EFECTRO SRL
CUI: RO14961034
Nr. Reg. Com.: J2002002080121
Capital social: 10200 RON

Sediu social
str. Jan Huss nr. 29,
Cluj-Napoca 400268

Adresă birou
str. Câmpul Păinii Nr. 3-5,
Coratim, intr. A, et. 4
Cluj-Napoca 400058

Conturi bancare
RO29 INGB 0000 9999 0237 6501
RO37 RZBR 0000 0600 2598 4475
RO79 TREZ 2165 069X XX00 9157

Politica de securitate a informațiilor | EFECT

Data: 12 noiembrie 2026

POLITICA EFECT DE SECUREITATE A INFORMATIEI	CE ÎNSEAMNĂ PENTRU TINE
1. Scop	
EFECT stabilește prin prezenta politică principiile, angajamentele și responsabilitățile pentru protejarea confidențialității, integrității și disponibilității informațiilor.	Stabilim reguli și responsabilități pentru a proteja informațiile pe care le gestionăm.
Politica oferă cadrul pentru stabilirea obiectivelor SMSI, tratarea riscurilor și îmbunătățirea continuă a sistemului, în concordanță cu ISO/IEC 27001:2022.	Astfel urmărim să reducem riscurile de acces neautorizat, modificare sau indisponibilitate.
2. Domeniu de aplicare	
Politica se aplică persoanelor, proceselor, informațiilor și activelor aflate în domeniul SMSI aprobat, inclusiv angajaților, colaboratorilor și terților care accesează sau gestionează informații în numele EFECT.	Aplicăm aceste reguli activităților și serviciilor din domeniul SMSI.
În limitele domeniului SMSI și ale responsabilităților contractuale, sunt avute în vedere serviciile ITSM externalizate, hosting, datacenter, backup, recuperare în caz de dezastru, administrare și monitorizare la distanță, precum și informațiile clienților.	Pentru serviciul tău, ne asumăm responsabilitățile stabilite prin contract; certificarea acoperă doar domeniul său declarat.
Domeniul certificat al SMSI este definit separat conform clauzei 4.3; această politică nu îl extinde implicit.	
3. Referințe și documente asociate	
ISO/IEC 27001:2022; domeniul SMSI; metodologia de evaluare și tratare a riscurilor; registrul riscurilor; Declarația de Aplicabilitate (SoA); obiectivele SMSI; inventarul activelor; procedurile de control al accesului, gestionare a incidentelor, continuitate, audit intern și acțiuni corective.	Folosim proceduri și evidențe pentru a aplica în mod consecvent măsurile de securitate în serviciile pe care le gestionăm.
Codurile și edițiile documentelor asociate se mențin în lista documentelor controlate.	
Prezenta politică reprezintă cadrul general de securitate a informațiilor al EFECT. Politicile tematice, standardele și procedurile aprobate detaliază aplicarea principiilor sale.	Clarificăm cerințele care se suprapun sau se contrazic, pentru ca regulile aplicabile să rămână coerente.
Responsabilul SMSI coordonează menținerea coerenței documentației și inițiază clarificarea suprapunerilor sau	

POLITICA EFECT DE SECUREITATE A INFORMATIEI	CE ÎNSEAMNĂ PENTRU TINE
neconcordanțelor, în cadrul procesului de control al informațiilor documentate.	
4. Principii și obiective generale de securitate	Limităm accesul la informațiile tale la persoanele autorizate care au nevoie de ele pentru activitatea lor.
EFECT urmărește: protejarea confidențialității prin acces autorizat; păstrarea integrității informațiilor și procesărilor; asigurarea disponibilității potrivit cerințelor de afaceri și contractuale; aplicarea principiului privilegiului minim; protecția informațiilor pe întreg ciclul lor de viață; gestionarea proporțională cu riscul a controalelor.	
Obiectivele măsurabile, indicatorii, responsabilii și termenele sunt stabilite și urmărite într-un document distinct privind obiectivele SMSI.	Urmărim să protejăm corectitudinea și disponibilitatea informațiilor, potrivit obligațiilor asumate.
EFECT clasifică informațiile în funcție de sensibilitate, valoare, criticitate și cerințele aplicabile și stabilește măsuri de protecție proporționale cu clasificarea și riscurile asociate.	Adaptăm măsurile de protecție la sensibilitatea, importanța și riscurile informațiilor.
Proprietarii informațiilor participă la stabilirea cerințelor de protecție și a condițiilor de acces și utilizare, în limitele responsabilităților atribuite.	
5. Angajamentul managementului	Conducerea noastră aprobă și susține măsurile de securitate, inclusiv prin resurse și responsabilități.
Managementul superior stabilește și aprobă politica, susține integrarea cerințelor de securitate în procesele organizației, asigură resurse adecvate și promovează responsabilitatea pentru securitatea informațiilor.	
Managementul se angajează să îndeplinească cerințele legale, reglementare, contractuale și alte cerințe de securitate aplicabile, să sprijine atingerea obiectivelor și să îmbunătățească continuu SMSI.	Astfel tratăm securitatea ca parte a modului în care lucrăm, nu doar ca pe o sarcină IT.
6. Roluri, responsabilități și autorități	Stabilim cine decide, cine aplică și cine verifică măsurile de securitate.
Managementul superior aprobă politica, alocă resurse și analizează eficacitatea SMSI, păstrând responsabilitatea generală pentru funcționarea și îmbunătățirea acestuia.	
Responsabilul SMSI are responsabilitatea și autoritatea de a se asigura că SMSI îndeplinește cerințele ISO/IEC 27001:2022, coordonează implementarea, monitorizarea și revizuirea politicii și raportează performanța sistemului către managementul superior.	
Responsabilul IT intern și responsabilii tehnici aplică măsurile de securitate în ariile atribuite. Proprietarii de informații și de active	Când apare o problemă, identificăm rolurile care trebuie să o evalueze, să o trateze și să o raporteze.

