**Confirmarea înțelegerii și asumării cerințelor de Securitate**

**Ofertant:** ……………………………………………………………………………………………………………..……………….…………………
**Reprezentant autorizat: [Numele și funcția**] ………………………………………………………………………….…………………
**Data completării: [zz/ll/aaaa]** ………………………………………………………………………………..……………….……………….

Prin prezenta, confirmăm că am **citit, înțeles și acceptat cerințele de securitate** detaliate mai jos și că ne **angajăm să respectăm** aceste cerințe în cadrul executării proiectului, în cazul atribuirii contractului.

**1. Controlul Accesului și Autorizarea Utilizatorilor**

**Control RBAC (Role-Based Access Control) la nivelul CMS:**

* Implementarea unui sistem granular RBAC pentru a defini și aplica permisiunile per rol.
* Rolurile trebuie să fie configurabile în funcție de atribuțiile operaționale (ex: editor conținut, manager produse, administrator, marketing).
* Fiecare rol va avea permisiuni clar delimitate, respectând principiul privilegiului minim (least privilege):
	+ Editor conținut: creare, editare, publicare articole doar în anumite secțiuni.
	+ Manager produse: gestiune catalog, prețuri, stocuri.
	+ Administrator: acces complet la configurare CMS, gestionare utilizatori, setări sistem.
	+ Marketing: campanii, promoții, analitică.
* Revizuirea periodică a permisiunilor și automatizarea acestui proces prin scripturi sau unelte specifice.
* Utilizarea unui framework de securitate (ex: Spring Security pentru CMS Java sau alternativ echivalent pentru alte limbaje).

**Principiul Privilegiului Minim:**

* Aplicat la toate nivelurile soluției: utilizatori, procese, baze de date, sistem de fițiere, API-uri.
	+ Baze de date: conturi separate pentru aplicație și CMS cu permisiuni restrânse (ex: SELECT, INSERT pe tabele specifice).
	+ Sistem fițiere: serverul web rulează cu un utilizator dedicat cu permisiuni minime (scriere doar în directoarele de upload).
	+ API: acces controlat prin OAuth 2.0 și scope-uri clare per aplicație.

**Flux de Aprobare a Conținutului:**

* Implementarea unui flux obligatoriu de creare-revizie-aprobare-publicare.
* Separare clară de roluri (ex: Creator → Reviewer → Aprobare → Publicare).
* Audit complet: jurnalizare utilizator, dată/ora și modificările efectuate (ex: CMS Drupal + module de audit).

**Autentificare:**

* Autentificare puternică pentru CMS, backend e-shop și portal Azure:
	+ Activarea MFA (autentificare multi-factor) prin Azure AD + politici de acces condiționat
	+ MFA obligatorie pentru:
		- Administratorii CMS
		- Utilizatorii cu acces la date sensibile
		- Acces de la distanță
* Politici stricte de parolă:
	+ Min. 12 caractere, combinație de majuscule, cifre, simboluri
	+ Expirare la 90 zile, reutilizare interzisă
	+ Implementare bibliotecă de complexitate (ex: zxcvbn)
* Integrare SSO prin Azure AD + OpenID Connect

**Management sesiune:**

* ID-uri de sesiune protejate (secure, HTTP-only cookies)
* Expirare automata: 20 min inactivitate (user), 30 min (admin)
* Regenerare ID după autentificare
* Generator criptografic puternic pentru ID sesiune

**2. Securitate Infrastructură (Azure)**

**Disponibilitate ridicată și redundanță:**

* Arhitectură multi-zonă cu Azure Availability Zones
* Load balancing (Azure Load Balancer/Application Gateway) + health probes
* Baze de date redundantă (Azure SQL Active Geo-Replication / Availability Zones / read replicas pentru MySQL/PostgreSQL)

**Web Application Firewall (WAF):**

* Azure WAF activ cu reguli OWASP Top 10, protecție bot, rate limiting, filtre HTTP
* Update automat al regulilor prin pipeline CI/CD

