesită un grad ridicat de confidențialitate (de ex. date financiare preliminare, oferte în curs), integritate bună și disponibilitate rezonabilă. Compromiterea ar putea produce pierderi financiare limitate sau afectarea moderată a reputației. *Exemplu:* baza de date cu clienți obișnuiți, rapoarte financiare interne, e-mail-uri corporative.

- **CIS 4 (Nivel Ridicat):** Informații foarte sensibile sau sisteme critice de producție. Confidențialitatea este esențială (de ex. planuri strategice, proiecte tehnice proprietare), integritatea datelor trebuie menținută absolut, iar disponibilitatea sistemelor este critică pentru operațiuni. Compromiterea ar provoca prejudicii serioase, financiare sau de imagine, și/sau ar putea afecta continuitatea activității. *Exemplu:* planuri de investiții, date tehnice despre echipamente hidroenergetice critice, sistemul de control industrial (SCADA) al uzinei.

- **CIS 5 (Nivel Foarte Ridicat/Critic):** Informații de importanță națională (inclusiv **informații clasificate secret de stat**) sau sisteme a căror indisponibilitate/arhivare ar avea consecințe catastrofale. Necesită cel mai înalt nivel de securitate pe toate dimensiunile – acces extrem de restricționat, integritate verificată riguros, disponibilitate permanentă (fără întreruperi). *Exemplu:* documente clasificate **Strict**

Secret de Importanță Deosebită, date privind securitatea fizică a hidrocentralelor majore, chei criptografice root ale sistemelor de comandă. Compromiterea unor astfel de informații ar amenința direct securitatea națională sau siguranța populației.

Tratamentul în funcție de clasificare: Pentru fiecare nivel CIS sunt definite controale de securitate adecvate. În general, cu cât nivelul este mai ridicat, cu atât **măsurile de protecție** vor fi mai stricte (vezi Secțiunile 5 și 6): de la politici standard de parolare și backup-uri (nivel 2-3) până la criptare robustă, sisteme dedicate izolate și verificări de background ale personalului (nivel 4-5). **Informarea utilizatorilor** despre nivelul de clasificare se face prin marcaje pe documente (ex. "Confidențial – Intern", "Secret de serviciu – UCMH") sau prin etichete în sistemele informatice. Orice document sau fișier care conține date sensibile va avea inscripționat nivelul de clasificare și restricția de diseminare aferentă.

Pentru **informațiile clasificate** conform legii (Secret de Stat sau de Serviciu), tratamentul va respecta cerințele legale specifice acelui nivel (vezi Secțiunea 5 pentru măsuri detaliate). Informațiile *Secret de Stat* (SSID, Strict Secret, Secret) vor fi încadrate automat la nivelul intern CIS 5 și supuse tuturor măsurilor maxime de securitate, iar cele *Secret de Serviciu* cel puțin la nivel CIS 4. Documentele clasificate vor fi gestionate separat de cele neclasificate, conform principiului compartimentării, și vor fi înregistrate, depozitate, copiate, transportate și distruse doar în condițiile permise de lege.

5. Măsuri de Protecție Fizică și Electronică pentru Informații Clasificate și Neclasificate

UCMH implementează un set complet de **măsuri de securitate fizică și cibernetică**, adaptate în funcție de nivelul de clasificare al informației (conform Secțiunii 4). Aceste măsuri urmăresc prevenirea accesului fizic sau electronic neautorizat, protejarea împotriva divulgării accidentale sau deliberate a datelor și asigurarea continuității operațiunilor chiar și în situații de incident sau dezastru.

5.1. Protecția fizică a informațiilor și echipamentelor

- **Zone de securitate și controlul accesului fizic:** UCMH definește *zone de securitate delimitate* în incinta sa (birouri, arhive, hale de producție IT/OT) în care sunt gestionate informații sensibile sau clasificate. Aceste zone sunt marcate și protejate corespunzător (pereți rezistenți, uși securizate, grilaje, folie anti-vizibilitate etc.), iar accesul este permis doar persoanelor autorizate, pe baza de legitimații, cartele magnetice sau sisteme biometrice, conform principiului *need-to-know*. Zonele unde se lucrează cu **informații clasificate** (ex.: biroul structurii de securitate, camera documentelor clasificate) sunt amenajate și autorizate conform standardelor naționale – perimetru clar determinat, cu

acces restricționat, registre de intrare-ieșire și supraveghere video. Personalul care intră în aceste zone este limitat și supus procedurilor de verificare de securitate (certificat ORNISS pentru acces la secret de stat, de exemplu).

- **Depozitarea documentelor și mediilor de stocare:** Documentele pe hârtie și mediile de stocare (CD, USB, HDD) ce conțin informații **clasificate** sau **confidențiale** sunt ținute în fișiere securizate (fișete metalice încuiate, seifuri certificate pentru nivelul de clasificare corespunzător). Cheile/codurile acestor seifuri sunt gestionate strict, cu evidența persoanelor care le dețin. Pentru informațiile clasificate, se aplică cerințele H.G. 585/2002 privind păstrarea în *fișete de securitate* (clasificate conform nivelului – de ex. fișet clasei A pentru SSID). Accesul la fișierele clasificate este permis doar personalului avizat, și orice consultare se notează în registrul de evidență a documentelor clasificate. Documentele *Secret de Serviciu* pot fi stocate în dulapuri încuiate la birouri cu acces controlat, iar cele *confidențiale interne* în sertare sau dulapuri închise, pentru a preveni accesul întâmplător.

