Ministerul Educaţiei și Cercetării

al Republicii Moldova   
Universitatea Tehnică a Moldovei

Faculatea Calculatoare, Infromatică și Microelectronică   
  
  
  
  
  
  
  
RAPORT

# LUCRARE DE LABORATOR NR. 6

# LA TEHNOLOGII ALE SECURITĂȚII INFORMAȚIONALE

**Tema:** Crearea politicilor de securitate bazate pe SMSI.

Au efectuat:

st. gr. TI-211 Budeanu Cristian

st. gr. TI-211 Popa Catalin

A verificat: Octavian Răducanu

UTM, Chișinău 2023

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | NUME | FUNCTIA | DATA | SEMNATURA |
| ELABORAT | Popa Cătălin | Director General | 01.05.2023 | **POPA** |
| VERIFICAT | Budeanu Cristian | Administrator | 04.05.2023 | **Budeanu** |
| APROBAT | Răducanu Octavian |  |  |  |

*Note:*

*1. Acest document contine informatii si date care sunt proprietatea S.C. Synergy Softworks*

*2. Prezentul document este destinat utilizarii exclusive pentru propriile cerinte.*

*3. Utilizarea integrala sau partiala a acestui document in orice scop sau activitate sau reproducerea partiala/ integrala in orice publicatie si prin orice procedeu (electronic, mecanic, fotocopiere, microfilmare etc) este interzisa fara acordul scris al PROPRIETARULUI.*

Sectiune introductiva

## Inregistrarea editiilor si reviziilor

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Revizia | Pag/Cap | Cauza reviziei | Descrierea modificarii | Autorul modificarii | Data |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Difuzare:

# Documentatia sistemului management al securitatii informatiei este disponibila pentru intreg personalul pe serverul societatii. Este mentinut un exemplar martor tiparit gestionat de RMI.

CUPRINS

|  |  |  |
| --- | --- | --- |
| Nr. capitol | Denumire capitol | Pagina |
|  | Sectiune introductiva Inregistrarea editiilor si reviziilor |  |
|  | Cuprins |  |
| 1.1 | Prezentarea si organizarea SC Synergy Softworks SRL |  |
| 1.2 | Organizarea SC Synergy Softworks SRL |  |
| 2 | Referinte normative |  |
| 3 | Termeni, definitii, abrevieri |  |
| 3.1 | Termeni de baza si definitii |  |
| 3.2 | Lista abrevierilor |  |
| 4 | Contextul in care SC Synergy Softworks SRL a proiectat si implementat sistemul de management al securitatii informatiei |  |
| 5 | Leadership |  |
| 5.1 | Leadershipul si obligatiile |  |
| 5.2 | Angajamentul Directorului General privind implementarea si imbunatatirea sistemului de management al securitatii informatiei |  |
| 5.3 | Politica in domeniul securitatii informatiei |  |
| 6 | Planificarea sistemului de management al securitatii informatiei |  |
| 6.1 | Analiza riscurilor si oportunitatilor pentru SMSI |  |
| 6.2 | Obiectivele SMSI si planul de atingere a acestora |  |
| 7 | Activitatile suport pentru SMSI |  |
| 7.1 | Resursele |  |
| 7.2 | Competenta |  |
| 7.3 | Constientizare privind cerintele SMSI |  |
| 7.4 | Comunicarea in cadrul SMSI |  |
| 7.5 | Documentarea informatiilor |  |
| 8 | Functionarea sistemului de management al securitatii informatiei |  |
| 8.1 | Planificarea operationalA si controlul sistemului de management al securitatii informatiei |  |
| 8.2 | Evaluarea riscurilor de securitatea informatiei |  |
| 8.3 | Tratarea riscurilor de securitatea informatiilor |  |
| 9 | Evaluarea performantelor SMSI |  |
| 9.1 | Monitorizarea, masurarea, analiza si evaluarea performantelor SMSI |  |
| 9.2 | Auditul intern |  |
| 9.3 | Analiza efectuata de management |  |
| 10 | Implementarea SMSI |  |
| 10.1 | Neconformitatea si actiuni corective |  |
| 10.2 | Imbunatatire continua |  |

***1.1. Prezentarea si organizarea SC Synergy Softworks SRL***

*1.1.1. Prezentarea SC Synergy Softworks SRL*

SC Synergy Softworks SRL, cu sediul in Chisinau, Ialoveni, Bulevardul Alexandru cel Bun 70, Republica Moldova, CIF MD 1122334, Nr. Reg.Com. J13/192/2022,

Compania are urmatoarele puncte de lucru:

Prezentarea organizatiei

Organizația SC Synergy Softworks SRL este o companie de tehnologie cu sediul în Chișinău, Ialoveni, Republica Moldova. Compania se specializează în furnizarea unei game largi de servicii IT, printre care se numără dezvoltarea de software, consultanță IT, securitate cibernetică, suport și mentenanță, precum și alte servicii.

Compania a fost înființată în anul 2022 și de atunci și-a consolidat poziția pe piața locală, devenind un jucător de încredere prin oferirea de soluții inovatoare și satisfacerea cerințelor clienților săi. Cu o echipă de specialiști talentați în domeniul IT, Synergy Softworks SRL livrează soluții personalizate pentru fiecare client, adaptate nevoilor și obiectivelor specifice ale acestora.

Politica internă a companiei se axează pe garantarea securității și confidențialității datelor clienților și este aliniată cu standardele ISO 27001. Synergy Softworks SRL dispune de o echipă specializată de experți în securitate cibernetică, care monitorizează în mod constant amenințările și vulnerabilitățile, luând măsuri avansate de securitate pentru a preveni orice incidente de securitate.

Cu un număr de 70 de angajați, Synergy Softworks SRL are departamente specializate în dezvoltare software, consultanță IT, securitate cibernetică și suport tehnic. Portofoliul de clienți al companiei include o gamă diversă de industrii, precum sectorul bancar, industria medicală, retail și altele.