POLITICA EFECT DE SECUREITATE A INFORMATIEI	CE ÎNSEAMNĂ PENTRU TINE
stabilesc cerințele de protecție și validează necesitatea drepturilor de acces.	
Angajații, colaboratorii și terții respectă cerințele aplicabile și raportează prompt evenimentele suspecte. Atribuirea formală a rolurilor și autorităților se documentează în organigramă, fișe de post sau decizii interne.	
7. Managementul riscurilor de securitate a informațiilor	Evaluăm riscurile care pot afecta informațiile și serviciile gestionate, alegem măsuri proporționale și urmărim aplicarea lor.
EFECT identifică, analizează, evaluează și tratează riscurile folosind o metodologie aprobată și criterii consecvente de evaluare și acceptare.	
Pentru fiecare risc relevant se desemnează un proprietar, se stabilesc opțiuni de tratare și se documentează deciziile. Proprietarii competenți aprobă planurile de tratare și acceptă riscurile reziduale, conform nivelurilor de autoritate stabilite.	
Evaluările se revizuiesc periodic și la schimbări semnificative. Controalele selectate se corelează cu SoA, iar măsurile se urmăresc prin planul de tratare.	
Riscurile care depășesc criteriile de acceptare aprobate sunt escaladate către nivelul de management competent, potrivit autorităților desemnate.	Escaladăm riscurile care depășesc limitele acceptate, pentru ca persoanele competente să decidă asupra lor.
Orice excepție de la politicile și controalele de securitate necesită justificare documentată, evaluarea riscurilor asociate, identificarea măsurilor compensatorii, dacă este cazul, și aprobarea formală de către autoritatea competentă.	Aprobăm excepțiile de la regulile de securitate numai după justificare și evaluare; apoi le monitorizăm.
Excepțiile aprobate sunt înregistrate, monitorizate și revizuite periodic sau la schimbări relevante.	
8. Principii privind aplicarea controalelor de securitate	Protejăm informațiile și serviciile pe care le gestionăm prin controale de acces și monitorizare adaptate riscurilor.
Controalele de securitate sunt selectate în funcție de riscuri, cerințe aplicabile și contextul serviciilor.	
EFECT gestionează identitățile și drepturile de acces, inventariază și protejează activele, urmărește vulnerabilitățile și modificările, protejează infrastructura și informațiile și monitorizează evenimentele relevante.	
EFECT identifică, documentează și gestionează responsabilitățile de securitate a informațiilor în relațiile cu furnizorii, partenerii și clienții, inclusiv pentru servicii cloud și infrastructuri administrate.	Delimităm responsabilitățile noastre de cele ale furnizorilor, partenerilor și clienților, conform obligațiilor asumate.
Organizația evaluează riscurile asociate acestor relații, stabilește cerințe contractuale adecvate și urmărește îndeplinirea	