- **Securitatea perimetrului și supraveghere:** Clădirile UCMH sunt dotate cu sisteme de alarmă anti-efracție și control perimetral. Există personal de pază sau contractori de securitate care supraveghează intrările, verifică identitățile vizitatorilor și patrulează zonele sensibile. Sistemele CCTV (circuite de televiziune închise) monitorizează punctele de acces și zonele critice (server rooms, arhive), imaginile fiind înregistrate și păstrate o perioadă determinată, în conformitate cu legislația. În zonele unde se lucrează cu *informații secrete*, se evită instalarea camerelor interioare pentru a preveni captarea accidentală a documentelor, dar sunt supravegheate intrările.

- **Protecția contra incendiilor și dezastrelor:** Arhivele de documente și serverele critice sunt echipate cu sisteme de detecție și stingere a incendiilor (ex. senzori de fum și instalații cu gaz inert pentru servere), precum și cu sisteme de control al mediului (HVAC) pentru prevenirea supraîncălzirii sau umidității excesive. Documentele clasificate de importanță majoră, dacă există, sunt duplicate și depozitate într-un loc separat de siguranță (un seif la altă locație sau la ORNISS, dacă impune legea). Planuri de protecție fizică includ proceduri pentru situații de urgență – evacuarea în siguranță a materialelor sensibile sau distrugerea lor controlată în caz de pericol iminent (conform principiului că, în situații extreme, protecția informațiilor clasificate primează).

5.2. Protecția electronică și cibernetică a informațiilor

- **Segmentarea și securizarea rețelelor:** Rețeaua informatică a UCMH este segmentată pe zone de securitate logică, separând sistemele în funcție de nivelul de clasificare și de

rol (ex.: rețeaua administrativă office, rețeaua de producție/SCADA, rețeaua pentru vizitatori etc.). Între aceste segmente sunt implementate firewall-uri de nouă generație, care filtrează traficul și permit doar comunicațiile strict necesare. Sistemele ce procesează informații **clasificate** sau date critice sunt izolate de rețeaua externă și de internet (*air-gap* sau prin diode de date unidirecționale), pe cât posibil, pentru a elimina vectorii de atac extern. Dacă este necesară transmiterea electronică a informațiilor clasificate, se utilizează canale criptate aprobate (ex.: echipamente și algoritmi de criptare certificați de autoritățile competente – STS/ORNISS).

- **Controlul dispozitivelor și al mediilor de stocare:** Pentru a preveni exfiltrarea sau introducerea neautorizată de date, porturile USB și unitățile optice ale calculatoarelor ce gestionează informații sensibile pot fi dezactivate sau controlate prin politici de grup. Doar dispozitive de stocare criptate și aprobate pot fi folosite pentru transferul de date confidențiale, cu evidența exactă a lor. În mediile clasificate, utilizarea oricăror dispozitive de înregistrare (telefoane mobile, camere foto, stick-uri USB neautorizate) este interzisă. Computerele din zonele clasificate sunt marcate distinct și au politici restrictive (fără conexiune internet dacă nu e absolut necesar, fără posibilitatea de a conecta echipamente auxiliare neautorizate).

- **Criptarea și protecția datelor în tranzit:** UCMH aplică metode criptografice pentru a proteja datele stocate și transmise. Documentele electronice cu informații **confidențiale** sau **personale** sunt păstrate, pe cât posibil, în formă criptată sau pe suporturi criptate (ex.: folosirea criptării full-disk la laptopuri, criptarea bazelor de date cu date personale). Pentru comunicațiile prin email, se folosește criptarea end-to-end sau cel puțin transmiterea fișierelor sensibile parolate, cu parole comunicate separat. Rețeaua internă folosește protocoale securizate (ex.: HTTPS, SSH, VPN IPsec pentru acces de la distanță) pentru a preveni interceptarea traficului. Cheile criptografice sunt gestionate centralizat, cu acces limitat la personal autorizat, și sunt rotite periodic conform politicii de criptografie.

- **Sisteme și aplicații securizate:** Toate serverele, stațiile de lucru și aplicațiile critice sunt configurate conform **principiului "secure by design"** și al cerințelor minime de securitate (conform Ordinului SGG 1323/2020). Sistemele de operare și software-ul sunt menținute la zi cu ultimele actualizări de securitate (*patch management* regulat), reducând expunerea la vulnerabilități cunoscute. Sunt dezactivate serviciile nefolosite și conturile implicite. Configurațiile sunt revizuite periodic prin audituri de vulnerabilitate, iar înainte de punerea în producție a noilor aplicații, se efectuează teste de securitate (ex.: teste de penetrare, code review) pentru a identifica și remedia eventuale breșe.

- **Back-up și recuperare în caz de dezastru:** Pentru a asigura disponibilitatea informațiilor esențiale, UCMH operează un sistem de backup periodic. Datele critice (financiare, proiecte tehnice, configurații SCADA etc.) sunt salvate conform unui calendar (zilnic, săptămânal), pe medii securizate, stocate off-site într-o locație securizată. Back-up-urile sunt criptate și verificate periodic prin exerciții de restaurare, asigurând că pot fi folosite în caz de incident (ex.: atac ransomware – vezi Secțiunea 7). Planul de **Continuitate a Afacerii și Recuperare la Dezastru** (BCP/DRP) este parte integrantă a politicii de securitate, definind proceduri clare pentru restaurarea operațiunilor în urma unor incidente majore, inclusiv ordinea de recuperare a sistemelor și comunicarea de criză.

6. Politici de acces, autentificare, control și jurnalizare

Controlul accesului la informațiile și sistemele UCMH este esențial pentru menținerea confidențialității și integrității. UCMH aplică **politici stricte de autentificare și autorizare**, precum și mecanisme de monitorizare a accesului, pentru a se asigura că doar personalul autorizat poate accesa resursele în limitele necesare funcției lor.