Synergy Softworks SRL pune accentul pe îmbunătățirea continuă a serviciilor sale și pe satisfacția clienților. Prin oferirea de soluții personalizate, de înaltă calitate și performanță, Synergy Softworks SRL își propune să devină un partener de încredere pentru clienții săi și să rămână un jucător important pe piața de tehnologie din Republica Moldova și din regiune.

*1.2 Organizarea SC Synergy Softworks SRL*

1.2.1 Activitatea curenta a organizatiei este condusa de catre Director General, Popa Catalin și de Admnistratorul firmei, Budeanu Cristian.

Preocuparea noastra principala este de a oferi avantaj competitiv clientilor nostrii prin inovatie, excelenta, diversitate, profesionalism si pasiunea pentru munca noastra si pentru clientii nostri.   
  
1.2.2 In cadrul organizatiei exista o organigrama SC Synergy Softworks SRL actualizata

1.2.3 Organizarea, atributiile si responsabilitatile conducerii si personalului din SC Synergy Softworks SRL sunt definite prin decizii, fise post etc.

1.2.4 Pentru a raspunde cerintelor standardelor alese ca model de referinta in cadrul SMSI au fost definite responsabilitatile si autoritatea necesare pentru toate functiile/persoanele care au influenta asupra SMSI asa incat:

* sa se asigure resursele necesare proiectarii, implementarii si mentinerii sistemului de management al securitatii informatiei;
* sa fie definite politica si obiectivele sistemului de management al securitatii informatiei;
* sa se aloce autoritatea si responsabilitatea necesare Responsabilului SMSI pentru proiectarea, implementarea si mentinerea sistemului de management al securitatii informatiei;
* sa se asigure ca procesele necesare sistemului de management al securitatii informatiei sunt stabilite, implementate si mentinute;
* sa raporteze managementului de la cel mai inalt nivel al organizatiei despre functionarea si performanta sistemului de management al securitatii informatiei, in vederea analizei periodice a acestuia si despre orice neconformitati inclusiv recomandari pentru imbunatatire;
* raporteaza conducerii stadiul indeplinirii obiectivelor SMSI si monitorizeaza programele de management din
* domeniul SMSI;
* sa se asigure ca sistemul de management al securitatii informatiei este implementat si mentinut in conformitate cu cerintele standardelor de referinta;
* sa se initieze actiuni de prevenire a aparitiei neconformitatilor;
* sa se identifice, sa se analizeze si sa se inregistreze problemele legate de neconformitati;
* sa se initieze si/sau sa se intreprinda actiuni corective in vederea inlaturarii neconformitatilor;
* sa se verifice modul de implementare si eficacitatea actiunilor corective intreprinse;
* sa se controleze realizarea serviciilor in toate fazele, de la contractare si pana la receptia la client.

2. Referinte normative

Urmatoarele documente, in intregime sau partial, sunt referinte normative si sunt necesare pentru proiectarea, implementarea si mentinerea SMSI.

Pentru documentele datate numai editia citata se aplica. Pentru referintele nedatate, ultima editie a documentului se aplica.

Actele normative, standarde, normative, avizele si autorizatiile necesare, sunt tinute sub control de RMI .

Prin programele de instruire periodice, se face cunoscuta legislatia nou aparuta intregului personal al organizatiei.

Identificarea noilor cerinte legale, actualizarea celor existente cu noile prevederi legale si transmiterea catre cei interesati a prevederilor legale aparute sunt in responsabilitatea Directorului General. Fiecare coordonator de activitate are obligatia de a detine lista prevederilor legale aplicabile activitatilor coodonate si de a aduce la cunostinta subordonatilor sai cerintele legale nou aparute in departamentele de activitate desfasurate de acestia.

In cadrul documentatiei SMSI au fost elaborate liste cu documentele de reglementare a sistemului de management al securitatii informatiei.

In continure sunt prezentate cateva standardelor de referinta pentru SMSI:

SR ISO/CEI 27001:2013, Tehnologia informaţiei. Tehnici de securitate. Sisteme de management al securitaţii informaţiei. Cerinţe.

SR ISO/CEI 27002:2013, Tehnologia informaţiei. Tehnici de securitate. Cod de buna practica pentru managementul securitaţii informaţiei

SR ISO 31000: 2010. Managementul riscului. Principii si linii directoare.

SR EN ISO 19011: 2011. Ghid pentru auditarea sistemelor de management.

In cadrul organizatiei exista o lista actualizata cu documentele externe de reglementare pentru proiectarea, implementarea si mentinerea SMSI.

***3. Termeni, definitii, abrevieri***

*3.1 Termeni de baza si definitii*

Definitii:

actiune corectiva - actiune de eliminare a cauzei unei neconformitati detectate sau a altei situatii

nedorite;

audit – proces sistematic, independent si documentat in scopul obtinerii de dovezi de audit si de

evaluarea lor cu obiectivitate pentru a determina masura in care sunt indeplinite criteriile de audit;

capabilitate – abilitatea unei organizatii, sistem sau proces de a realiza un produs care va indeplini

cerintele pentru produs;

client - destinatar al unui produs furnizat de furnizor (sau executant). Prin client se poate intelege:

consumator final, utilizator, cumparator, beneficiar;

document – informatia impreuna cu mediul sau suport;

dovada obiectiva – date care sustin ca ceva exista sau este adevarat;

furnizor - organizatie care furnizeaza un produs clientului; intr-o situatie contractuala poate fi

denumit contractant.

furnizor poate fi: producatorul, distribuitorul, importatorul, montatorul sau organizatia prestatoare

de servicii;

imbunatatire continua - activitate repetata pentru a creste abilitatea de a indeplini cerinte.

inregistrare - document care furnizeaza dovezi obiective ale gradului de satisfacere a conditiilor

referitoare la securitatea informatiei;

neconformitate - nesatisfacere a unei conditii specificate. Neconformitatea poate fi: abaterea sau

absenta fata de conditiile specificate a unei sau mai multor caracteristici;

politica in domeniul al securitatii informatiei - obiective si orientari generale ale unei organizatii in

ceea ce priveste al securitatii informatiei, asa cum sunt exprimate oficial de catre managementul la

nivelul cel mai inalt;

proces - ansamblu de resurse si activitati interdependente care transforma datele de intrare in date

de iesire;

produs - rezultat al activitatilor sau proceselor; un produs poate cuprinde servicii, hardware,

materiale procesate, software sau o combinatie a acestora;

sistem de management al securitatii informatiei- structuri organizatorice, proceduri, procese si

resurse, necesare pentru implementarea SMSI.

