POLITICĂ DE SECURITATE IT
MĂSURI TEHNICE ȘI ORGANIZATORICE

A

OPTICNET SERV S.R.L.

cu privire la Regulamentul UE 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogarea Directivei 95/46/CE

INFORMAŢII CONTROL DOCUMENT

Numele Documentului	POLITICĂ DE SECURITATE IT MĂSURI TEHNICE SI ORGANIZATORICE
Categorie Document	Public
Proprietarul Documentului	OpticNet-Serv SRL
Autor	MUSCĂ Vasile
Data primei ediţii	1 nov 2018
Editia Documentului	1.0
Data aprobării	1 nov 2018
Aprobat de:	Director General OpticNet-Serv SRL MUSCĂ Vasile
Data următoarei revizii	

LISTĂ DE DISTRIBUŢIE

Revizia	Numele	Titlu/Companie
1.0	Vasile Musca	OpticNet Serv SRL

AUDITURI EFECTUATE

Data	Numele	Constatari audit
1 nov 2018	Vasile Musca	Conform

ISTORICUL REVIZIILOR

Numărul editiei/reviziei	Data aprobării	Modificări/Motivele modificării/Comentarii
1.0	1 nov 2018	Integral

POLITICĂ DE SECURITATE IT

Societatea OPTICNET SERV S.R.L. (denumită în continuare *„Compania”* sau *„Societatea”)* se aliniază Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului European – privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE *(denumit în continuare în prezentul plan “Regulamentul” sau „GDPR”)* aplicabil din data de 25 mai 2018.

Prezenta politică face parte din politica generală de securitate a informației care este parte integrantă din Sistemul de Management a Securității Informatiei din societate.

Sistemul de Management a Securității Informatiei din **OPTICNET SERV S.R.L.** este certificat în conformitate cu Standardul International **ISO 27001** pentru dezvoltare și furnizare servicii de comunicații electronice securizate, servicii de hosting, servere virtuale, servere dedicate, servere de aplicații, aplicații online și servicii cloud.

Prezenta politică vizează asigurarea de măsuri **adecvate** privind protecția datelor cu caracter personal cu care OPTICNET SERV S.R.L. intră în contact și se aplică:

- Sediilor și punctelor de lucru OPTICNET SERV S.R.L.
- Tuturor departamentelor OPTICNET SERV S.R.L.
- Întregului personal aparținând OPTICNET SERV S.R.L.
- Tuturor contractanților, furnizorilor și altor persoane care lucrează în numele OPTICNET SERV S.R.L.
- Paginilor de web si site-urilor de e-commerce operate de către OPTICNET SERV S.R.L.

Prezenta Politică are scopul de a conștientiza și familiariza personalul Societății OPTICNET SERV S.R.L. cu privire la metodele de protecție și securitate pentru asigurarea confidențialității, integrității și disponibilității informației. De asemenea prin această Politică se conturează metodele acceptabile de utilizare a resurselor informatice. Resursele informaționale vor fi utilizate într-o manieră aprobată, etică și în conformitate cu prevederile legale pentru a evita pierderea sau deteriorarea operațiunilor curente, a imaginii sau a activelor financiare. Angajații trebuie să se adreseze conducerii companiei înainte să se angajeze în orice activitate care nu este acoperită de prezenta politică.

OBIECTIVE:

a) Dezvoltarea unei strategii privind securitatea sistemelor informatice;
b) Promovarea standardelor etice în domeniul securității sistemelor informatice;
c) Asigurarea confidențialității, integrității și disponibilității resurselor informatice ale organizației;
d) Educarea personalului pentru a face față eficient amenințărilor cibernetice;

e) Cunoașterea riscurilor și amenințărilor venite din spațiul cibernetic;
f) Oferirea soluțiilor pentru a preveni și contracara amenințările cibernetice;

1. NOȚIUNI:

- **Operator** – entitatea, în cazul de față, OPTICNET SERV S.R.L., sau orice altă persoană juridică, autoritate publică, agenție sau organizație non-guvernamentală, care prelucrează sau stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal;

- **Date cu caracter personal** – orice informații privind o persoană fizică identificată sau identificabilă; o persoană identificabilă este acea persoană care poate fi identificată – direct sau indirect, prin referire la un element de identificare: nume/prenume, adresă, cod numeric personal, e-mail, telefon, venituri, date biometrice, imaginea, adresa de IP sau prin referire la datele medicale, genetice, datele privind originea etică sau rasială, convingeri politice, religioase, filosofice, culturale sau apartenența sindicală;

- **Prelucrare** – orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal (colectare, înregistrare, organizare, structurare, stocare, consultare, modificare, extragere, divulgare, restricționare, ștergere sau distrugere);

- **Persoana vizată** – orice persoană fizică ale cărei date cu caracter personal pot fi sau sunt prelucrate de operator;

- **Resurse IT** – toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unităţi de stocare şi toate activităţile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepţioneze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, să stocheze, să administreze date electronice, incluzând, dar nu limitat la: servere, calculatoare personale, calculatoare-agendă (*notebookuri*, *laptop*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), sisteme de procesare distribuită, echipament de laborator şi medical conectat la reţea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicaţii, medii de reţea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilităţile, programele şi datele care sunt proiectate, construite, puse în funcţiune (operaţionale) şi menţinute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia

- **Cont** – o entitate specificată printr-un identificator şi/sau parolă pentru accesul la sistemul de comunicaţie şi/sau la o resursă de calcul;

- **Utilizator** – o persoană, o aplicaţie automatizată sau proces utilizator autorizat să folosească Resursele IT

