**SERVICIUL DIGITALIZARE, REPREZENTARE, PROTOCOL**

**Serviciul Digitalizare, Reprezentare, Protocol are următoarele atribuții:**

1. **Strategia de informatizare**
2. Armonizeză și urmărește realizarea strategiei de informatizare, în conformitate cu *Strategia națională de informatizare și implementare* în ritm accelerat al societății informaționale în colaborare cu factorii de decizie de la nivelul compartimentelor funcționale și a conducerii executive a instituției;
3. Pregătește proiectele pentru finanțarea externă (PNRR) pe linie de digitalizare, urmărește realizarea investițiilor aprobate în colaborare cu factorii de decizie de la nivelul compartimentelor funcționale și a conducerii executive a instituției și participă activ la implementarea lor;
4. Revizuiește periodic strategia de informatizare, în funcţie de realităţile şi orientările curente în tehnologia informatică, în conformitate cu priorităţile locale, judeţene, naţionale şi tendinţele mondiale în domeniu;
5. Gestionează eficient resursele materiale și tehnologice existente, propune variante de dotare cu tehnică de calcul și alte echipamente electronice necesare unei activității eficiente;
6. Realizează studii, analize, sinteze și activități de proiectare și dezvoltarea de noi soluții /aplicații privind domeniul de activitate și asigură implementarea acestora și a instruirii personalului în vederea utilizării optime a aplicaţiilor;
7. Realizează analize de impact pentru orice schimbare tehnologică – adăugarea unei noi soluții tehnice, schimbarea unei soluții tehnice etc.;
8. Colaborează cu toate compartimentele din cadrul Consiliului Județean Cluj și cu instituțiile subordonate pentru stabilirea strategiei de informatizare a activității desfășurate de fiecare compartiment, prin analiza permanentă asupra sistemului informatic și propune soluții de informatizare adecvate;
9. **Digitalizare**
10. Monitorizarea implementării proiectelor de digitalizare, prin evaluarea constantă a modalităților de utilizare a datelor și asigurarea coordonării bazelor de date, pentru a evita duplicarea lor.
11. Proiectează, realizează şi administrează bazele de date aferente procesului de digitalizare;
12. **Raportări**
13. Întocmește rapoartele de specialitate în domeniul de activitate al compartimentului pentru proiectele de hotărâri, în vederea promovării lor în Consiliul Județean;
14. Elaborează diferite rapoarte şi sinteze, folosind datele existente în cadrul Consiliului Județean Cluj;
15. Realizează prelucrări de date informatice, la solicitarea departamentelor de specialitate din cadrul Consiliului Județean Cluj, în colaborare cu acestea, în vederea obţinerii de informaţii pentru diverse raportări, dacă acest lucru este posibil informatic.
16. **Politici de securitate IT**
17. Concepe şi implementează împreună cu angajaţii Consiliului Județean Cluj politici de securitate IT;
18. Concepe și impune ceea ce se numește „Privacy by Design” (securitate prin proiectare) în tot procesul de dezvoltare software astfel încât tehnici de analiză de risc și de securitate a datelor să fie încorporate de la început pentru toata durata de viață a procesului de dezvoltare, iar în cazul în care dezvoltatorul de software este externalizat, aceste cerințe trebuie să fie asigurate și urmărite să se regăsească în cadrul contractului dintre beneficiar și dezvoltator;
19. Concepe și impune identificarea de tehnici pentru incidente de securitate inclusiv raportarea lor în timp util către autoritatea de supraveghere și, după caz, către persoana vizată;
20. Întocmește o politică internă pentru aplicații, software, servere, cloud, back-up, imprimante, scanere etc., înlocuirea acestora și procedura exactă prin care se face dispunerea de aceste echipamente scoase din uz care dețin, medii de stocare internă;
21. Monitorizează registrele de control pe baza cărora securitatea organizației este verificată în cadrul auditului intern (similar cu ISO 27001);
22. Analizează și evaluează permanent sistemului informatic al Consiliului Județean CLUJ;
23. Asigură aplicarea politicii de securitate a Consiliului Județean Cluj în domeniul IT și digitalizare;