structura organizatorica – responsabilitati, autoritati si relatii dispuse intr-o schema, prin care o

organizatie isi exercita functiile;

trasabilitate - aptitudine de regasire a istoricului, a utilizarii sau a localizarii unei entitati prin

identificari inregistrate;

validare - confirmare prin examinare si furnizare de dovezi obiective a faptului ca sunt satisfacute

conditiile particulare pentru o anumita utilizare, prevazuta;

verificare - confirmare prin examinare si furnizare de dovezi obiective a faptului ca au fost satisfacute

conditiile specificate.

resurse - orice prezinta valoare pentru organizaţie

disponibilitate - proprietatea de a fi accesibil si utilizabil la cerere de catre o entitate autorizata

confidenţialitat - proprietatea ca informaţia sa nu fie facuta disponibila sau divulgata persoanelor, entitaţilor sau proceselor neautorizate

securitatea informaţiei – pastrarea confidenţialitaţii, integritaţii si a disponibilitaţii informaţiei; in

plus, alte proprietaţi precum autenticitatea, responsabilitatea, non-repudierea si fiabilitatea pot fi de asemenea implicate

eveniment de securitate a informaţiilor - situaţie identificata in legatura cu un sistem, un serviciu sau o reţea care indica posibila incalcare a politicii de securitate a informaţiilor, un esec al masurilor de protecţie sau o situata ignorata anterior, dar relevanta din punct de vedere al securitaţii.

incident privind securitatea informaţiei - Un eveniment sau o serie de evenimente de securitate a informaţiei care au o probabilitate semnificativa de a compromite activitaţile organizaţiei si de a aduce ameninţari la securitatea informaţiei.

sistem de management al securitaţii informaţiei SMSI -- partea din intreg sistemul de management, bazata pe o abordare a riscului afacerii, folosita pentru a stabili, implementa, funcţiona, monitoriza, revizui, menţine si imbunataţi securitatea informaţiei

NOTA - Sistemul de management include structuri organizaţionale, politici, activitaţi de planificare, responsabilitaţi, practici, proceduri, procese si resurse.

Integritate proprietatea de a pastra acurateţea si deplinatatea resurselor

*risc residual* - riscul care ramane dupa tratarea riscului

*acceptarea riscului* - decizie de acceptare a unui risc

*analiza riscului* - utilizarea sistematica a informaţiei pentru a identifica sursele si pentru a estima riscul

*determinarea riscului* - procesul global de analiza si evaluare a riscului

*evaluarea riscului* - proces de comparare a riscului estimat cu criteriile de risc agreate in vederea stabilirii importanţei riscului

*managementul riscului* - activitaţi coordonate pentru indrumarea si controlul unei organizaţii luand in considerare riscurile

*tratarea riscului* - proces de selecţie si implementare a unor masuri in vederea reducerii riscului.

*declaraţie de aplicabilitate* - declaraţie documentata care descrie obiectivele de control si masurile de securitate care sunt relevante si aplicabile SMSI al organizaţiei.

*confidentialitate* - atribut de securitate care se referablocare accesului utiliztorilor neautorizati/ nelegitimi la informatii.

*integritatea* - atribut de securitate care se refera la protejarea informatiei de modificari neautorizate sau accidentate. Ex. stegere, adaugare, inlocuirea unei parti sau ainocuire in intregime.

*disponibilitatea* - atribut de securitate care se refera la punerea la dispozitia utilizatorilor legali a informatiei atunci cand acestia au nevoie conform reglementarilor stabilite.

*autenticitatea* - atributul de securitate care permite asocierea informatiei cu autorul ei. ( vezi si lege 455/2001)

*non-repudierea* - atribut de securitatea care permite asocierea informatiei cu dovada ca informatia fost trimisa de expeditor la destinatarul legal iar acesta a primit-o fara ca acestia sa poata contesta acest lucru.

*expunere a la risc* - o combinaţie de probabilitate şi impact, pe care le poate resimţi o organizaţie în raport cu obiectivele prestabilite, în cazul în care riscul se materializeaza. Se defineste ca produsul dintre probabilitate si impact conform formulei convenite.

NOTE - Obiectivele de control si masurile sunt bazate pe rezultatele si concluziile analizei de risc si pe procesele de tratare a riscului, cerinţe legale sau de reglementare, obligaţii contractuale si cerinţele afacerii organizaţiei pentru securitatea informaţiei.

*criptare* - Procesul de transformare a unui text simplu in text cifrat aplicand un algoritm care rearanjeaza sau il schimba in ceva de nerecunoscut.

*firewall*  - Un sistem configurat special care serveste drept poarta de siguranta intre o retea externa (ex.: Internet), si retelele interne ale organizatiei.

*hacker*  - un individ care acceseaza un sistem dejucandu-i siguranta pentru scopuri rau intentionate .

*intranet* - O retea locala care poate sa nu fie conectata la Internet, dar care are functii similare. Unele organizatii creeaza servere World Wide Web servers pentru propriile lor retele, astfel incat angajatii sa aiba acces la documentele web ale organizatiei.

*internet* - O retea de comunicare electronica care conecteaza retelele calculatoarelor si facilitatile computerelor din intreaga lume,

*ISDN -* (Integrated Services Digital Network) - Linii de telecomunicatie digitala care pot transmite servicii de voce si digitale.

*LAN*  - Un set de conexiuni intre computere care reprezinta baza transmiterii electronice a informatiilor, in general intr-o zona geografica restransa, ce deserveste o singura organizatie.

*cal troian* - Un program care pretinde a fi ceva ce nu este, in general pentru a sparge un cont sau pentru a folosi comenzile prin intermediul privilegiilor unui alt utilizator.