- **Administrator de rețea / IT** – responsabil la nivelul companiei cu administrarea tehnicii de calcul și a software-ului aferent. El poate fi intern sau externalizat.
- **Sistem de operare** – un ansamblu de programe care are rolul de a gestiona și de a facilita utilizatorului accesul la resursele sistemului de calcul
- **Server** – calculatorul pe care rulează una sau mai multe aplicații server
- **Aplicație server** – program de aplicație care furnizează servicii altor aplicații (numite aplicații client)
- **Aplicație internă** – aplicație de bază într-o companie, în care își desfășoară activitatea unul sau mai multe departamente
- **Active directory** – soluție software care pune la dispoziția administratorilor un mediu flexibil cu efect global pentru: asignarea permisiunilor, instalarea programelor, înnoirea securității
- **VPN (Virtual Private Network)** – extinde o rețea privată peste o rețea publică, precum internetul. Permite unui calculator sau unui dispozitiv ce poate fi conectat la rețea să trimită și să primească date peste rețele publice sau comune ca și cum ar fi conectat la rețeaua privată, beneficiind în același timp de funcționalitatea, securitatea și politicile rețelei publice
- **Antivirus / Antimalware** – software care este folosit în general pentru prevenirea și eliminarea virușilor de computer, viermilor și cailor troieni. De asemenea, poate detecta și elimina adware, spyware și malware
- **Back-up (copie de rezervă)** – Copii ale fişierelor şi aplicaţiilor făcute pentru a evita pierderea datelor şi pentru a permite recuperarea în cazul unor evenimente care pot conduce la pierderi de date
- **Incident de securitate** – În termeni informatici este definit ca un eveniment prin care se încearcă sau se realizează accesul la un sistem informatic, un atac asupra integrităţii şi/sau confidenţialităţii informaţiei de pe un sistem informatic automatizat. Aceasta include examinarea sau navigarea neautorizată, întreruperea sau anularea unui serviciu, date alterate sau distruse, prelucrarea (procesarea), stocarea sau extragerea informaţiilor, modificarea informaţiilor sistemului referitoare la caracteristicile componentelor hardware, firmware sau software cu sau fără ştiinţa sau intenţia utilizatorului.
- **Pen test** – un atac simulat autorizat asupra unui sistem informatic, efectuat pentru a evalua securitatea sistemului. Testul este efectuat pentru a identifica atât punctele slabe (denumite, de asemenea, vulnerabilități), inclusiv posibilitatea ca părțile

neautorizate să aibă acces la caracteristicile și datele sistemului, precum și punctele forte, permițând finalizarea evaluării complete a riscurilor

- **SPAM** - mesaje electronice trimise către o multitudine de destinatari în scopuri publicitare sau nelegale fără acordul acestora.

  Ce intră în această categorie:

  • mesaje publicitare nesolicitate

  • mesaje ce urmăresc realizarea unei fraude prin obţinerea de date confidenţiale.

- **Sistem de management a securității informației** – Sistem de management prin care se asigura securitatea informatiei în organizație în special în ceea ce priveste integritatea, confidentialitatea și diponibilitatea datelor si informatiilor
- **Sistem de management a securității informației certificat**– Sistem de management a securitatății informatiei din organizație care este certificat de terță parte în conformitate cu un standard de referință. În cadrul OpticNet-Serv SRL sistemul de management a securității informației este certificat în conformitate cu standardul ISO27001

2. IMPLICAȚII IT ÎN LUMINA REGULAMENTULUI UE 2016/679

Noul Regulament aduce mai multe referiri la domeniul IT, în menirea acestuia de a păstra securitatea datelor personale la un nivel adecvat cu volumul lor, dar și cu riscurile care reies din prelucrarea acestora. Astfel:

Articolul 5(2) și Articolul 30: Aceste articole obligă companiile să demonstreze că sunt aliniate cu GDPR. Alinierea trebuie demonstrată prin crearea și menținerea documentației care dovedește că o companie folosește monitorizarea și evaluarea vulnerabilităților.

Articolul 25 (1): Impune unei companii implementarea principiilor protecției datelor, ca de exemplu minimizarea suprafeței de atac. Aceasta măsură impune atât demersuri tehnice, cât și organizatorice.

Articolul 32: Impune de asemenea unei companii implementarea măsurilor tehnice pentru a asigura securitatea datelor. În particular:
- abilitatea de a asigura confidențialitatea, integritatea, disponibilitatea și reziliența sistemelor și serviciilor IT ;
- abilitatea de a restaura disponibilitatea accesului la datele personale într-un timp rezonabil în cazul unui incident de securitate.

Articolele 33 și 34: În cazul unui incident, aceste articole trimit la evaluarea, documentarea și notificarea acestuia.

Articolul 42 prevede posibilitatea instituirii mecanismelor de certificare în domeniul protecției datelor pentru demonstrarea faptului ca operațiunile de prelucrare respecta prezentul regulament. O buna practica este folosirea standardului ISO 27001 pentru asigurarea securității informației. Acest standard se bazează pe evaluare și tratare de riscuri de securitate a informațiilor și aplicarea de masuri adcvate care să asigure un anumit nivel de încredere în ceea ce privește securitatea informațiilor, inclusiv a preluclării datelor cu caracter personal.

De asemenea, GDPR introduce și conceptul de **Privacy by Design,** ceea ce înseamnă ca orice sistem IT software și hardware din companie va trebui să fie proiectat, implementat și exploatat cu respectarea confidențialității datelor personale prelucrate prin intermediul acestor sisteme.

O altă noutate care ține de domeniul IT este obligativitatea notificării autorității în cazul incidentelor de securitate, în maxim 72 de ore de la conștientizarea producerii acestuia.

3. POLITICI DE UTILIZAREA RESURSELOR IT

Aceste reguli privind modul de utilizare al resurselor IT - se aplică întregului personal, partenerilor și afaceri și colaboratorilor externi care au acces la sistemul informatic al Societății OPTICNET SERV S.R.L.