24. Îndeplineşte şi răspunde de aplicarea procedurilor legale în vigoare privind prelucrarea, stocarea sau transmiterea informaţiilor clasificate în format electronic;
25. **Securitatea datelor**
26. **Utilizator**
27. Monitorizează și operează aplicațiile puse în funcțiune, accesul și acțiunile la nivel de aplicație;
28. Monitorizează accesul la servicii, aplicaţii şi servere;
29. Asigură asistenţă tehnică şi suport pentru personalul din cadrul Consiliului Județean Cluj;
30. Concepe și impune identificarea de tehnici cum ar fi maparea datelor personale și securizarea acestora;
31. Clasifică corect documentele și controlul asupra acțiunilor fiecărui utilizator;
32. Implementează mecanisme de detecția a malware-ului avansat;
33. Implementează unui proces de actualizare (upgrade) pentru endpointuri, automatizat care nu-i lăsa utilizatorului posibilitatea de a amâna aceasta acțiune;
34. Implementează soluții de DLP (data loss prevention) care să blocheze informații confidențiale ce se încearcă să fie sustrase din organizație, pe medii interzise;
35. Instruieşte personalul din cadrul Consiliului Județean Cluj în utilizarea tehnicii de calcul din dotare şi exploatarea aplicaţiilor proprii;
36. Instalează, configurează şi administrează sistemele de operare utilizate în instituţie;
37. Instalează, configurează staţii de lucru, imprimante, scannere şi alte echipamente;
38. Instalează şi configurează programele de tip antivirus pe staţiile de lucru şi servere;
39. Asigură aprovizionarea cu materiale consumabile necesare bunei funcţionări a tehnicii de calcul din dotarea Consiliului Județean Cluj;
40. Monitorizează încărcarea echipamentelor și propune moduri de optimizare a utilizării acestora;
41. **Retea**
42. Face recomandările de securitate și le implementează, după cum urmează: pentru securitatea rețelei, pentru securitate la nivel de infrastructură, la nivel de utilizatori și aplicații, securitatea datelor, mentenanța datelor, răspuns la incidente, etc;
43. Colaborează cu celelalte compartimente pentru a asigura funcţionarea în bune condiţii a reţelei interne, a accesului la internet şi poşta electronică, a posturilor de lucru individuale.
44. Furnizează servicii de VPN, proxy, e-mail şi mesagerie instant pentru utilizatorii din reţelele internet şi intranet;
45. Asigură conectarea la internet a utilizatorilor reţelei şi stabileşte parametrii de routing;
46. Instalează şi configurează echipamente de reţea;
47. Administrează și monitorizează accesul în cadrul reţelelor (LAN, WAN);
48. **Management**
49. Evaluează în mod constant sistemele implementate din punct de vedere al eficienței, eficacității și flexibilității acestora, în vederea îmbunătățirii lor;
50. Implementează soluții de management a evenimentelor de securitate și folosește mecanisme avansate de protecție;
51. Implementează soluții de IAM (identity and acces management) integrată atât cu Active Directory, cât și cu toate aplicațiile de business folosite pentru management centralizat al accesului pe bază de autorizare și control al acțiunilor utilizatorilor / monitorizare și răspuns la incidente;
52. Implementează soluții de Privileged Identity Management (PIM) pentru utilizatorii privilegiați;
53. Implementează soluții de analiză a tranzacțiilor la nivel de Active Directory;
54. Asigură securitatea informaţiilor şi protecţia împotriva alterării şi distrugerii acestora;
55. Asigură suport tehnic pentru implementarea arhivei electronice și a centrului de date în sistemul informatic al Consiliului Județean CLUJ;
56. Implementează sisteme de management al securității informației (ISMS), de tipul ISO 27001, care să nu implice neapărat necesitatea unei certificări, dar care să urmărească cele mai bune practici în industrie;
57. **Baze de date**
58. Instalează, administrează, dezvoltă, optimizează și participă la culegerea şi introducerea informaţiilor în bazele de date;
59. Implementează soluții de criptare a fluxului de date între aplicațiile interne și baza de date și a criptării datelor stocate în bazele de date;