- **Administrarea identităților și controlul accesului:** Fiecărui utilizator (angajat sau terț autorizat) i se alocă o **identitate digitală unică** (nume de utilizator) în sistemele UCMH. Conturile de utilizator sunt gestionate centralizat de departamentul IT, urmând principiul *principle of least privilege* – fiecărui utilizator i se acordă doar permisiunile minime necesare îndeplinirii atribuțiilor de serviciu. Structura de roluri și grupuri de securitate reflectă organigrama și separarea atribuțiilor: de exemplu, personalul financiar nu are acces la sistemele tehnice de producție, iar personalul tehnic nu accesează datele HR. Orice acces la informații cu caracter personal sau date sensibile este permis doar persoanelor îndreptățite și, dacă legea cere, numai după semnarea unor acorduri de confidențialitate suplimentare.

- **Autentificare robustă:** Toate sistemele critice și conturile cu privilegii (ex.: administratori de sistem, conturi cu acces la date sensibile) folosesc mecanisme de autentificare puternică. Parolele trebuie să respecte politica de complexitate (lungime minimă, combinație de caractere, schimbare periodică la 90 de zile, interdicția reutilizării ultimelor parole etc.). Oriunde este posibil, se implementează **autentificarea multi-factor (MFA)** – combinând parola cu un al doilea factor, cum ar fi token hardware/software sau autentificare biometrică – în special pentru accesul remote la rețeaua UCMH sau accesul la aplicații cu date critice. Conturile de serviciu și cele partajate sunt limitate la minimum; dacă astfel de conturi există, parolele lor sunt stocate securizat și accesul la ele este jurnalizat și aprobat managerial.

- **Politica de parole și gestionarea sesiunilor:** Utilizatorii au obligația să-și păstreze credențialele secrete; este interzisă partajarea parolei sau folosirea contului altui utilizator. Sesiunile inactive se blochează automat după o perioadă prestabilită (ex.: 15 minute) pentru a preveni accesul neautorizat în absența utilizatorului. Sistemele sensibile afișează banner de avertizare la logare (interzicerea accesului neautorizat și monitorizarea). După un număr limitat de încercări eșuate de autentificare, conturile sunt blocate temporar pentru a preveni forțarea parolelor.

- **Controlul accesului la rețea și la aplicații:** Se utilizează liste de control al accesului (ACL) pe echipamentele de rețea pentru a restricționa accesul la segmente sensibile doar din anumite stații sau de către anumiți utilizatori. Aplicațiile critice (ERP, SCADA, sisteme financiare) au propriile mecanisme de autentificare și autorizare granulară: rolurile de aplicație sunt alocate în funcție de funcția utilizatorului, cu separarea obligațiilor (ex.: o persoană care inițiază o plată nu poate și să o autorizeze singură).

- **Jurnalizare și monitorizare:** Toate accesările resurselor critice sunt **jurnalizate (logate)** automat de sistemele IT. Se păstrează în jurnale evenimente precum autentificări (reușite și eșuate), acces la fișiere sensibile, modificări de configurație, operațiuni de administrare, transferuri de date importante etc. Jurnalele includ detalii ca identitatea utilizatorului, timestamp, adresa IP/stația de lucru, acțiunea întreprinsă și rezultatul. Aceste log-uri sunt protejate împotriva ștergerii sau modificării neautorizate (stocate centralizat pe un server de log-monitoring, cu acces restricționat la administratori autorizați). În plus, se implementează un **Sistem de Detecție și Răspuns la Intruziuni (SIEM/IDPS)** care analizează în timp real jurnalele critice, generând alerte în cazul detectării unor activități anormale sau care corespund unor semnături de atac cunoscute.

- **Revizuirea drepturilor și gestionarea ciclului de viață al accesului:** Accesul utilizatorilor este revizuit periodic (ex.: trimestrial) de către managerii de departament împreună cu echipa de securitate IT, pentru a se asigura că permisiunile sunt actuale și justificate. Orice modificare în statutul unui angajat (angajare, schimbare de rol, plecare din companie) declanșează un proces formal de actualizare a accesului: la plecare, conturile sunt **dezactivate sau șterse imediat**, cardurile de acces recuperate, parolele privilegiate schimbate dacă au fost cunoscute de persoana care pleacă, iar semnăturile digitale revocate. Angajaților transferați pe alte funcții li se ajustează drepturile în consecință, evitând acumularea nejustificată de privilegii.

Aceste controale de acces și autentificare, combinate cu măsurile de protecție din Secțiunea 5, asigură un mediu în care **doar persoanele autorizate pot accesa informațiile necesare, exact în măsura necesară și cu trasabilitate completă** a acțiunilor lor.

7. Mecanisme de protecție împotriva incidentelor cibernetice și hibride (inclusiv ransomware)

Având în vedere creșterea amenințărilor la adresa infrastructurilor critice, UCMH adoptă o strategie **proactivă și reactivă** pentru a preveni și a răspunde incidentelor de securitate cibernetică, inclusiv atacurilor de tip ransomware și amenințărilor hibride (combinație de acțiuni cibernetice cu acțiuni fizice sau de altă natură). Scopul este menținerea rezilienței companiei în fața atacurilor avansate și reducerea la minimum a impactului asupra operațiunilor esențiale.