*virus*  - Un set de instructiuni care se gasesc intr-un software; si poate fi folosit pentru a distruge alte fisiere sau pentru a indeplini unele activitati in numele unui alt utilizator.

*worm* - Un program care se propaga dedublandu-se in fiecare gazda a retelei, cu scopul de a invada sistemele

*informatii sensibile* - Informatii sau cunostinte care ar putea duce la o pierdere de avantaje sau a nivelului de siguranta daca sunt dezvaluite altor persoane cu un nivel redus de incredere si/sau cu intentii necunoscute sau ostile.

*datele firmei* - Toate datele si toate Bunurile de Calcul ale Societatii inclusiv,dar fara a se limita la, Informatii Confidentiale; Informatii Proprietare; si Informatii Personale, fisiere, emailuri, mesaje instant si date in formate fizice si electronice.

*date personale* - Date de identificare personala, fisiere, documente si alte informatii, inclusiv Informatii personale protejate, din Bunurile de Calcul ale Societatii.

*datele clientilor* - Toate datele care apartin unui client.

*bunurile/ infrastructura de calcul* - Toate calculatoarele societatii, inclusiv, dar fara a se limita la laptopuri, PC-uri, servere, dispozitive de stocare, drivere, monitoare, sisteme de inregistrare, switch-uri, routere, faxuri, media si media mobile; telefoane mobile; BlackBerry, Retelele de calculatoare; software detinut si licentiat de societate; Cablajele Societatii; Perifericele Societatii etc.

3.2 Lista abrevierilor

SMSI - Sistemul de management al securitatii informatiei

M-SMSI - Manualul sistemului de management al securitatii informatiei

RMI- Reprezentantului managementului integrat ( aceasta persoana este si Responsabilul cu SMSI)

P - Procedura

P- Politica

4. Contextul in care SC Synergy Softworks SRL a proiectat si implementat sistemul de management al securitatii informatiei

Intelegerea organizatiei si contextul

SC Synergy Softworks SRL a determinat problemele interne si externe care sunt relevante pentru scopul propus si care afecteaza abilitatea de a atinge rezultatele asteptate ale sistemului de management a securitatii informatiei.

Intelegerea nevoilor si asteptarilor partilor terte

SC Synergy Softworks SRL a determinat:

* + - Partile interesate care sunt relevante pentru sistemul de management al informatiei si
    - Cerintele acestor parti interesate relevante pentru securitatea informatiei. Cerintele partilor interesate includ cerinte si obligatii contractuale.

Determinarea scopului sistemului de management al securitatii informatiei

SC Synergy Softworks SRL a determinat limitele si aplicabilitatea a sistemului de management al securitatii informatiei pentru stabilirea scopului in conformitate cu cerintele politicii MSIS si declaratia de aplicabilitate.

La determinrea scopului, SC Synergy Softworks SRL a luat in considerare urmatoarele elemente:

* posibile problemele interne si externe care afecetaza SMSI
* cerintele cu referinta pentru SMSI
* interfetele si dependentele dintre activitatile desfasurate de SC Synergy Softworks SRL si cele care sunt efectuate de alte organizatii.

In cadrul organizatiei se realizeaza periodic analize ale mediului de afaceri si contextului in care SMSI este implementat si mentinut. Acest document nu este anexat la manualul SMSI.

***5. Leadership***

* 1. *Leadershipul si obligatiile*

Managementul de top demonstreaza leadership prin respectarea sistemului de management al securitatii informatiei prin:

* asigurarea politicii de securitate a informatiilor si a obiectivelor de securitate a informatiilor care sunt stabilite si sunt compatibile cu directia strategica de dezvoltarea a SC Synergy Softworks SRL;
* asigurarea integrarii cerintelor sistemului de management de securitate a informatiilor in
* procesele SC Synergy Softworks SRL ;
* asigurarea ca resursele necesare pentru sistemul de management al securitatii informatiei sunt disponibile;
* comunicarea importantei gestionarii eficiente a securitatii informatiilor si de conformare la cerintele de sistem de management al securitatii informatiilor;
* asigurarea ca sistemul de management al securitatii informatiei atinge rezultatele stabilite;
* orientare si sprijinirea persoanelor implicate in aasigurarea eficacitaii si eficientei SMSI;
* promovarea imbunatatirii continue
* sprijinirea personalului pentru implementarea, mentinerea si impunatatirea SMSI.

5.2. Angajamentul Directorului General privind implementarea si imbunatatirea sistemului de management al securitatii informatiei (in continuare sunt prezentate doar cateva aspecte privind angajamentul managementului pentru proiectarea, implementarea, mentinerea si imbunatatirea SMSI)

Directorul General considera ca succesul SC Synergy Softworks SRL si atingerea obiectivelor SMSI pot fi realizate numai prin implicarea tuturor salariatilor si va urmari asigurarea resurselor si mijloacelor necesare pentru realizarea serviciilor intr-un mediu stimulativ bazat pe colaborarea pe orizontala si pe verticala in cadrul companiei precum si cu toti partenerii.

Sistemul de managemental securitatii informatiei aflat in subordinea directa a Directorului General acopera toate subdiviziunile organizatorice ale organizatiei si va fi utilizat, imbunatatit si extins in cadrul intregii organizatii, pentru a asigura eficienta si eficacitatea activitatilor.

Directorul General SC Synergy Softworks SRL isi exprima angajamentul ferm pentru:

* indeplinirea politicilor in ceea ce priveste securitatea informatiei pentru serviciile care se realizeaza
* prin implicarea tuturor angajatilor;
* respectarea si aplicarea integrala a prevederilor SMSI, obligatorie pentru intreg personalul
* organizatiei; imbunatatirea continua a sistemului de management al securitatii informatiei.

Reprezentantul managementului pentru sistemul de management al securitatii informatiei este Resposabilul SMI, acesta este direct responsabil de asigurarea functionarii sistemului de management al securitatii informatiei.

Politica in domeniul sistemului de management al securitatii informatiei va fi actualizata periodic pentru a asigura adaptare continua la necesitatile organizatiei si va fi disponibila atat pentru salariati, cat si pentru clienti sau partile interesate.