3.1. REGULI DE UTILIZARE:

1. Accesul la echipamentele IT ale organizației de către terți se va face sub supraveghere. În contractele cu tertii se vor include clauze privind măsurile de protecție a datelor și, în special, a datelor cu caracter personal;
2. Informațiile vor avea diferite grade de sensibilitate și importanță, informațiile personale (datele cu caracter personal) necesitând un nivel suplimentar de protecție, cu grad sporit pentru datele personale catalogate ca date sensibile;
3. Responsabilitatea angajaților privind securitatea va fi implementată încă din etapa recrutării și inclusă în contractele de muncă sau fișă postului și monitorizată permanent;
4. Parolele utilizate pentru autentificare sunt şiruri de caractere, adecvate din punct de vedere al securităţii ca lungime şi compoziţie, conform politicii interne de gestionare a parolelor.
5. Angajații firmei sau alte terțe părți care au acces la sistemele informatice ale organizației trebuie să semneze un contract de confidențialitate;
6. Angajații trebuie să fie instruiți anual cu privire la Politica de Securitate IT din companie;
7. Toate incidentele de Securitate vor fi raportate conducerii, pentru a decide dacă este cazul ca acestea să fie raportate Autorității de Supraveghere și/sau persoanelor vizate. Se va implementa în acest sens o Politică privind managementul adecvat al incidentelor de Securitate;
8. Informațiile de business critice sau sensibile, precum și datele cu caracter personal trebuie să fie păstrate în locuri sigure, protejate într-un perimetru de securitate adecvat, cu bariere de securitate corespunzătoare și controale de acces. Acestea ar trebui să fie protejate fizic împotriva accesului neautorizat, deteriorare şi interferenţe. Protecţia oferită trebuie să fie proporţională cu riscurile identificate, conform politicii de securitate IT în vigoare.
9. Utilizarea oricărui sistem IT va fi conformă legislației în vigoare.

10. Este strict interzisă distribuirea oricăror documente interne sau alte informații către persoane neautorizate;
11. Este strict interzisă orice modificare neautorizată a echipamentelor utilizate;
12. Este strict interzisă conectarea echipamentelor personale de orice fel (hard-diskuri interne sau externe, memory stick, laptop etc) la orice echipament al organizației (PC, server, rețea internă).
13. Toate sursele externe (CD, atașamente la e-mail, stick-uri, hard-disk etc) vor fi verificate cu un program anti-virus.
14. Este strict interzisă utilizarea sistemelor IT în alte scopuri decât îndeplinirea atribuțiilor de serviciu.
15. Este interzisă orice fel de bruscare a echipamentelor IT.
16. Este interzisă orice intervenție asupra echipamentelor IT de către personalul neautorizat.
17. Transportul laptopurilor este permis doar în geantă adecvată.
18. Se interzice folosirea oricărui echipament IT de către orice persoană care nu face parte din personalul Societății fără acordul prealabil al conducerii Societății.
19. Mijloacele de autentificare în sistem (username, parolă etc) aparțin fiecărui angajat și acesta este singurul responsabil de a nu divulga aceste informații.
20. Este strict interzisă utilizarea credențialelor altui angajat.
21. Fiecare angajat va fi responsabil să mențină securitatea oricărei informații, și în special informațiilor personale (datelor cu caracter personal) și să le protejeze de acces neautorizat (vizualizare, alterare, furt sau distrugere).
22. Pentru copierea fișierelor electronice, Societatea își rezervă dreptul de a depune plângere penală împotriva angajatului și de a-l acționa pe acesta la instanțele judecătorești competente pentru acoperirea oricărui prejudiciu adus firmei.
23. Este interzisă navigarea prin fișierele personale sau conturile altor angajați, cu excepția cazului în care acest lucru a fost aprobat în prealabil.
24. Programatorii care vor dezvolta sisteme IT nu vor avea acces la date cu caracter personal, decât în condițiile stabilite prin acordurile de confidențialitate încheiate cu terții de care aparțin
25. Personalul care asigură suportul tehnic nu va avea acces la date cu caracter personal, decât în situații excepționale și, în toate cazurile, cu respectarea tuturor obligațiilor impuse de Regulamentul (EU) 679/2016 persoanelor împuternicire și, în special, existența unor clauze contractuale exprese privind protecția datelor.
26. Notarea sau stocarea parolelor pe orice suport fizic este strict interzisă.
27. Sistemul trebuie blocat ori de câte ori angajatul părăsește biroul sau nu utilizează calculatorul pentru o perioada de 120 secunde.
28. După terminarea programului, calculatorul va fi închis. De asemenea, se va verifica faptul că închiderea s-a finalizat cu succes și fără erori.
29. Este strict interzisă utilizarea „Print screen-ului” (prin folosirea tastei print screen sau a altor procedee) sau prin fotografierea monitorului cu telefonul pentru a salva/imprima datele cu caracter personal existente pe monitor.
30. Listarea documentelor ce conțin date cu caracter personal se va realiza doar de către utilizatorii autorizați sau cu aprobarea scrisă și prealabilă a conducerii.

31. Angajații nu vor uita documente pe birou care conțin date cu caracter personal după terminarea programului sau în pauză.
32. Angajații vor lua din imprimantă documentele proprii imediat după tipărire.
33. Angajații care prelucreaza intens date cu caracter personal în cadrul societății vor avea pozitionat ecranul astfel incat să nu fie expus direct razei vizuale a altui angajat. În acest scop se pot folosi ecrane speciale de reducere a unghiului de vizibilitate.
34. Angajații vor folosi numai conturile de poștă electronică aprobate de societate. Mesajele trimise de pe aceste conturi vor fi strict destinate activității curente din companie.
35. Angajații nu vor deschide mesaje e-mail și nu vor accesa link-uri pe care nu le cunosc și care prezintă un risc de infectare pentru echipamentele pe care le exploatează
36. Angajații vor semnala departamentului IT orice mesaj de atenționare din partea programelor anti-virus și anti-malware instalalate pe echipamentele pe care le exploatează
37. Angajații se vor asigura ca în cazul transferului de informații ce conțin date cu caracter personal, au luat măsuri de securitate adecvate în funcție de volumul și tipul acestora (verificare destinatari, informare destinatari în spiritul confidențialității, parolare, criptare etc.) și că respectă politicile de confidențialitate ale companiei.

4. MĂSURI TEHNICE ȘI ORGANIZATORICE DE SECURITATE

4.1 MĂSURI LUATE DE ORGANIZAȚIE

Organizația se angajează să nu realizeze comunicări comerciale nesolicitate.

Toate comunicările comerciale vor avea la bază consimțământul persoanei, cu excepția situației în care legea prevede altfel.

Măsuri tehnice sunt implementate astfel încât consimțământul să poată fi retras la fel de simplu, precum a fost acordat.