Mecanisme proactive de apărare cibernetică:

- **Securitate perimetrală consolidată:** UCMH utilizează firewall-uri avansate și sisteme de prevenire a intruziunilor (IPS) la granița rețelei sale, configurate să blocheze trafic malițios cunoscut și tentative de acces neautorizat. Politicile firewall sunt actualizate constant, iar echipamentele de securitate sunt monitorizate prin *Security Operations Center (SOC)* intern sau externalizat, care urmărește alertele în timp real. Traficul către/dinspre internet este trecut prin *gateway-uri de securitate* care includ filtre anti-malware, anti-phishing și de control al conținutului, prevenind descărcarea de cod malitios și accesul la site-uri periculoase.

- **Protecție endpoint și actualizări de securitate:** Toate stațiile de lucru și serverele dispun de soluții endpoint de securitate (antivirus/antimalware cu EDR – Endpoint Detection & Response). Aceste soluții sunt configurate să se actualizeze automat (semnături de viruși la zi) și să scaneze fișierele în timp real, blocând și carantinând amenințările detectate. Sistemele sunt actualizate (patch-uri aplicate) într-un mod prompt, conform unui calendar bine definit, pentru a acoperi vulnerabilitățile cunoscute – o politică *zero-day patching* este promovată pentru vulnerabilitățile critice. În plus, se folosesc politici de *Application Whitelisting* în zonele critice – doar anumite aplicații certificate pot rula pe serverele SCADA, de exemplu, prevenind execuția codului necunoscut/rău intenționat.

- **Detectarea avansată a amenințărilor:** Pe lângă SIEM-ul menționat (vezi Secțiunea 6), UCMH implementează mecanisme precum *honeypots/honeynets* în rețea pentru a detecta comportamente ale atacatorilor și a le întări profilul. De asemenea, sunt folosite instrumente de monitorizare a integrității fișierelor pe serverele critice – orice modificare neautorizată a fișierelor de sistem sau configurație declanșează alerte (File

Integrity Monitoring). Pentru protecția sistemelor industriale (ICS), se monitorizează traficul de rețea industrială prin IDS specializate (care recunosc comenzi anormale pe protocoale industriale) și se izolează imediat componentele compromise.

- **Politica de *backup* și reziliență la ransomware:** Conștientă de riscul ridicat de ransomware, compania se bazează pe copiile de siguranță periodice (vezi Secțiunea 5.2) și păstrează **backup-uri offline** (deconectate de la rețea) ale datelor esențiale. În plus, se implementează soluții anti-ransomware ce monitorizează comportamentul (ex.: criptare bruscă a multor fișiere) și pot opri procesul suspect. Periodic, se efectuează exerciții de recuperare din backup a unor sisteme pentru a testa capacitatea de a relua activitatea în cazul în care un atac ransomware criptează sistemele primare.

- **Conștientizarea amenințărilor hibride:** UCMH recunoaște că un atac cibernetic sofisticat poate fi însoțit de acțiuni fizice (ex.: sabotaj al echipamentelor, întreruperea alimentării cu energie) sau de campanii de dezinformare. Prin urmare, planurile de securitate includ scenarii hibride: de exemplu, existența de *UPS* și generatoare pentru continuitatea alimentării serverelor și sistemelor de control în caz de pană de curent, sau verificarea identității personalului de mentenanță pentru a preveni infiltrarea de intruși care ar putea instala dispozitive malițioase în rețea.

Mecanisme reactive (managementul incidentelor):

- **Echipa de Răspuns la Incidente (CERT intern):** UCMH a desemnat o echipă internă de răspuns la incidente de securitate informatică, condusă de Responsabilul cu Securitatea IT, care include specialiști IT și reprezentanți ai managementului. Această echipă are proceduri documentate de **incident response** pentru diferite tipuri de incidente (malware, pierdere de date, acces neautorizat, atac DoS, compromise SCADA etc.). La primirea unei alerte de securitate, echipa evaluează gravitatea și impactul, izolează sistemele afectate (de ex., deconectează o stație infectată de la rețea), colectează dovezi (log-uri, fișiere suspecte) și începe remedierea. Există un *plan de comunicare* care stabilește pe cine anunță echipa și în ce ordine (managementul de vârf, departamente afectate, autorități – vezi Secțiunea 9).

- **Investigarea și atenuarea incidentelor:** În cazul unui incident cibernetic, prioritatea este *limitarea daunelor* și *recuperarea serviciilor*. De exemplu, în cazul unui ransomware care criptează un server, serverul este scos imediat din rețea, se trece la restaurarea din backup a datelor, iar copia compromisă este păstrată pentru analiză forenzică. Se aplică imediat *patch*-uri sau *workaround*-uri dacă incidentul a exploatat o vulnerabilitate, pentru a preveni recurența. Dacă un cont de utilizator este compromis, se resetează credențialele și se analizează log-urile pentru acțiunile efectuate de atacator

cu acel cont.

- **Colaborare cu autoritățile și specialiști externi:** UCMH cooperează strâns cu autoritățile competente în cybersecurity (DNSC, SRI etc., detaliat în Secțiunea 9) în cazul incidentelor majore sau cu potențial impact național. De asemenea, dacă este necesar, compania are contracte cu firme specializate de răspuns la incidente (CSIRT extern) care pot fi apelate pentru investigații avansate (analiză malware, eradicare). Orice incident care poate constitui infracțiune (ex.: atac provenit de la actori statali sau grupări de criminalitate organizată) va fi raportat organelor legii (ex.: către structurile de combatere a criminalității cibernetice din cadrul poliției sau către SRI dacă e vorba de securitatea națională).