Pentru indeplinirea obiectivelor organizatiei s-au identificat riscurile aplicabile (inclusiv amenintarile, vulnerabilitatile, impactul si probabilitatea de aparitie) determinandu-se riscurile ce trebuie tratate. Pentru a le trata s-au aplicat masuri tehnice de securitate la nivelul fizic, al resurselor umane dar si la nivel informatic (configurare si dispunere echipamente hardware, aplicatii software). Masurarea eficacitatii implementarii masurilor de securitate referitoare la obiectivele organizatiei si riscurile existente cu privire la SMSI se realizeaza prin audit intern.

Managementul companiei furnizeaza dovezi ale angajamentului sau la planificarea, stabilirea, implementarea, operarea, monitorizarea, analizarea, mentinerea si imbunatatirea SMSI si a serviciilor prin:

1. stabilirea si comunicarea domeniului de aplicare a SMSI, politicii si obiectivelor de management al serviciilor;
2. asigurarea faptului ca planul de gestionare a serviciului este creat, implementat si mentinut in scopul de a adera la politicile SMSI;
3. imbunatatirea comunicarii privind serviciile;
4. imbunatatirea comunicarii referitoare la cerintele legale si de reglementare si obligatiile contractuale;
5. asigurarea furnizarii de resurse;
6. efectuarea analizelor legate de management la intervale planificate;
7. asigurarea ca riscurile referitoare la servicii sunt evaluate si gestionate.

Director General, Popa Cătălin

In cadrul organizatiei exista un document semnat de Directorul General privind anagajamentul pentru proiectarea, implementarea, mentinerea si imbunatatirea SMSI.

Documentul complet se actualizeaza periodic si nu face parte din manualul SMSI din considereate de eficienta a documentatiei SMSI.

***5.3. Politica in domeniul securitatii informatiei***

(in continuare sunt prezentate doar cateva aspecte privind politica in domeniul securitatii informatiei)

*5.3.1. Cerinte generale privind politica in domeniul securitatii informatiei*

Managementul de top a stabilității o politica informationala care:

* este specifica scopului organizatiei;
* include directii strategice pentru securitatea informatiei si furnizeaza cadrul pentru stabilirea obiectivelor pentru securitatea informatiilor;
* include un angajament pentru a satisface cerintele aplicabile securitatii informatiei
* include un angajament pentru imbunatatirea continua a sistemului de management al securitatii informatiei

Politica securitatii informatiei este disponibila partilor interesate.

Rolurile organizationale, responsabilitatile si autoritatile privind SMSI

Managementul SC Synergy Softworks SRL se asigura ca responsabilitatile si autoritatile pentru rolurile relevante pentru securitatea informatiei sunt atribuite si communicate.

Managementul SC Synergy Softworks SRL a atribuit responsabilitati pentru:

* a asigura ca sistemul de management al securitatii informatiei este in conformitate cu cerintele ISO 27001
* raportarea privind performanta sistemului de management al securitatii informatiei catre top managementul SC Synergy Softworks SRL.

*5.3.2. Politica privind sistemul de management al securitatii informatiei*

Conducerea Synergy Softworks srl precum si intreg personalul al organizatiei se angajeaza sa pastreze securitatea informatiilor proprii dar si a celor cu care intra in contact in sensul mentinerii confidentialitatii, integritatii si disponibilitatii acestora.

Scopul si domeniul de aplicabilitate pentru asigurarea securitatii informatiei se refera la urmatoarele activitati desfasurate de Synergy Softworks:

* Implementare și configurare de soluții de securitate: Compania oferă servicii de implementare și configurare a soluțiilor de securitate cibernetică, cum ar fi firewall-uri, sisteme de detecție a intruziunilor, soluții antivirus și anti-malware, și altele. Aceste activități asigură protecția adecvată a infrastructurii și datelor clienților.
* Monitorizare și răspuns la incidente de securitate: Synergy Softworks are o echipă dedicată de specialiști în securitate cibernetică care monitorizează în mod constant activitățile și evenimentele de securitate pentru a detecta și răspunde prompt la orice incidente sau încercări de atac. Această include monitorizarea sistemelor, analiză jurnalelor de evenimente și investigarea potențialelor amenințări.
* Testare de penetrare: Pentru a evalua nivelul de securitate al infrastructurii și sistemelor clienților săi, Synergy Softworks desfășoară teste de penetrare. Aceste activități implică încercarea controlată de a exploata vulnerabilități și de a identifica eventualele puncte slabe în sistemul de securitate al clienților.
* Educație și conștientizare în domeniul securității cibernetice: Compania organizează sesiuni de formare și programe de conștientizare a angajaților clienților în ceea ce privește bunele practici de securitate cibernetică. Acest lucru contribuie la creșterea nivelului de conștientizare și competență în domeniul securității informațiilor.
* Dezvoltare și implementare de politici și proceduri de securitate: Synergy Softworks ajută clienții să elaboreze și să implementeze politici și proceduri de securitate adaptate nevoilor lor specifice. Acestea includ politici de utilizare a sistemelor și a rețelelor, proceduri de gestionare a incidentelor de securitate și alte directive relevante.
* Servicii de recuperare după dezastru (Backup): Compania furnizează soluții și planuri de recuperare după dezastru pentru a asigura continuitatea afacerilor în caz de incidente majore sau dezastru natural. Aceste activități implică planificarea, implementarea și testarea soluțiilor de backup și de recuperare a datelor critice.

Aceste activitati se desfasoara in sediile din urmatoarrele locatii/ puncte de lucru:

* Chisinau, Ialoveni, Bulevardul Alexandru cel Bun 70, Republica Moldova.

In acest sens conducerea organizatiei a alocat resurse financiare si umane si sprijin pentru ducerea la indeplinire a urmatoarelor obiective legate de securitatea informatiei: protejarea bunurile informationale ale organizatiei noastre, ale clientilor si ale partenerilor, asigurarea continuitatii afacerii, minimizarea daunelor aduse afacerii prin prevenirea si minimizarea impactului incidentelor de securitate.