În orice caz, retragerea consimțământului își va produce efectele în cel mult 48 de ore.

Orice newsletter va avea o opțiune de dezbonare, iar orice sms va avea o modalitate de retragere a contimțământului, fie link, fie apel telefonic, fie sms.

4.2 MĂSURI APLICABILE CONFORM SISTEM DE MANAGEMENT AL SECURITATII INFORMAȚIEI DIN OPTICNET-SERV SRL CERTIFICAT IN CONFORMITATE CU STANDARDUL ISO 27001

A.5. POLITICA DE SECURITATE
A.5.1. Politica de securitate a informatiilor
Obiectiv: Asigurarea de indrumari si suport managerial privind securitatea informatiilor, in conformitate cu cerintele afacerii, legile si reglementarile relevante.
A.5.1.1 Politici de securitatea informatiei
Stabileste directia si demonstreaza angajamentul managementului de la cel mai inalt nivel pentru
securitatea informatiilor.
A.5.1.2 Analiza politicilor de securitatea informatiei

Trebuie sa se asigure faptul ca politica in domeniul securitatii informatiilor este in mod continuu corespunzatoare chiar si in cazul unor modificari.

A.6. ORGANIZAREA SECURITATII INFORMATIEI

A.6.1. Organizarea interna

Obiectiv: Managementul securitatii informatiilor in cadrul organizatiei.

A.6.1.1. Roluri si responsabilitati Rolurile si responsabilitatile in domeniul securitatii ale angajatilor, furnizorilor si utilizatorilor tertului sunt definite si documentate in conformitate cu politica de securitatea informatiei a OpticNet Serv.

A.6.1.2. Separarea atributiilor Responsabilitatile din cadrul OpticNet Serv privind securitatea informatiilor sunt foarte clar precizate. Atributiile si zonele de responsabilitate incompatibile sunt separate, in vederea diminuarii posibilitatilor de modificare neautorizata / neintentionata sau utilizarea necorespunzatoare a resurselor organizatiei.

A.6.1.3. Contactul cu autoritatile Persoanele desemnate de conducerea OpticNet Serv mentin contacte corespunzatoare cu autoritati din domeniul legislativ, cu organizatii care elaboreaza regulamente si standarde, furnizori de servicii de informatii si operatori de telecomunicatii. Sunt mentinute contacte corespunzatoare cu autoritatile relevante.

A.6.1.4. Contact cu grupuri de interes specializate

OpticNet Serv a stabilit contacte corespunzatoare cu grupuri de interes, forumuri sau asociatii profesionale specializate in securitatea informatiei.

A.6.1.5. Securitatea informatiei in managementul proiectelor

Se aplica in cadrul fiecarui proiect.

A.6.2. Dispozitive mobile si teleworking

A.6.2.1. Politica privind dispozitivele mobile

OpticNet Serv a adoptat politica insotita de masuri de securitate pentru a administra riscurile introduse de utilizarea dispozitivelor mobile.

A.6.2.2. Teleworking Politica insotita de masuri de securitate trebuie implementata pentru a proteja informatiile accesate, procesate sau stocate la locatiile unde este utilizat teleworking-ul.

A.7. MANAGEMENTUL RESURSELOR UMANE

A.7.1. Inainte de angajare

Obiectiv: Asigurarea ca angajatii, partenerii contractuali si utilizatorii tertului isi inteleg responsabilitatile, corespund rolurilor/functiilor pentru care au avut in vedere, cat si reducerea riscului de furt, fraud dau utilizare necorespunzatoare a facilitatilor.

A.7.1.1. Verificarea preliminara

Verificarea tuturor candidatilor la angajare se realizeaza in conformitate cu legislatia, reglementarile si principiile de etica aplicabile. Verificarea este proportionala cu cerintele activitatii, cu nivelul de clasificare al informatiilor ce urmeaza a fi accesate si cu riscurile potentiale.

A.7.1.2. Termenii si conditii de angajare

Aranjamentele contractuale cu angajatii si contractorii stabilesc responsabilitatile acestora precum si pe cele ale organizatiei privind securitatea informatiei in OpticNet Serv.

A.7.2. Pe parcursul angajarii

Obiectiv: Asigurarea faptului ca angajatii, furnizorii si utilizatorii tertului sunt constienti de amenintarile si vulnerabilitatile privind securitatea informatiilor, de responsabilitatile si

obligatiile lor si ca sunt capabili sa sustina politica de securitate a organizatiei pe durata activitatii lor normale, cat si reducerea riscului de erori
umane.

A.7.2.1. Responsabilitatile Managementul OpticNet Serv solicita tuturor angajatilor / colaboratorilor sa aplice securitatea informatiei **OpticNet-Serv SRL**

A.7.2.2. Constientizare, educare si instruire in domeniul securitatii informatiilor

Toti angajatii/colaboratorii OpticNet Serv si, dupa caz, furnizorii si utilizatorii tertului, sunt constientizati, educati si instruiti cu privire la politicile si procedurile organizatiei, potrivit postului detinut.

A.7.2.3. Procesul disciplinar In cadrul OpticNet Serv incalcarea securitatii de catre angajati sau terti atrage dupa sine aplicarea procesului disciplinar, civil sau penal, dupa caz. Procesul disciplinar exista si este comunicat angajatilor.

A.7.3. Terminarea angajarii sau schimbarea incadrarii

Obiectiv: Asigurarea ca angajatii,colaboratorii, furnizorii si utilizatorii tertului pleaca din organizatie sau schimba incadrarea, in mod organizat.

A.7.3.1. Terminarea angajarii sau schimbarea incadrarii Da
Responsabilitatile si sarcinile privind securitatea informatiei care raman valabile dupa terminarea angajarii sau schimbarea incadrarii este definita si comunicata angajatului / colaboratorului si este urmarita aplicare ei.

A.8. MANAGEMENTUL RESURSELOR IT

A.8.1. Responsabilitatea pentru resurse

A.8.1.1. Inventarul resurselor In OpticNet Serv resursele asociate informatiilor si mijloacelor de analiza si procesare a informatiilor sunt identificate si se efectueaza inventarul acestor resurse.