**Protecție Anti-DDoS:**

* Azure DDoS Protection Standard (nivel rețea și aplicație)
* Alertare prin Azure Monitor pentru anomalii de trafic sau atacuri

**Bune practici Azure:**

* RBAC pentru toate resursele
* Segmentare rețea prin VNet + Network Security Groups (NSG)
* Configurare sigură a serviciilor conform benchmark-urilor CIS
* Teste de penetrare anuale + după schimbări majore

**Management chei:**

* Azure Key Vault pentru chei criptografice, certificate, secrete
* Control acces prin Azure RBAC, rotație periodică automatizată

**Criptare date:**

* În repaus: Azure Storage Encryption, TDE pentru baze de date
* În tranzit: HTTPS/TLS 1.2+, HSTS activ, certificate valide

**3. Securitate Aplicație**

**Dezvoltare sigură (SSDLC):**

* Integrat securitate în toate fazele: cerințe, dezvoltare, testare, lansare
* Review-uri de cod + SAST (ex: SonarQube, Veracode), DAST (ex: OWASP ZAP, Burp Suite)
* Prioritizarea vulnerabilităților OWASP Top 10

**Validare input / encoding output:**

* Validare date de intrare (regex server-side)
* Encoding context-aware pentru prevenirea XSS (ex: HTML encoding, JS encoding)

**Management vulnerabilități:**

* Scanare regulată (ex: Nessus, OpenVAS)
* Patching automat prin Ansible, Puppet etc.
* SLA-uri de remediere:
	+ Critice: 7 zile
	+ High: 30 zile
	+ Medii/Mici: 90 zile / următorul release (max. 6 luni)
* Status de remediere documentat + notificări către RetuRO

**Securitate API:**

* Autentificare/autorizare API (OAuth 2.0, token-uri cu expirare)
* Validare input, encoding output, rate limiting (ex: Azure API Management)
* Documentare API prin OpenAPI / Swagger

**4. Logging, Monitorizare și Audit**

**Loguri de securitate:**

* Activitate autentificare, acces date sensibile, erori sistem, modificări de configurare
* Loguri aplicație, server web (Apache/IIS), baze de date

**Păstrare loguri:**

* Min. 3 luni în Azure Monitor Log Analytics

**Monitorizare/anomalii:**

* Integrare cu Azure Monitor + Application Insights
* Alarme: autentificări eșuate, acces neautorizat, modificări neprevăzute
* Revizuiri regulate ale logurilor

**Raportare:**

* Generare rapoarte automate privind accesul, autentificarea, erorile, incidentele

**Sisteme IDS/IPS:**

* Azure Security Center, Network Watcher, soluții IDS/IPS gazdă

**5. Backup și Recuperare**

* Backup zilnic prin Azure Backup pentru site, e-shop și baze de date
* Retenție: min. 3 luni
* Backupuri criptate și stocate cu politici stricte de acces
* Teste regulate de restaurare (min. 1 dată/an)
* Plan de Disaster Recovery:
	+ Identificare componente critice
	+ RTO: 4h, RPO: 1h
	+ Proceduri pas cu pas testate regulat

**6. Conformitate**

* GDPR: protecția datelor personale, minimizare date, limitare scop, drepturi utilizator
* Politici interne de securitate care acoperă:
	+ Control acces
	+ Management parole
	+ Protecția datelor
	+ Răspuns la incidente
	+ Vulnerabilități
	+ Backup & restaurare

**Declarație**

Confirmăm că informațiile prezentate în această anexă sunt complete și conforme cu realitatea și că, în cazul atribuirii contractului, ne angajăm să respectăm în integralitate cerințele de securitate prevăzute de RetuRO.

**[Semnătură reprezentant autorizat]** ……………………………………………………………………………………………………………..………
**[Nume complet]** ……………………………………………………………………………………………………………..……………….…………………..
**[Funcție]** ……………………………………………………………………………………………………………..……………….……………………………….
**[Compania ofertantă]**……………………………………………………………………………………………………………..……………….……………
**[Dată]** ……………………………………………………………………………………………………………..……………….……………………………………