Ducerea la indeplinire a masurilor interne privind asigurarea securitatii informatiei va fi facuta in cadrul Comitetului de Securitate a Informatiei (CSI) din care fac parte: Directorul General, Responsabilul cu securitatea informatica si Responsabilul cu sistemul de management al securitatii informatiei/ Reprezentantul sistemului de management integrat.

CSI deleaga responsabilitatea implementarii, mentinerii si imbunatatirii sistemului de management al securitatii informatiei (SMSI) catre Responsabilul cu sistemul de management al securitatii informatiei/ Reprezentantul sistemului de management integrat.

Conducerea Synergy Softworks srl este preocupata si aloca resurse si pentru urmatoarele directii de dezvoltare:

* Cresterea satisfactiei partilor interesate prin imbunatatirea continua a performantei si calitatii produselor si serviciilor oferite;
* Protejarea bunurilor informationale ale organizatiei si ale partenerilor de toate amenintarile;
* Asigurarea confidentialitatii, integritatii si disponibilitatii informatiilor;
* Prevenirea incidentelor de securitate;
* Mentinerea si imbunatatirea continua a performantelor SMSI;
* Crearea unui sistem propriu de monitorizare a riscurilor;
* Desfasurarea proceselor in conformitate cu reglementarile interne si externe aplicabile organizatiei.

SC Synergy Softworks SRL a definit in mod clar nivelurile de autorizare care nu pot fi delegate.

Comitetul pentru Securitatea Informatiilor (CSI) este autoritatea finala pentru coordonarea SMSI. El aproba si autorizeaza toate modificarile politicii de securitate, declaratiei de aplicabilitate, manualului sistemului de management al securitatii informatiei, precum si oricarei alte politici separate (nivelul 1 al documentatiei).

Directorul General este autoritatea executiva pentru securitatea informatiei; aproba si emite toate documentele SMI.

Orice documente referitoare la securitatea informatiilor detinute personal de sefii de departament sunt aprobate si autorizate de catre directorul general.

Detinatorii activelor informationale, sunt responsabili pentru securitatea lor, clasificarea lor si pentru protectia lor activa si functionarea proceselor legate de securitate. Responsabilitatea pentru realizarea acestor procese sau a sarcinilor asociate poate fi delegata oricarui om aflat in zona de responsabilitate a proprietarului acestor informatii, cu conditia ca:

a) persoana sa aiba aptitudinile, competentele si resursele necesare pentru a efectua procesele sau a realiza sarcinile.

b) proprietarul isi pastreaza responsabilitatea de a se asigura ca procesul sau sarcina se efectueaza in mod corect.

Drepturile de acces sunt specificate in sectiunea - Cerintele afacerii pentru controlul accesului. Drepturile de acces sunt personale, sunt stabilite in acordurile individuale de utilizare (vezi: cap. „Managementul accesului utilizatorului” si „Responsabilitatile utilizatorului” si nu pot fi delegate.

Procedurile de autorizare pentru noile locatii si facilitati de prelucrare a informatiilor vor fi stabilite de CSI in functie de procesele desfasurate in locatia respectiva si de conditiile locale.

Documentatia SMSI SC Synergy Softworks SRL este protejata si controlata. Exista o procedura documentata „Controlul documentelor”, care ia in considerare - Nivelurile de Autorizare si stabileste actiunile de management pentru controlul documentelor.

SC Synergy Softworks SRL a implementat procedura „Controlul inregistrarilor” care defineste controalele pentru identificarea, pastrarea, protectia, extragerea, pastrarea in timp si distrugerea de inregistrari. Documentele sunt disponibile pentru cei care au nevoie si sunt autorizati pentru a le accesa, in conformitate cu aceste cerinte de pastrare.

Riscurile sunt identificate si definite in raport cu obiectivele a caror realizare este afectata de materializarea lor. Din aceasta cauza existenta unui sistem de obiective clar definite constituie premisa esentiala pentru identificarea si definirea riscurilor.

Metodologia descrisa se bazeaza pe identificarea efectului incertitudinii asupra atingerii obiectivelor.

Se defineste valoarea 4 ca fiind valoarea pragului de risc acceptat. Riscurile identificate cu valori intre [4, 50] nu sunt acceptate si trebuie tratate pentru a fi reduse sub valoarea pragului de risc acceptat prin aplicarea sistematica a masurilor de securitate.

Responsabilul cu gestionarea riscurilor numit prin decizie a managementului informeaza conducerea firmei daca nivelul de risc rezidual ramane peste valoarea de prag stabilita chiar si dupa aplicarea masurilor de tratare a riscurilor.

Implementarea, mentinerea si imbunatatirea SMSI se va face in baza riscurilor specifice de securitate a informatiei identificate de partile interesate. Criteriul in functie de care riscul trebuie evaluat depinde de impactul asupra organizatiei al exploatarii vulnerabilitatilor identificate de amenintarile specifice si al probabilitatii ca acest lucru sa se intample.

Personalul Synergy Softworks srl va duce la indeplinire sarcinile ce ii revin prin fisa postului precum si din prevederile regulamentului intern.

Orice abatere de la prevederile acestuia si de la normele interne de protejare a informatiei din domeniul de aplicabilitate se va pedepsi confrom Regulamentului Intern.

Toate incidentele de securitate trebuie raportate imediat RMI de catre persoana care le constata.

Responsabilul cu sistemul de management al securitatii informatiei/ Reprezentantul sistemului de management integrat este direct responsabil pentru ducerea la indeplinire a acestei politici, furnizarea de sprijin si indrumare pentru implementarea acesteia.

Toti managerii sunt direct responsabili de implementarea acestei politici in ariile lor de responsabilitate.

Este responsabilitatea fiecarui angajat al organizatiei noastre sa adere la aceasta Politica, sa cunoasca si sa aplice procedurile, normele si cerintele SMSI.

Toti angajatii organizatiei trebuie sa respecte prevederile legislatiei in vigoare (legea dreptului de autor, a protectiei datelor cu caracter personal etc) aplicabile domeniului de activitate dar si cele contractuale cu toate partile interesate.