A.8.1.2. Proprietatea asupra resurselor

Resursele inventariate au proprietar OpticNet Serv.

A.8.1.3. Utilizarea acceptabila a resurselor

In cadrul OpticNet Serv sunt identificate, documentate si implementate reguli pentru utilizarea acceptabila si judicioasa a informatiilor si resurselor asociate cu informatiile si mijloacele de procesare a informatiilor.

A.8.1.4. Returnarea resurselor Angajatii/colaboratorii OpticNet Serv si partile externe trebuie sa returneze toate resursele organizationale care se afla in posesia lor dupa terminarea angajarii sau contractului.

A.8.2. Clasificarea informatiilor

A.8.2.1. Classificarea informatiilor Exista proceduri privind clasificarea informatiilor.

A.8.2.2. Etichetarea informatiilor Informatiile sunt etichetate si utilizate conform gradului de clasificare.

A.8.2.3. Manipularea resurselor Sunt implementate proceduri privind manipularea resurseor, corespunzator gradului de clasificare a informatiilor.

A.8.3. Manipularea mediilor de stocare

A.8.3.1. Managementul mediilor de stocare amovibile

In cadrul OpticNet Serv sunt implementate proceduri pentru managementul mediilor de stocare amovibile in conformitate cu schema de clasificare.

A.8.3.2. Distrugerea mediilor de stocare

Mediile de stocare amovibile sunt casate in mod securizat si in siguranta.

A.8.3.3. Transferul fizic al mediilor de stocare

Mediile de stocare care contin informatii sunt protejate impotriva accesului neautorizat, utilizarii necorespunzatoare sau deteriorarii, pe durata transportului, in afara perimetrului fizic al organizatiei.

A.9. CONTROLUL ACCESULUI

A. 9.1. Cerinte organizationala privind controlul accesului

Obiectiv: Controlul accesului la informatii

A.9.1.1. Politica privind controlul accesului

In OpticNet Serv este stabilita, documentata si analizata politica de control a accesului, avand la baza cerintele organizatiei si cele de securitate privind accesul.

A.9.1.2. Accesul la retele si la servicii de retea

Responsabilul cu sistemul de management privind securitatea informatiei, impreuna cu coordonatorii de departament analizeaza drepturile de acces ale utilizatorului, la intervale de timp prestabilite, utilizand un proces formal.

A. 9.2. Managementul accesului utilizatorului

A.9.2.1. Autorizarea si revocarea
autorizarii utilizatorului

In cadrul OpticNet Serv este stabilita documentatia si analizata politica de control a accesului, avand la baza cerintele organizatiei si cele de securitate, privind accesul.

A.9.2.2 Asigurarea accesului utilizatorului

In cadrul OpticNet Serv este implementat un proces formal de asigurare a accesului utilizatorului pentru activarea sau revocarea drepturilor de acces pentru toate tipurile de utilizatori si toate sistemele si serviciile.

A.9.2.3. Managementul dreptului de acces privilegiate

OpticNet Serv dispune de mecanisme si protectii de securitate pentru alocarea si utilizarea drepturilor de acces privilegiat. Acestea sunt restrictionate si controlate.

A.9.2.4. Managementul informatiilor de autentificare secreta a utilizatorilor

Alocarea informatiilor de autentificare secreta este controlata printr-un proces formal de management.

A.9.2.5. Verificarea drepturilor de acces ale utilizatorilor

Detinatori resurselor verifica drepturile de acces ale utilizatorilor la intervale regulate.

A.9.2.6. Revocarea sau ajustarea drepturilor de acces

Drepturile de acces ale angajatilor, colaboratorilor, furnizorilor si utilizatorilor tertului la informatii si mijloacele de procesare a informatiilor, sunt revocate la incetarea angajarii, contractului sau conventiei acestora, ori adaptate conform schimbarilor survenite.

A.9.3. Responsabilitatile utilizatorului

A.9.3.1 Utilizarea informatiilor de autentificare secreta

In OpticNet Serv utilizatorilor li se solicita sa urmareasca practicele organizationale cu privire la utilizarea informatiilor de autentificare secreta.

A.9.4. Controul accesului la sistem si aplicatie

A.9.4.1. Restrictionarea accesului la informatii

Accesul utilizatorilor si a personalului de mentenanta la informatii si la functiile sistemelor de aplicatii este restrictionat.

A.9.4.2. Proceduri de conectare securizate

Accesul la sistemele de operare este controlat printr-o procedura de conectare autorizata.

A.9.4.3. Sistemul de management al parolelor

Sistemele de management al parolelor sunt interactive si asigura parole de calitat

A.9.4.4. Utilizarea programelor utilitare privilegiate
In cadrul OpticNet Serv este utilizat un sistem de parole eficace pentru autentificarea utilizatorilor.
A. 9.4.5. Accesul la codul sursa al programului
In cadrul OpticNet Serv accesul la codul sursa al programului este restrictionat.

A.10. CRIPTOGRAFIE
A.10.1. Controale criptografice
Obiectiv: Asigurarea operarii corecte si securizate a mijloacelor de procesare a informatiilor.
A.10.1.1 Politica privind utilizarea controalelor criptografice
In cadrul OpticNet Serv se utilizeaza certificate digitale si criptare. Este dezvoltata si implementata o politica de folosire a controalelor criptografice pentru protectia informatiei
A.10.1.2 Managementul cheilor de criptare
Managementul cheilor criptografice se face conform politicilor organizatiei.

