**Anexa nr. 4 la regulament – Securitate**

Răspundeți la următoarele întrebări:

| **Nr. crt** | **Intrebare** | **Răspuns /**  **DA / NU /**  **Nu se aplica** |
| --- | --- | --- |
| 1 | Specificați clasa de risc a informațiilor vehiculate în sistem (mic / mediu / mare). |  |
| 2 | Există firewall în cadrul sistemului? |  |
| 3 | Există Web Application Firewall în cadrul sistemului? |  |
| 4 | Sistemul are antivirus și anti-malware? |  |
| 5 | Există IDS/IPS în cadrul sistemului? |  |
| 6 | Există Web/Email Gateway în cadrul sistemului? |  |
| 7 | Sistemul utilizează tehnologii de tip whitelisting? |  |
| 8 | Sistemul are o soluție de identificare vulnerabilități infrastructură? |  |
| **9** | Sistemul realizează actualizarea permanentă și în mod automat a aplicațiilor instalate? |  |
| 10 | Sunt dezactivate serviciile ce nu sunt folosite la nivelul sistemului de operare? |  |
| 11 | Sistemul prezintă control acces (ex profile utilizator)? |  |
| 12 | În cadrul proiectul se vor realiza cursuri pentru conștientizarea securității utilizatorilor? |  |
| 13 | În cadrul proiectul se vor realiza cursuri de securitate pentru administratori? |  |
| 14 | Sistemul are mecanisme de autentificare utilizatori și administratori conform Zero – Trust Security Model? |  |
| 15 | Sistemul este prevăzut cu soluții informatice redundante (HA)? |  |
| 16 | Sistemul este prevăzut cu o soluție de recuperare în caz de dezastru? |  |
| 17 | Proiectul cuprinde planuri de continuitate? |  |
| 18 | Sistemul utilizează tehnologii care permit restaurarea sistemului de operare către o stare predefinită, necompromisă? |  |
| 19 | Sistemul are asigurare suport în perioada garanției? |  |
| 20 | Sistemul are asigurat suport în perioada post garanție? |  |
| 21 | Este prevăzut managementul vulnerabilității (inclusiv teste de penetrare anuale în perioada garanției)? |  |
| 22 | Sunt prevăzute teste de penetrare anuale în perioada post garanție? |  |
| 23 | Sunt prevăzute măsuri de protecție fizică (cameră servere)? |  |
| 24 | Sunt asigurate condițiile de mediu (climatizare)? |  |
| 25 | Sistemul oferă vizibilitate asupra activităților din cadrul aplicațiilor și analize detaliate privind utilizarea datelor? |  |
| 26 | Sistemul este prevăzut cu capabilități de tip Data Loss Prevention (DLP)? |  |
| 27 | Sistemul utilizează autentificare de tip SSO și multi-factor? |  |
| 28 | Proiectul prevede testare whitebox a componentelor dezvoltate? |  |
| 29 | Proiectul prevede testare de penetrare greybox a întregului sistem înainte de go live? |  |
| 30 | Sistemul criptează datele aflate în transit (ex. TLS, VPN)? |  |
| 31 | Sistemul stochează datele în formă criptată? |  |
| 32 | Copiile backup sunt criptate și stocate într-o altă locație? |  |
| 33 | Sistemul implementează mecanisme de API Rate Limiting? |  |