Directorul general se angajeaza sa imbunatateasca continuu sistemul de management al securitatii informatiei si sa asigure resursele necesare realizarii obiectivelor propuse si aplicarii cerintelor SMSI.

Director General, Popa Cătălin

In cadrul organizatiei exista un document semnat de Directorul General privind Politica in domeniul securitatii informatiei.

Documentul complet se actualizeaza periodic si nu face parte din manualul SMSI din considereate de eficienta a documentatiei SMSI.

***6. Planificarea sistemului de management al securitatii informatiei***

*6.1. Analiza riscurilor si oportunitatilor pentru SMSI*

La planificarea sistemul de management al securitatii informatiei, SC Synergy Softworks SRL ia in considerare problemele

mentionate la punctul 4.1 (Intelegerea organizatiei si contextual) si cerintele mentionate la punctul 4.2 (intelegerea nevoilor si asteptarilor partilor terte) si determina riscurile si oportunitatile care trebuie sa fie abordate pentru:

* a asigura ca sistemul de management al securitatii informatiei poate atinge rezultatul prevazut prevenirea sau reducerea riscurilor si a efecte nedorite si
* realizareaa imbunatatirii continue.

6.1.1 SC Synergy Softworks SRL planifica:

* actiuni de abordare a acestor riscuri si oportunitati; si
* modul de integrarea si punerea in aplicare a actiunilor in procesul de implementarea a sistemului sau de management al securitatii informatiei sievalueaza eficacitatea acestor actiuni.

6.1.2 Evaluarea riscurilor de securitatea informatiilor

SC Synergy Softworks SRL defineste si aplica un proces de evaluare a riscurilor de securitate a informatiilor,

stabileste si mentine criterii de evaluare a riscurilor de securitate a informatiilor si

criteriile de acceptare a riscurilor.

SC Synergy Softworks SRL se asigura ca evaluarile riscurilor de securitate a informatiilor produc rezultate coerente, valabile si comparabile

La identificarea riscurilor de securitate a informatiilor se au in vedere elementele:

- se aplica procesul de evaluare a riscurilor de securitate a informatiilor pentru identificarea riscurilor asociate cu pierderea de confidentialitate, integritate si disponibilitate pentru informatii;

- se identifica proprietari de risc;

La analizarea riscurile de securitate de informatii sunt avute in vedere elementele:

- se evalueaza consecintele potentiale care ar rezulta daca riscurile identificate se materializeaza;

- se evalueaza probabilitatea realista a producerii riscurilor identificate; si

- se determina nivelurile de risc;

La evaluarea riscurile de securitate de informatii sunt avute in vedere elementele:

- se compara rezultatele analizei de risc cu criteriile de risc acceptat stabilite;

- se acorda prioritate riscurile analizate care depasesc nivelul de risc acceptat pentru implementarea de masuri de tratare a riscurilor.

SC Synergy Softworks SRL pastreaza informatiile documentate despre procesul de evaluare a riscurilor de securitate a informatiilor (registrul riscurilor si planul de masuri de tratare a riscurilor).

* + 1. *Tratarea riscurilor de securitatea informatiilor*

SC Synergy Softworks SRL defineste si aplica un proces de tratare a riscurilor de securitate a informatiilor la:

1. selectarea optiunilor adecvate de tratare a informatiilor cu risc de securitate, tinand seama de riscul calculat in urma evaluarii;
2. stabilirea tuturor controaleor care sunt necesare pentru punerea in aplicare a tratamentului riscului de securitate a informatiilor pentru varianta aleasa;
3. compararea controalele stabilite cu cele din anexa A si verificarea daca controale necesare nu au fost omise;

Politica P-015 contine metodologia de evaluare a riscurilor in cadrul SC Synergy Softworks SRL.

SC Synergy Softworks SRL elaboreaza planuri de informare privind tratarea riscului de securitate si mentine documentele informatizate cu privire la procesul de tratare a riscurilor de securitatea informatiei.

SC Synergy Softworks SRL a elaborat o declaratie de aplicabilitate care contine controalele necesare si justificare pentru incluziuni, indiferent daca acestea sunt puse in aplicare sau nu, precum si justificarea excluderii controalelor din anexa A/ ISO 27001. Acesta declaratie de aplicabilitate privin SMSI se actualizeaza periodic in functie de evaluarile riscurilor SMSI, declaratia nu este anexata manualui din considerente de eficientizare a documentatiei SMSI.

*6.2. Obiectivele SMSI si planul de atingere a acestora*

SC Synergy Softworks SRL stabileste obiectivele SMSI pentru functii relevante si diverse nivele iar obiectivele SMSI sunt :

* in concordanta cu politica de securitate a informatiilor;
* masurabile
* iau in considerare cerintele de securitate a informatiilor, daca este cazul, si rezultatele de la evaluarea riscului si tratarea riscurilor;
* sunt comunicate;
* sunt updatate;

SC Synergy Softworks SRL pastreaza documentele privind obiectivele SMSI. Atunci cand se planifica modul de a realiza obiectivele SMSI, SC Synergy Softworks SRL stabileste:

* ce trebuie facut;
* ce resurse vor fi necesare;
* cine va fi responsabil;
* cand vor fi terminate;
* cum vor fi rezultatele evaluate.

***7. Activitatile suport pentru SMSI***

Laproiectarea, implementarea, mentinerea SMSI organizatia are in vedere urmatoarele categorii de resurse: umane, informtionale, financiare, materiale si de timp.

*7.1. Resursele*

SC Synergy Softworks SRL determina si furnizeaza resursele necesare pentru stabilirea, implementarea, mentinerea si imbunatatirea continua a sistemului de management al securitatii informatiei.

*7.2. Competenta*

SC Synergy Softworks SRL asigura urmatoarele activitati:

* Determinarea necesarului de persoane competente care sa asigura functionarea SMSI fara sa afecteze performantele securitatii informatiei
* se asigura ca aceste persoane sunt competente pe baza educatiei adecvate, training sau experienta;
* daca este cazul, ia masuri pentru a dobandi competenta necesara, si evalueaza eficacitatea actiunilor intreprinse; si
* pastreaza informatiile documentate corespunzator ca dovada a competentei.