60. Realizează arhivarea datelor şi restaurarea lor în caz de incident;
61. Asigură securitatea informaţiilor şi protecţia împotriva alterării şi distrugerii acestora;
62. **Servere**
63. Administrează aplicaţiile şi serverele pe care sunt instalate, inclusiv accesul la aplicaţiile externe;
64. Actualizează (upgrade) la ultimele variante de sisteme de operare pentru servere;
65. Instalează şi configurează servere şi firewall-uri;
66. Administrează serverele WEB (care sunt fizice sau în cloud);
67. Implementează soluții de criptare a back-up-urilor.
68. Administrează sistemul de back-up al Consiliului Județean Cluj;
69. Aplică procedurile de salvare / restaurare de date pentru servere pentru a face posibilă restaurarea lor în caz de corupere sau distrugere;
70. Asigură supravegherea funcţionării echipamentelor de climă, securitate, grup generator în vederea asigurării condiţiilor optime de funcţionare a serverelor;
71. Implementează soluții de monitorizare și corelare log-uri provenite de la toate sistemele IT, inclusiv utilizatori și servere, care să ofere vizibilitate extinsă asupra posibilelor breșe;
72. **Email**
73. Monitorizează funcţionarea serviciilor oferite pe cale electronică şi defineşte strategiile de extindere a acestora;
74. Creează pe server conturi de mail şi configurează aceste conturi pe staţiile de lucru din reţeaua internă a Consiliului Județean Cluj;
75. **Site-uri**
76. Asigură gestionarea şi întreţinerea site-ului instituţiei, postează informaţiile primite de la direcţiile de specialitate;
77. Actualizează zilnic site-ul cu informaţii de interes public privind activitatea Consiliului Județean Cluj, în colaborare cu direcţiile de specialitate;
78. Realizează promovarea turistică prin intermediul mediului on-line;
79. Realizează actualizarea permanentă a site-ului [www.clujtourism.ro](http://www.clujtourism.ro);
80. Asigură coordonarea actualizării, pe site-ul instituției, la solicitarea scrisă a compartimentelor de specialitate, informaţiile de interes public, conform procedurilor în vigoare existente la nivelul Consiliului Județean Cluj;
81. Realizează teste de penetrare anuale pentru website-urile aflate sub gestiunea Consiliului Județean Cluj;
82. **Legis**
    1. Asigură administrarea aplicaţiei / site de legislaţie;
83. **Conferințe**
84. Asigură asistenţă tehnică în vederea desfăşurării în condiţii optime a videoconferinţelor organizate de către Consiliul Județean Cluj;
85. **Contracte service**
86. Monitorizează desfăşurarea activităţilor în cadrul contractelor de service şi întreţinere preventivă pentru echipamentele din dotare;
87. **Extern**
88. Urmăreşte asigurarea compatibilităţii şi interoperabilităţii sistemului informatic propriu cu sistemele informatice în exploatare şi cu reţele informaţionale de interes naţional sau local;
89. Exploatează şi monitorizează sistemul de comunicaţii de arie extinsă (WAN);
90. **GDPR**
91. Concepe și impune diligențele de tip GDPR, prin mecanisme și tehnici de identificare, guvernanță, securitate, analiză și raportare;
92. Impune și urmărește anumite măsuri tehnice pentru întărirea nivelul protecția datelor personale;
93. Implementează mecanisme de criptare și pseudonimizare la nivelul tuturor aplicațiilor – pe baza drepturilor de acces – dezvoltatorii acestor aplicații pot fi contactați pentru up-datarea soluțiilor pe baza noilor cerințe generate de prevederile GDPR;
94. Implementează sisteme de verificare a calității datelor, în special în ceea ce privește acțiunile de ștergere și suprimare necesare conform GDPR;
95. Implementează sisteme reale informatice de Case Management orientat GDPR care să realizeze managementul cererilor venite din partea cetățenilor pe baza drepturilor prevăzute de GDPR – de exemplu, dreptul de a fi uitat, de a fi informat, la opoziție, de portabilitate;
96. Implementează sisteme GRC (governance, risk and compliance) cu precădere orientat către GDPR care să monitorizeze conformarea sistemelor și a bunelor practici interne cu GDPR;
97. Organizează cursuri regulate (anuale) în cadrul organizației, susținute de către OPD și responsabil IT / securitate prin care să fie scoase în evidență toate procedurile interne, tipurile de atac la care utilizatorii trebuie să fie vigilenți și importanța acestor mecanisme pentru siguranța datelor;
98. Realizează audituri interne regulate din punct de vedere al prelucrării și protejării tuturor datelor dar și a datelor cu caracter personal;
99. **General**
100. Decide asupra modului de rezolvare a incidentelor semnalate şi în funcţie de gravitatea problemei, contactează furnizorii de servicii IT şi informează şeful ierarhic;
101. Asigură elaborarea referatelor și documentelor necesare pentru a asigura obținerea de certificate calificate pentru semnătura electronică ;
102. Monitorizează implementarea contractelor de achiziție a semnăturii electronice calificate și întreprinde demersurile necesare pentru achiziția periodică a semnăturii electronice calificate;