- **Învățarea din incidente:** După rezoluția unui incident, echipa de răspuns efectuează o analiză post-incident (*post-mortem*). Se identifică cauzele principale, modul de operare al atacatorului și eficacitatea reacției. Raportul de incident conține recomandări privind îmbunătățirea controlelor (tehnice sau procedurale) care ar fi putut preveni sau atenua incidentul. Aceste recomandări sunt apoi implementate ca acțiuni de remediere – de exemplu, întărirea politicilor de parolare dacă atacul a reușit prin forțarea parolelor, sau training suplimentar anti-phishing dacă vectorul a fost un e-mail malițios deschis de un angajat.

Prin îmbinarea acestor mecanisme **preventive**, de **detecție** și de **răspuns**, UCMH își consolidează apărarea împotriva amenințărilor cibernetice complexe și își protejează atât infrastructura proprie, cât și contribuția esențială la sistemul energetic național.

8. Responsabilități și organigramă de securitate

Securitatea informației la UCMH este un efort colectiv care implică întregul personal, dar anumite roluri și structuri organizatorice au responsabilități clare în implementarea și supravegherea acestei politici. Organigrama de securitate a informației include atât funcții executive, cât și tehnice, asigurând o **linie de comandă și control** bine definită pentru toate aspectele de securitate.

- **Consiliul de Administrație al UCMH:** Are responsabilitatea supremă de a asigura că UCMH dispune de un cadru adecvat de securitate a informației. Aprobă prezenta politică și revizuirile sale ulterioare, alocă resursele necesare implementării măsurilor de securitate și se asigură că securitatea informației este integrată în strategia generală de afaceri. De asemenea, monitorizează indicatorii de risc majori și este informată despre incidentele semnificative.

- **Directorul General UCMH:** Asigură punerea în aplicare a politicii la nivel operațional. Îi revin sarcini precum: desemnarea formală a persoanelor responsabile de securitatea informației și a datelor personale, susținerea inițiativelor de securitate, includerea obiectivelor de securitate în evaluarea performanței organizației și, dacă e cazul, raportarea situațiilor de risc către autoritățile tutelare sau către acționari.

- **Responsabilul cu Securitatea Informației (CISO / RSI):** UCMH numește un Responsabil pentru Securitatea Informației (care poate fi un *Chief Information Security Officer* sau echivalent). Acesta coordonează toate activitățile de securitate IT și a informației în companie. Responsabilul elaborează și actualizează politicile și procedurile de securitate, efectuează evaluări de risc periodice, propune măsuri de securitate și supervizează implementarea lor de către departamentele tehnice. De asemenea, el consiliază managementul pe teme de securitate și asigură comunicarea cu entitățile externe (ex.: CERT-RO/DNSC) pe linie de securitate cibernetică. Responsabilul raportează direct Directorului General sau unei alte poziții de conducere suficient de înalte, pentru a asigura independența și autoritatea necesare.

- **Structura de Securitate pentru Informații Clasificate:** În conformitate cu cerințele legale, UCMH va organiza un *compartiment specializat de securitate* pentru protecția informațiilor clasificate (acolo unde compania deține sau operează astfel de informații). Această structură este condusă de un **Ofițer de Securitate/Funcționar de Securitate** avizat ORNISS, care răspunde de implementarea măsurilor prevăzute de Legea 182/2002 și HG 585/2002: evidența și controlul documentelor clasificate, instruirea personalului care lucrează cu secrete de stat/de serviciu, evaluarea securității locurilor de păstrare, verificările de securitate pentru personalul care necesită acces la secret etc. Ofițerul de securitate colaborează cu CISO pentru a alinia cerințele de securitate cibernetică cu cele de securitate fizică a informațiilor clasificate, evitând conflictele (de exemplu, implementarea de criptosisteme aprobate STS pentru protecția electronică a secretelor de stat).

- **Departamentul IT:** Este responsabil de administrarea tehnică a sistemelor informatice și de rețea în conformitate cu politicile de securitate. Personalul IT (administratori de sistem, de rețea, de baze de date etc.) aplică configurările de securitate, gestionează accesul utilizatorilor (creează/dezactivează conturi la cererea HR și cu aprobări necesare), realizează backup-urile, monitorizează infrastructura și reacționează la alertele de securitate conform procedurilor. De asemenea, Dep. IT participă la testele periodice de restaurare și la exercițiile de răspuns la incidente. Orice modificare majoră de infrastructură (instalare de noi servere, actualizări critice) se face cu evaluare de securitate prealabilă de către echipa IT împreună cu CISO.

- **Responsabilul cu Protecția Datelor (DPO):** Conform GDPR, UCMH are un DPO care se ocupă specific de conformitatea cu normele de protecție a datelor cu caracter personal. DPO colaborează îndeaproape cu CISO și cu departamentele de specialitate pentru a se asigura că datele personale sunt prelucrate în siguranță și legal. DPO participă la evaluări de impact privind protecția datelor (DPIA) pentru proiecte noi ce implică date personale, gestionează cererile persoanelor vizate și supraveghează măsurile tehnice (pseudonimizare, acces limitat) dedicate protejării datelor personale. În caz de incidente de securitate care implică date cu caracter personal (ex.: breșe de date), DPO coordonează notificarea Autorității Naționale de Supraveghere a Datelor cu Caracter Personal (ANSPDCP) în termenul legal, în paralel cu gestionarea incidentului de către echipa de securitate.