A.11. SECURITATEA FIZICA SI A MEDIULUI
A.11.1. Zone de securitate
A.11.1.1. Perimetrul de securitate fizica
OpticNet Serv dispune de mecanisme si protectii de securitate pentru a proteja zonele unde se afla informatii si mijloace de procesare a informatiilor.
A.11.1.2. Controale fizice pentru intrari
Zonele de acces sunt protejate prin masuri corespunzatoare de securitate, ele fiind controlate pentru a asigura accesul numai a personalului autorizat.
A.11.1.3. Securizarea birourilor
In cadrul OpticNet Serv este conceputa si pusa in practica securitatea fizica a birourilor, incaperilor și dotarilor.
A.11.1.4. Protectia impotriva amenintarilor externe si de mediu
OpticNet Serv a intreprins masurile necesare pentru protectia fizica impotriva distrugerilor cauzate de incendiu, inundatie, cutremur, explozie, tulburari civile, si alte forme de dezastre naturale sau provocate de om.
A.11.1.5. Lucrul in zone sigure
In OpticNet Serv a fost conceputa protectia fizica si exista instructiuni pentru lucrul in zonele securizate.
A.11.1.6. Zonele de acces al publicului, de livrare si incarcare
Punctele de acces in locatia OpticNet Serv sunt tinute sub control. Persoane neautorizate care intra in incinta sunt controlate si pe cat posibil izolate de sistemele de procesare a informatiilor pentru a evita accesul neautorizat.
A.11.2. Echipament
Obiectiv: Asigurarea accesului utilizatorului autorizat si prevenirea accesului neautorizat la sistemele informatice.
A.11.2.1. Amplasarea si protejarea echipamentului
Echipamentul este amplasat si protejat pentru reducerea riscurilor datorate amenintarilor si pericolelor din mediul inconjurator, cat si a oportunitatilor de acces neautorizat.
A.11.2.2. Utilitati suport
Echipamentele sunt protejate impotriva caderilor de tensiune si altor intreruperii cauzate de caderea utilitatilor suport.
A.11.2.3. Securitatea cablarii

Cablurile electrice si de telecomunicatii utilizate pentru transportul datelor sau pentru portul serviciilor informatice, sunt protejate impotriva interceptarii sau deteriorarii.

A.11.2.4. Mentenanta echipamentului

Echipamentul este intretinut corect pentru a asigura permanenta disponibilitate si integritate.

A.11.2.5. Resurse scoase in afara organizatiei

Echipamentul, informatiile sau software-ul nu sunt scoase din organizatie fara autorizatie prealabila.

A.11.2.6. Securitatea echipamentului si resurselor scoase in afara organizatiei

In cadrul OpticNet Serv sunt aplicate masuri de securitate pentru resursele aflate in afara organizatiei luand in considerare diferitele riscuri implicate de lucrul in afara premiselor organizatiei.

A.11.2.7. Casarea in conditii desiguranta sau reutilizarea securizata a echipamentului

Toate componentele echipamentelor din OpticNet Serv continand medii de stocare sunt verificate pentru a asigura ca orice date de uz intern sau software licentiat au fost indepartate sau suprascrise in mod securizat inainte de casare.

A.11.2.8. Echipamenmt lasat nesupravegheat

Utilizatorul are obligatia de a se asigura ca echipamentul nesupravegheat este protejat corespunzator.

A.11.2.9. Politica biroului si ecranului curate

OpticNet Serv a adoptat o politica privind biroul curat (ce priveste hartiile si mediile de stocare amovibile) si ecranul curat (aplicabila sistemelor de procesare a informatiilor).

A. 12. SECURITATEA OPERATIILOR

A.12.1. Proceduri operationale si responsabilitati

A.12.1.1 Proceduri de operare documentate

Procedurile de operare utilizate sunt documentate, mentinute si puse la dispozitie tuturor utilizatorilor carora le sunt necesare.

A.12.1.2 Managementul schimbarii

Schimbarile care privesc mijloacele de procesare a informatiilor si sistemele, sunt tinute sub control.

A.12.1.3 Managementul capacitatii

Utilizarea resurselor este monitorizata si optimizata. Sunt efectuate proiectii ale cerintelor de capacitate viitoare pentru a asigura performanta necesara a sistemului.

A.12.1.4. Separarea medilor de dezvoltare, testare si operationale

Mediile de dezvoltare, testare si operationale sunt separate pentru a reduce riscurile de acces neautorizat sau schimbarile mediului operational.

A.12.2. Protectia impotriva programelor malitioase

A.12.2.1 Controale impotriva programelor malitioase

In OpticNet Serv sunt implementate masuri de control pentru a detecta, a preveni si a putea asigura recuperarea in cazul programelor malitioase. Aceste masuri sunt combinate cu constientizarea corespunzatoare a utilizatorilor.

A.12.3. Backup

Obiectiv: Protejarea confidentialitatii, autenticitatii sau integritatii informatiilor prin mijloace criptografice.

A.12.3.1. Backup al informatiilor

Periodic, personalul desemnat din OpticNet Serv efectueaza si testeaza copii de siguranta ale informatiilor, software-ului si sistemului in conformitate cu politica de backup a organizatiei.

A.12.3.2. Politica privind utilizarea masurilor de securitate criptografice

In cadrul OpticNet Serv se utilizeaza metode de criptare conform politicilorutilizate.

A.12.4. Inregistrare si monitorizare

A.12.4.1. Inregistrarea evenimentelor

Jurnalele de audit in care se inregistreaza activitatile utilizatorului, abaterile si evenimentele de securitate a informatiilor sunt generate si pastrate pe o perioada convenita pentru a fi utilizate in investigatii ulterioare si monitorizarea controlului accesului.

A.12.4.2. Protejarea informatiilor din jurnal

Mijloacele de inregistrare in jurnal si informatiile din jurnal sunt protejate impotriva falsificarii si accesului neautorizat.

A.12.4.3. Inregistrarea activitatilor administratorului si operatorilor

Activitatile administratorului de sistem si ale operatorilor sunt inregistrate in jurnale acre sunt protejate si sunt analizate periodic.

A.12.4.4. Sincronizarea ceasurilor

Ceasurile tuturor sistemelor importante de procesare a informatiilor din organizatie sau din domeniul de securitate sunt sincronizate cu o sursa convenita pentru ora exacta.

A.12.5. Controlul software-ului operational

A.12.5.1. Instalarea software-ului pe sisteme operationale

In OpticNet Serv sunt implementate proceduri de control pentru instalarea de software pe sisteme operationale.

A.12.6. Managementul vulnerabilitatii tehnice

***Obiectiv*: Reducerea riscurilor rezultate din exploatarea vulnerabilitatilor tehnice facute publice.**

A.12.6.1. Managementul vulnerabilitatilor tehnice

In cadrul OpticNet Serv sunt procurate informatii actuale despre vulnerabilitatile tehnice ale sistemelor informatice utilizate, este evaluata expunerea organizatiei la aceste vulnerabilitati si sunt luate masuri corespunzatoare pentru tratarea riscului asociat.