POLITICA EFECT DE SECUREITATE A INFORMATIEI	CE ÎNSEAMNĂ PENTRU TINE
obligațiilor de securitate asumate, în limitele domeniului SMSI și ale responsabilităților contractuale.	
EFECT stabilește măsurile de backup, continuitate și recuperare pe baza impactului potențial al întreruperilor asupra proceselor și serviciilor, a criticității resurselor, a riscurilor identificate și a obligațiilor contractuale asumate.	Adaptăm măsurile de backup și recuperare la criticitatea serviciului și la contract și verificăm periodic dacă funcționează.
Organizația verifică periodic eficacitatea măsurilor de continuitate și recuperare, potrivit procedurilor aplicabile.	Condițiile concrete diferă de la un serviciu la altul.
Cerințele operaționale, frecvențele și configurațiile se stabilesc în proceduri și standarde specifice, nu în această politică.	Stabilim detaliile tehnice și frecvențele în proceduri și standarde dedicate. Această politică prezintă principiile generale.
9. Gestionarea evenimentelor și incidentelor de securitate	Investigăm evenimentele suspecte, limităm impactul și documentăm intervențiile.
Personalul și părțile relevante raportează fără întârziere evenimentele suspecte prin canalele interne comunicate.	
EFECT evaluează evenimentele, determină dacă acestea constituie incidente, stabilește prioritățile, limitează impactul, investighează și documentează răspunsul.	
Atunci când este cazul, gestionează notificările legale și contractuale în termenele aplicabile. Lecțiile învățate sunt utilizate pentru îmbunătățirea controalelor și procedurilor.	Când legea sau contractul ne obligă să te notificăm, comunicăm în termenele aplicabile.
10. Conștientizare, instruire și comunicare	Instruim persoanele care gestionează informații și verificăm dacă își cunosc responsabilitățile.
EFECT asigură informarea și instruirea adecvată rolurilor, verifică înțelegerea responsabilităților și păstrează dovezi corespunzătoare.	
Politica este disponibilă personalului relevant prin platforma documentară internă Confluence, cu acces controlat; pentru părțile interesate externe este comunicată în măsura în care este adecvat.	
Personalul și celelalte părți relevante cărora li se aplică politica confirmă luarea la cunoștință prin mecanismele stabilite de organizație, iar EFECT păstrează evidențele aferente. Modificările importante sunt comunicate în mod documentat.	Comunicăm regulile celor vizați, ca să știe ce au de făcut.

POLITICA EFECT DE SECUREITATE A INFORMATIEI	CE ÎNSEAMNĂ PENTRU TINE
11. Conformitate legală, reglementară și contractuală	
EFECT identifică și respectă cerințele aplicabile de securitate a informațiilor, protecție a datelor cu caracter personal, confidențialitate, proprietate intelectuală și obligațiile contractuale asumate.	Respectăm obligațiile legale și contractuale aplicabile serviciilor noastre și le reevaluăm când apar schimbări.
Cerințele aplicabile se revizuiesc la schimbări legislative, tehnologice și contractuale. Aplicabilitatea unor reglementări specifice se determină separat, fără a presupune automat că toate se aplică organizației.	Verificăm separat ce reguli se aplică fiecărui context.
12. Monitorizare, audit și analiza managementului	
EFECT monitorizează performanța SMSI prin indicatori și evaluări adecvate, realizează audituri interne planificate și efectuează analiza managementului la intervale stabilite.	Verificăm prin indicatori, audituri și analize ale conducerii dacă măsurile de securitate își ating obiectivele.
Analiza ia în considerare rezultatele auditurilor, incidentele, neconformitățile, obiectivele, evoluția riscurilor, schimbările relevante și oportunitățile de îmbunătățire. Deciziile și acțiunile rezultate sunt înregistrate, atribuite și urmărite.	Urmărim acțiunile când identificăm probleme.
13. Neconformități, acțiuni corective și îmbunătățire continuă	
La identificarea unei neconformități, EFECT reacționează pentru a o controla și corecta și tratează consecințele, după caz.	Când identificăm o problemă, analizăm cauzele, luăm măsuri și verificăm dacă funcționează, pentru a reduce riscul reapariției.
Organizația evaluează cauzele și necesitatea acțiunilor pentru prevenirea reapariției, implementează măsuri proporționale, verifică eficacitatea lor și actualizează SMSI atunci când este necesar.	
Evidențele privind natura neconformităților, acțiunile întreprinse și rezultatele acestora se păstrează conform procedurii de acțiuni corective. EFECT urmărește îmbunătățirea continuă a adecvării, suficienței și eficacității SMSI.	Documentăm acțiunile și rezultatele.
14. Revizuire, comunicare și control document	
Responsabilul SMSI propune revizuirea politicii cel puțin anual și ori de câte ori apar schimbări semnificative ale riscurilor, cerințelor, serviciilor sau structurii organizației. Managementul superior aprobă versiunile actualizate.	Revizuim politica anual și când apar schimbări importante.
Versiunea în vigoare, istoricul modificărilor, distribuirea și retragerea versiunilor depășite se gestionează conform regulilor de control al informațiilor documentate.	

POLITICA EFECT DE SECUREITATE A INFORMATIEI	CE ÎNSEAMNĂ PENTRU TINE
Data aprobării și data intrării în vigoare a fiecărei versiuni sunt înregistrate înainte ca aceasta să fie distribuită ca versiune aplicabilă.	Ținem evidența versiunilor aprobate, astfel încât să fie clar ce reguli aplicăm.