- **Angajații și colaboratorii UCMH:** Toți utilizatorii (indiferent de poziție) au responsabilitatea de a respecta această politică și procedurile asociate. Ei trebuie: să participe la sesiunile de instruire în domeniul securității (vezi Secțiunea 10), să protejeze informațiile și activele pe care le utilizează (prin măsuri simple precum blocarea ecranului când părăsesc biroul, păstrarea sub cheie a documentelor, nu divulgă parole sau informații sensibile), să raporteze imediat orice incident sau suspiciune (email suspect, pierdere de echipament, comportament anormal al sistemelor) către Service Desk IT sau către responsabilul de securitate. Nerespectarea cerințelor de securitate de către personal poate conduce la măsuri disciplinare, conform Secțiunii 11.

Prin clarificarea acestor roluri, UCMH asigură o **guvernanță eficientă a securității informației**, unde responsabilitățile sunt bine definite și se evită lacunele sau suprapunerile. Toți angajații cu funcții de conducere, în special, au obligația de a da exemplu personal în respectarea politicilor de securitate și de a-și informa subordonații despre importanța conformării.

9. Obligativitatea notificării autorităților naționale relevante în caz de incident

UCMH, în calitatea sa de companie ce operează infrastructură critică și servicii esențiale (sectorul energetic hidroenergetic), se supune obligațiilor legale de notificare a incidentelor de securitate către autoritățile competente ale statului. Această secțiune stabilește **cadrul de notificare externă**, asigurând coordonarea UCMH cu autoritățile naționale în domeniul securității cibernetice și al protecției infrastructurilor critice.

Conform **OUG nr. 155/2024)** și reglementărilor asociate, UCMH (ca operator de servicii esențiale) va notifica **imediat** orice incident de securitate care **îi afectează rețelele și sistemele informatice esențiale** către punctul unic de contact național – respectiv către Directoratul Național de Securitate Cibernetică, prin PNRISC. Notificarea se face prin canalele

desemnate (portal de raportare sau punct de contact de urgență), incluzând informații despre natura incidentului, sistemele afectate, impactul estimat și măsurile luate. DNSC va trata notificarea și, la rândul său, o va transmite către autoritățile/echipele CSIRT din alte state membre, dacă este cazul, acționând ca punct unic de contact la nivel internațional.

Colaborarea cu SRI și alte autorități: UCMH recunoaște că protecția cibernetică a infrastructurilor critice este o problemă de securitate națională. Astfel, compania cooperează cu Serviciul Român de Informații (în special prin Centrul Național Cyberint) și cu alte instituții abilitate. Conform cadrului legislativ, DNSC beneficiază de suport din partea SRI, STS, precum și a altor entități în gestionarea incidentelor majore. În practică, aceasta înseamnă că, pentru incidente de gravitate ridicată (atacuri complexe, posibile acțiuni ale unor actori statali, incidente ce vizează siguranța națională), UCMH va informa de urgență și direct Serviciul Român de Informații (CNC) și va permite implicarea acestuia în investigație sau remediere, după caz. De asemenea, dacă un incident afectează comunicațiile speciale sau infrastructuri IT&C guvernamentale conexe, Serviciul de Telecomunicații Speciale (STS) poate fi implicat. UCMH va coopera cu STS în măsura în care acesta furnizează servicii de încredere sau expertiză tehnică pentru sectorul energetic.

Notificarea incidentelor care implică informații clasificate: În situația puțin probabilă a compromiterii unor informații clasificate (ex. pierderea sau acces neautorizat la un document *Secret de serviciu* al UCMH ori la un document *Secret de stat* provenit de la autorități), UCMH va proceda conform Legii 182/2002 și HG 585/2002. Aceasta implică notificarea de îndată a Autorității Desemnate de Securitate (ADS) – de regulă, **ORNISS** (Oficiul Registrului Național al Informațiilor Secrete de Stat) pentru secretele de stat, sau instituția emitentă în cazul documentelor primite. Ofițerul de securitate intern va întocmi un raport de eveniment și îl va transmite către ORNISS/SRI, care pot demara investigații de contrainformații. Totodată, se vor informa și conducerea UCMH și Hidroelectrica (dacă este cazul) despre incident.

Notificarea altor autorități specializate: În funcție de natura incidentului:

- Dacă incidentul implică o posibilă faptă penală (ex. atac de tip fraudă informatică, sabotaj intern), UCMH va sesiza **organele de urmărire penală** competente (Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism - DIICOT – Biroul de Criminalitate Cibernetică sau altă unitate de parchet, după caz).

- Dacă incidentul vizează date cu caracter personal (breach de securitate conform GDPR) și există risc pentru drepturile persoanelor vizate, DPO-ul va notifica **Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)** în cel mult 72 de ore, exceptând cazul în care este improbabil să rezulte un risc pentru persoane. Persoanele vizate afectate vor fi și ele informate, dacă breșa

este severă (ex.: expunerea datelor personale sensibile).

- Dacă incidentul are impact sau implică cooperarea internațională (ex.: afectează parteneri externi, proiecte UE), UCMH va urma procedurile de notificare transmise de autoritatea națională (DNSC) către rețeaua de cooperare NIS2 la nivel UE.

Formatul și conținutul notificărilor: Notificările către autorități vor conține, în general: detalii de contact UCMH, data și ora depistării incidentului, durata și statusul său, tipul de amenințare (dacă e cunoscut, ex.: ransomware, DDoS, APT), sistemele și serviciile afectate (ex.: "SCADA uzina – indisponibil, întrerupere producție 2 ore"), impactul asupra beneficiarilor sau populației (dacă e cazul), măsuri deja luate de UCMH și măsuri solicitate/dorite de la autoritate (ex.: asistență tehnică, schimb de informații). UCMH se angajează să furnizeze actualizări ale notificării pe măsură ce apar noi informații sau când incidentul este rezolvat.