A.12.6.2. Restrictii la instalarea de software

In cadrul OpticNet Serv sunt stabilite si implementate reguli privind instalarea de software de catre utilizatori.

A.12.7. Consideratii privind auditul sistemelor informatice

Obiectiv: Cresterea eficacitatii si diminuarea interferentei cu/din procesul de auditare a sistemelor informatice.

A.12.7.1. Controalele privind auditul sistemelor informatice

In OpticNet Serv cerintele privind auditul si activitatile ce implica verificarea sistemelor operationale sunt planificate atent si aprobate pentru a reduce la minimum disturbarile activitatii organizatiei.

A.13. SECURITATEA COMUNICATIILOR

A.13.1. Gestionarea securitatii retelei

A.13.1.1 Controalele retelei

Retelele sunt administrate si controlate in asa fel incat sa se protejeze informatiile aflate in sisteme si aplicatii.

A.13.1.2 Securitatea servicilor de retea

Mecanismele de securitate, nivelurile de furnizare a serviciilor si cerintele de administrare a tuturor serviciilor de retea sunt identificate si incluse in contractele referitoare la serviciile de retea, indiferent ca acestea sunt furnizate din intern sau sunt externalizate.

A.13.1.3 Segregarea in retele diferite

Grupurile de servicii informatice, utilizatorii si sistemele informatice sunt separate in retele diferite.

A.13.2. Transferul informatiilor

A.13.2.1. Politici si proceduri privind schimbul de informatii

In OpticNet Serv exista implementate politici, proceduri si masuri de securitate formale, pentru schimbul de informatii.

A.13.2.2. Acorduri privind transferul informatiilor

Sunt stabilite acorduri care sa trateze transferul sigur al informatiilor intre OpticNet Serv si parti externe.

A.13.2.3. Mesageria electronica

Informatiile implicate in trimiterea si procesarea mesajelor electronice sunt protejate corespunzator.

A.13.2.4. Confidentialitate sau intelegeri privind nedivulgarea informatiilor

In cadrul OpticNet Serv sunt identificate, analizate la intervale regulate si documentate cerintele legate de confidentialitate sau nedivulgarea informatiilor in conformitate cu nevoile organizatiei.

A.14 ACHIZITIA, DEZVOLTAREA SI MENTENANTA SISTEMELOR INFORMATICE

A.14.1 Cerinte de securitate pentru sistemele informatice

Obiectiv: Asigurarea faptului ca securitatea este parte integranta a sistemelor informatice.

A.14.1.1 Analiza si specificarea cerintelor de securitatea informatiei

Specificatiile cuprinzand cerintele organizationale pentru noile sisteme informatice sau pentru imbunatatirea sistemelor existente, precizeaza cerintele pentru masurile de securitate.

A.14.1.2 Securizarea aplicatiilor in retelele publice

Informatiile transmise prin aplicatiile din retelele publice sunt protejate impotriva fraudelor, litigiilor contractuale si divulgarii sau modificarii neautorizate.

A.14.1.3 Protejarea aplicatiilor pentru tranzactii

Informatiile utilizate in aplicatiile pentru tranzactii in OpticNet Serv sunt protejate pentru a preveni transmiterea incompleta, directionarea gresita, modificarea neautorizata a mesajului, divulgarea neautorizata, duplicarea neautorizata a mesajului sau raspunsul neautorizat la mesaj.

A.14.2. Securitatea in procesele de dezvoltare si suport

A.14.2.1. Politica privind dezvoltarea in conditii de siguranta

In OpticNet Serv sunt stabilite reguli pentru dezvoltarea de software si sisteme aplicate activitatilor de dezvoltare din cadrul organizatiei.

A.14.2.2. Proceduri de control al modificarilor din sistem

Schimbarile aduse sistemelor in cursul ciclului de viata al dezvoltarii sunt controlate prin utilizarea unor proceduri de control al modificarilor.

A.14.2.3. Analiza si specificarea cerintelor de securitatea informatiei

Cerintele referitoare la securitatea informatiei sunt incluse in cerintele pentru sisteme informatice noi sau cele pentru imbunatatirea sistemelor existente.

A.14.2.4. Restrictii la modificarea pachetelor software

Modificarile la pachetele software trebuie descurajate, limitate la necesitati si controlate strict.

A.14.2.5. Principii privind ingineria sistemelor sigure

Sunt stabilite, documentate, mentinute si aplicate principii privind ingineria sistemelor sigure pentru toate activitatile de implementare a sistemelor informatice.

A.14.2.6. Mediu de dezvoltare securizat

OpticNet Serv a stabilit si protejeaza corespunzator medii de dezvoltare securizate pentru dezvoltarea si integrarea de sisteme care sa acopere intregul ciclu de viata al dezvoltarii sistemului.

A.14.2.7. Externalizarea dezvoltarii

OpticNet Serv supervizeaza si monitorizeaza activitatea de dezvoltare externalizata a sistemului.

A.14.2.8. Testarea securitatii sistemului

Testari ale securitatii din punct de vedere functional se deruleaza pe parcursul dezvoltarii.

A.14.2.9. Testarea de acceptanta a sistemului

Sunt stabilite programe de testare de acceptanta si criterii aferente pentru sistemele informatice noi precum si pentru upgrad-urile la versiuni noi

A.14.3. Date de testare

A.14.3.1. Protejarea datelor de testare

Datele de testare sunt selectate cu atentie, protejate si controlate.

A.15. RELATIA CU FURNIZORII

A.15.1. Securitatea informatiei in relatiile cu furnizorii

A.15.1.1. Politica privind securitatea informatiei in relatiile cu furnizorii

OpticNet Serv agreaza impreuna cu furnizorii si cerintele documentate de securitatea informatiei menite sa reduca riscurile asociate cu accesul furnizorului la resursele organizationale.