Confidențialitatea și limitarea divulgării: Orice comunicare către autorități se va face *confidențial*, marcând informațiile transmise cu nivelul corespunzător (de exemplu, dacă includ detalii sensibile comerciale, se va menționa "confidențial – uz intern"). Personalul UCMH implicat în gestionarea incidentelor este instruit să nu divulge public detalii despre incidente, decât prin canalele oficiale aprobate. Comunicarea cu presa sau publicul, dacă necesară, va fi gestionată de conducerea UCMH și departamentul de comunicare, în consultare cu autoritățile (pentru a nu periclita investigațiile în curs).

Prin notificarea promptă și corectă a autorităților relevante, UCMH își îndeplinește obligațiile legale și contribuie la efortul național de răspuns la incidente, beneficiind totodată de sprijinul instituțional necesar pentru gestionarea eficientă a crizelor de securitate.

10. Politici privind formarea angajaților și cultura de securitate

Conștientizarea și pregătirea angajaților reprezintă o componentă critică a securității informației. UCMH promovează activ o **cultură de securitate** puternică, în care fiecare angajat își înțelege rolul în protejarea informațiilor. Pentru a atinge acest deziderat, compania instituie programe continue de formare și politici menite să integreze bunele practici de securitate în comportamentul zilnic al personalului.

- **Instruire inițială în domeniul securității informației:** Fiecare angajat nou al UCMH, precum și colaboratorii pe termen lung, vor primi, la momentul angajării sau începerii colaborării, o sesiune de **instruire introductivă** privind securitatea informației și protecția datelor. Această instruire cuprinde prezentarea principalelor politici (inclusiv prezenta politică), a regulilor de bază (ex.: clasificarea informațiilor, utilizarea în

siguranță a echipamentelor IT, reguli de parolare, igiena în spațiul de lucru curat – *clean desk policy*), precum și exemple de amenințări comune (phishing, inginerie socială, malware). Noii angajați vor semna un **angajament de confidențialitate** și de respectare a politicilor de securitate ca parte a procesului de integrare.

- **Instruire periodică și campanii de conștientizare:** Toți angajații participă la **cursuri de reîmprospătare** a cunoștințelor de securitate cel puțin o dată pe an, sau ori de câte ori apar amenințări noi relevante. Aceste instruiri pot lua forma unor prezentări, seminarii web sau module e-learning interactive, acoperind subiecte precum: cum să recunoști un e-mail de phishing, importanța actualizărilor software, protecția dispozitivelor mobile, politica "BYOD" (Bring Your Own Device) dacă este cazul, proceduri de raportare a incidentelor, și altele. Se vor derula periodic *simulări și exerciții* – de exemplu, teste de tip "phishing simulation" (trimiterea unor e-mailuri false controlate către angajați pentru a vedea reacția) urmate de feedback educativ pentru cei care au căzut victime.

- **Formare specializată pentru personal cu roluri cheie:** Angajații din departamente tehnice (IT, SCADA), precum și cei care manipulează date sensibile (HR, financiar, structură de securitate) beneficiază de cursuri avansate specifice rolului lor. De exemplu, echipa de administratori de sistem poate participa la training-uri privind configurarea securizată a serverelor sau răspunsul la incidente cibernetice, în timp ce personalul din structură de securitate poate urma cursuri organizate de ORNISS/SRI privind managementul informațiilor clasificate.

- **Promovarea culturii de "security first":** UCMH încurajează atitudinea proactivă a angajaților față de securitate. Comunicări periodice (newsletter intern de securitate, afișe în birouri, mesaje scurte pe intranet) reamintesc bunele practici: ex. "Nu divulga parolele", "Verifică identitatea înainte de a oferi informații sensibile la telefon" (prevenirea social engineering). În fiecare an, cu ocazia "Lunii Europene a Securității Cibernetice" (octombrie) sau a unor evenimente similare, UCMH poate organiza *workshop*-uri tematice, concursuri sau prezentări menite să implice angajații și să crească vizibilitatea subiectului.

- **Canal de raportare deschisă:** Cultura de securitate este întărită de existența unui mediu în care angajații se simt confortabil să raporteze probleme. UCMH menține un **canal dedicat de raportare a incidentelor sau suspiciunilor** (de tip helpline sau adresă de e-mail securizată), unde oricine poate semnala anonim, dacă dorește, o potențială încălcare de securitate sau o vulnerabilitate observată, fără teama de repercusiuni negative atâta timp cât raportarea se face cu bună credință. Echipa de securitate investighează prompt toate semnalările și mulțumește angajaților pentru

vigilență.

- **Integrarea securității în evaluarea performanței:** Pentru a încuraja respectarea regulilor, UCMH integrează componente de securitate în evaluările periodice ale performanței personalului de conducere și, acolo unde este relevant, ale personalului de execuție. De exemplu, indicatori precum *participarea la training-urile de securitate*, *numărul de incidente imputabile neglijenței* sau *inițiative de îmbunătățire a securității propuse* pot fi luați în considerare la evaluare. Astfel, securitatea devine parte a responsabilităților de zi cu zi, nu un element opțional.

Scopul final al acestor eforturi este ca **fiecare angajat UCMH să devină cea mai puternică verigă** în lanțul de securitate, nu cea mai slabă. Prin cunoaștere, vigilență și atitudine proactivă, personalul poate preveni multe incidente (întrucât eroarea umană este adesea o cauză principală a breșelor de securitate). O cultură solidă de securitate asigură faptul că procedurile nu rămân doar pe hârtie, ci sunt efectiv aplicate și susținute la nivel organizațional.

11. Audit intern, măsuri disciplinare și actualizarea politicii

Pentru a menține eficiența și relevanța sistemului de securitate a informației, UCMH implementează mecanisme de verificare și corecție continuă. Auditarea conformității, aplicarea unor sancțiuni în caz de abateri și revizuirea periodică a politicii sunt componente esențiale ale acestui proces de asigurare a calității și îmbunătățire continuă.

- **Audit intern și evaluarea conformității:** UCMH derulează **audituri interne periodice** pe zona securității informației, cel puțin anual sau ori de câte ori intervin schimbări majore. Auditul poate fi realizat de Structura Audit Intern al companiei (dacă există) sau de o echipă mixtă sub coordonarea RSI/CISO, și urmărește verificarea implementării politicii și procedurilor asociate. Se evaluează dacă măsurile planificate sunt în vigoare și eficace – de exemplu, auditul poate testa dacă accesurile neautorizate sunt într-adevăr blocate, dacă log-urile sunt păstrate corespunzător, dacă personalul cunoaște procedura de raportare a incidentelor etc. Auditul include și *scanări de vulnerabilitate* și teste tehnice (sau recurge la firme externe specializate pentru *penetration testing* anual, asigurând o evaluare independentă). Constatările auditului sunt documentate într-un raport ce evidențiază non-conformitățile sau zonele de risc rezidual, împreună cu recomandări. Conducerea UCMH va analiza raportul și va dispune măsuri de remediere cu termene și responsabilități clare. Realizarea măsurilor corective este ulterior verificată pentru închidere. În plus față de auditul intern, UCMH se supune și eventualelor controale ale organelor externe (ex.: controale DNSC conform Directivei NIS2, audituri ale Curții de Conturi, audit de conformitate ISO 27001 dacă

compania se certifică etc.), asigurând colaborare deplină și transparență față de auditori.

- **Măsuri disciplinare în caz de încălcare a politicii:** Încălcarea deliberată sau din neglijență gravă a prevederilor prezentei politici de către personalul UCMH este considerată o abatere disciplinară și va fi tratată conform Codului Muncii și regulamentelor interne de ordine interioară. În funcție de gravitatea faptei, sancțiunile pot include: avertisment scris, reducerea salariului pe o durată determinată, retrogradarea temporară din funcție, suspendarea contractului sau chiar **desfacerea disciplinară a contractului de muncă** în cazuri de încălcare majoră (de ex.: dezvăluirea intenționată a unor secrete comerciale sau clasificate, nerespectarea voită a procedurilor care a dus la un incident sever). Scopul sancțiunilor nu este punitiv în sine, ci de a sublinia importanța conformării și de a preveni recurența. Înainte de aplicarea oricărei sancțiuni, se va derula o cercetare disciplinară în care angajatul are ocazia să își expună punctul de vedere. Totodată, UCMH recunoaște diferența dintre eroare umană involuntară (caz în care accentul va fi pe instruire suplimentară) și neglijență repetată sau act intenționat. În cazurile care implică și încălcări ale legii (ex.: furt de date, fraudă), compania va sesiza organele de cercetare penală, indiferent de măsurile interne luate.

- **Actualizarea și îmbunătățirea politicii:** Prezenta politică de securitate a informației va fi revizuită **cel puțin o dată pe an** pentru a asigura actualitatea sa față de mediul de amenințări, evoluțiile tehnologice și modificările legislative sau organizaționale. Revizuirea va fi coordonată de RSI/CISO, care va implica părțile relevante (IT, juridic, HR, management operațional). Orice modificare propusă (de exemplu, adăugarea unor noi cerințe rezultate dintr-o lege apărută, sau ajustarea nivelurilor CIS, introducerea unei noi politici de telemuncă etc.) va fi supusă aprobării Directorului/Consiliului de Administrație al UCMH, similar cu aprobarea inițială a politicii. După aprobare, noile versiuni ale politicii sunt **comunicate întregului personal** și, dacă schimbările sunt semnificative, se vor organiza sesiuni de re-instruire focalizate pe noile aspecte. Fiecare angajat cu funcție de conducere, precum și personalul, vor semna din nou de luare la cunoștință dacă apar modificări substanțiale.

- **Integrarea feedback-ului și a lecțiilor învățate:** Între revizuirile anuale, politica poate fi amendată punctual dacă investigațiile de incidente sau rezultatele auditurilor indică lacune serioase. De exemplu, dacă un incident relevă că o anumită practică nu este acoperită de reguli, politica va fi actualizată pentru a acoperi situația respectivă. UCMH menține un istoric al versiunilor politicii, pentru a avea trasabilitate asupra modificărilor efectuate.

Prin aceste mecanisme de control și corecție, UCMH se asigură că politica sa de securitate nu rămâne un document static, ci un instrument **viu**, adaptat continuu pentru a răspunde provocărilor de securitate. Angajamentul față de audit și îmbunătățire constantă reflectă importanța pe care compania o acordă protecției informațiilor, ca parte integrantă a guvernanței sale corporative și a datoriei de diligență față de acționari, parteneri și societate.

Politica de Securitate a Informației UCMH Reșița SRL – versiune 2025. Document aprobat de administratorii UCMH și difuzat intern tuturor angajaților spre luare la cunoștință și conformare.

Aprobat,

Manuela Feder-Administrator Manuela Feder Semnat digital de Manuela Feder Data: 2025.07.01 10:09:52 +03'00'

Aurel Bara-Administrator Aurel Bara Semnat digital de Aurel Bara Data: 2025.07.01 11:14:07 +03'00'

Andrei Nicolae Popa-Administrator ANDREI-NICOLAE POPA Digitally signed by ANDREI-NICOLAE POPA Date: 2025.07.01 16:49:44 +03'00'