A.15.1.2. Includerea aspectelor referitoare la securitatea informatiei in contractele cu furnizorii

In OpticNet Serv toate cerintele relevante pentru securitatea informatiei sunt stabilite si agreate cu fiecare furnizor care ar putea accesa, procesa, depozita, comunica sau furniza componente de infrastructura IT

A.15.1.3. Lant de aprovizionare cu tehnologie IT

In contractele cu furnizorii, OpticNet Serv a inclus cerintele care sa trateze riscurile cu privire la securitatea informatiei, asociate cu produsele si serviciile IT.

A.15.2. Managementul furnizarii serviciilor de catre furnizori

A.15.2.1. Monitorizarea si analiza serviciului furnizorului

Conducerea OpticNet Serv monitorizeaza in mod regulat, analizeaza si auditeaza modul de furnizare a serviciilor de catre furnizor.

A.15.2.2. Managementul schimbarilor in serviciile furnizorului

Schimbarile in furnizarea de servicii de catre furnizori, inclusiv mentinerea si imbunatatirea politicilor, procedurilor si controalelor existente de securitatea informatiei trebuie administrate tinand cont de criticalitatea informatiilor medicale si nonmedicale, sistemele si procesele implicate si reevaluarea riscurilor.

A.16. MANAGEMENTUL INCIDENTELOR DE SECURITATEA INFORMATIEI

A.16.1. Managementul incidentelor de securitatea informatiei si imbunatatiri

A.16.1.1. Responsabilitati si proceduri In OpticNet Serv sunt stabilite responsabilitati si proceduri pentru a asigura un raspuns rapid, eficace si corespunzator la incidentele de securitatea informatiei.

A.16.1.2. Raportarea evenimementelor de securitatea informatiei

In OpticNet Serv se raporteaza orice eveniment cu privire la securitatea informatiei prin canale de management corespunzatoare.

A.16.1.3. Raportarea breselor de securitatea informatiei

In OpticNet Serv se inregistreaza si se raporteaza orice bresa de securitate observata sau suspectata.

A.16.1.4. Evaluarea si decizia cu privire la evenimentele de securitatea informatiei

Evenimentele de securitatea informatiei sunt evaluate in vederea deciderii daca ele vor fi clasificate ca si incidente de securitatea informatiei.

A.16.1.5. Raspuns la incidentele de securitatea informatiei

In OpticNet Serv la incidentele de securitatea informatiei, se raspunde in conformitate cu procedurile documentate.

A.16.1.6. Invatarea din incidentele de securitatea informatiei

Cunostintele acumulate din analiza si rezolvarea incidentelor de securitatea informatiei sunt utilizate pentru a reduce posibilitatea de producere sau impactul incidentelor viitoare.

A.16.1.7. Colectarea de probe

OpticNet Serv aplica proceduri pentru identificarea, colectarea, achizitia si pastrarea informatiilor care pot servi ca si probe in investigarea incidentelor de securitate.

A.17. ASPECTE DE SECURITATEA INFORMATIEI IN MANAGEMENTUL CONTINUITATII ACTIVITATII

A.17.1. Continuitatea securitatii informatiei

A.17.1.1. Planificarea continuitatii securitatii informatiei

Sunt determinate cerintele pentru securitatea informatiei si continuitatea securitatii informatiei in situatii dificile (ex. criza sau dezastru).

A.17.1.2. Implementarea continuitatii securitatii informatiei

OpticNet Serv stabileste, documenteaza, implementeaza si mentine procese, proceduri si controale pentru a asigura nivelul cerut de continuitate pentru securitatea informatiei in situatii dificile.

A.17.1.3. Verificarea, analiza si evaluarea continuitatii securitatii informatiei

Da OpticNet Serv verifica controalele stabilite si implementate pentru continuitatea securitatii informatiei la intervale regulate pentru a se asigura ca sunt valide si eficace in situatii dificile.

A.17.2. Redundante

A.17.2.1. Disponibilitatea mijloacelor de procesare a informatiei

In OpticNet Serv mijloacele de procesare a informatiei sunt implementate cu suficienta redundanta pentru a satisface cerintele de disponibilitate.

A.18. CONFORMITATE

A.18.1. Conformitate cu cerintele legale si contractuale

A.18.1.1. Identificarea legislatiei aplicabile si cerintelor contractuale

Toate cerintele legale, contractuale si de reglementare precum si abordarea organizatiei in indeplinirea acestora sunt identificate in mod explicit, documentate si actualizate pentru fiecare sistem informatic si pentru organizatie in ansamblu.

A.18.1.2. Drepturi de proprietate intelectuala

Exista proceduri implementate pentru a asigura conformitatea cu cerintele legale, de reglementare si contractuale referitoare la drepturile de proprietate intelectuala si utilizarea produselor sofware proprietare.

A.18.1.3. Protectia inregistrarilor

Este protejata intimitatea si asigurata protectia datelor cu caracter personal asa cum este cerut de legislatie si reglementari, dupa caz.

A.18.1.4. Intimitate si protectia datelor cu caracter personal

Se asigura intimitatea si protectia datelor cu caracter personal.

A.18.1.5. Reglementari privind masurile de securitate ce vizeaza criptografia

Masurile de securitate criptografice sunt in conformitate cu acordurile relevante, legislatia si reglementarile.

A.18.2. Analiza securitatii informatiei

A.18.2.1. Analiza independenta a securitatii informatiei

Abordarea organizatiei privind managementul securitatii informatiei si masurile de implementare (ex. obiective de control, politici, procese si proceduri pentru securitatea informatiei) este verificata in mod independent la intervale planificate sau ori de cate ori apar modificari substantiale.

A.18.2.2. Conformitate cu politicile si standardele de securitate

Conducerea analizeaza periodic conformitatea procesarii informatiei si procedurilor din zona lor de responsabilitate cu politicile, standardele si celelalte cerinte de securitate aplicabile.

A.18.2.3. Analiza conformitatii tehnice

Sistemele informatice sunt analizate periodic in ce priveste conformitatea cu politicile si standardele organziationale in domeniul securitatii informatiei.

CONSECINȚE

Nerespectarea prezentei Politici de către angajații companiei sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse Societății ca urmare a nerespectării prezentei Politici. Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), Societatea va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.