Actiunile implementate de SC Synergy Softworks SRL pot include: furnizarea de activitati de formare profesionala interna/ externa si participarea la conferinte pentru indrumarea angajatilor actuali; sau angajarea si contractarea de persoane competente.

*7.3. Constientizare privind cerintele SMSI*

Persoanele angajate in organizatie sunt constientizate privind:

* politica in domeniul SMSI
* contributia lor la asigurarea eficacitatii si eficientei sistemului de management al securitatii informatiei, inclusiv beneficiile de performanta de securitate a informatiilor imbunatatite; si
* implicatiile neconformitatilor in raport cu cerintele sistemului de management al securitatii informatiilor.
  1. *Comunicarea in cadrul SMSI*

SC Synergy Softworks SRL determina nevoile interne si externe pentru comunicarea relevanta in cadrul sistemului de management al securitatii informatiei incluzand:

* Ce se va comunica;
* Cand se va comunica;
* Cu cine se va comunica;
* Cine va comunica;
* Procesul prin care se va comunica va fi efectuat.

In cadrul SC Synergy Softworks SRL se desfasoara permanent un proces de comunicare interna, prin care se realizeaza informarea tuturor functiilor/ persoanelor din organizatie (dupa caz) cu privire la:

* politica in domeniul SMSI, obiectivele generale/specifice;
* cerintele si asteptarile partilor interesate;
* modul de organizare si desfasurare a proceselor SMSI;
* cerinte legale si de reglementare aplicabile;
* hotarari, decizii, schimbari organizatorice;
* cerintele documentelor si rezultatele functionarii SMSI, inclusiv privind eficacitatea acestuia;
* rezultatele actiunilor corective;
* riscurile SMSI evaluate si a masurilor de tratarea a acestora.

Alte elemente ale procesului de comunicare interna si externa referitoare la eficacitatea SMSI:

* instruirea personalului referitoare la cunoasterea SMSI, a procedurilor acestuia, a politicilor SMSI, si a obiectivelor SMSI;
* transmiterea datelor referitoare la cerintele partilor interesate catre functiile  relevante;
* circulatia intre toate nivelele ierarhice si in ambele directii a informatiilor referitoare la probleme legate de  (ne)conformitatea serviciului /procesului/ SMSI;
* accesul controlat la documentele de pe suport informatic;
* informari organizate referitoare la noutatile SMSI.

SC Synergy Softworks SRL se asigura prin proceduri ca informatii pertinente pentru SMSI sunt comunicate catre angajati si catre alte parti interesate. Implicarea anagajatilor si modalitatile de consultare sunt documentate.

Angajatii sunt:

* Implicati in dezvoltarea si revizuirea politicilor si procedurilor pentru a gestionarea riscurile SMSI;
* Consultati in cazul in care exista orice modificari care afecteaza SMSI.

Angajatii participa la dezvoltarea, revizuirea si actualizarea de politici, proceduri si reguli specifice SMSI. Aceasta se face prin: reuniuni, sedinte, emailuri etc.

Comunicarea cu partile interesate externe este coordonata de Responsabilul SMSI. Angajatii sunt informati privind cerintele SMSI de Responsabilul SMSI, se fac cursuri de formare, sedinte si se distribuie materiale de informare privind SMSI.

***7.5. Documentarea informatiilor***

* + 1. *Generalitati*

Sistemul de management al securitatii informatiei in SC Synergy Softworks SRL cuprinde:

* Informatiile documentate cerute de SMSI; si
* Informatiile documentate determinate de SC Synergy Softworks SRL ca fiind necesare pentru eficacitatea sistemului de management al securitatii informatiei.

Gradul de documentarea a informatiilor pentru sistemul de management al securitatii informatiei se poate modifica in timp in functie de urmatoarele criterii:

* marimea organizatiei si tipurile de activitati, produse sau servicii;
* complexitatea proceselor si interactiunile dintre ele; si
* competentele personalului.

Documentatia SMSI SC Synergy Softworks SRL contine inregistrari ale deciziilor de management ( ex. Decizi numire CSI, decizie numire RMI).

Documentatia SMSI include: politica SMSI, lista obiectivelor SMI; domeniul de aplicabilitate al SMSI; politici si proceduri, masuri de securitate pentru sustinerea SMSI (politici SMSI); o descriere a metodologiei de analiza a riscului ( conf. politica, ……….); raportul de analiza a riscului, planul de tratare a riscului (conform registrului riscurilor si planului de tratare a riscurilor SMSI); proceduri documentate de care are nevoie organizatia pentru a asigura planificarea eficcace , functionarea si controlul proceselor de securitate a informatiei si pentru cum se masoara eficienta masurilor de securitate ( conf. procedurilor ……….); inregistrarile cerute de standardul international; declaratia de aplicabilitate SMSI.

*7.5.2. Crearea si updatarea informatiilor*

Atunci cand informatiile documentate sunt create si updatate, SC……….. are in vedere urmatoarele elemente: identificarea si descrierea informatiilor (ex. Titlu, data, autor, numar de referinta) , formatul (ex. Limba, versiune software, grafic) si mediul ( ex. Hartie, electronic); revizuirea si aprobarea adecvata.

*7.5.3. Controlul documentelor*

Informatiile documentate cerute de sistemul de management al securitatii informatiilor sunt controlate pentru a se asigura:

* sunt disponibile si adecvate pentru utilizare, in cazul in care si atunci cand este necesar;
* si, aceastea sunt protejate in mod adecvat (de exemplu, de la pierderea confidentialitatii, utilizarii necorespunzatoare, sau pierderea integritatii si disponibilitatii etc).

Pentru controlul de informatii documentate, SC Synergy Softworks SRL are in vedere urmatoarele activitati, dupa caz:

* distributia, accesul, utilizarea
* depozitare si conservare;
* controlul modificarilor;
* mentinerea si disponibilitatea.

Informatiile documentate de origine externa, determinate de SC Synergy Softworks SRL ca fiind necesare pentru planificarea si functionarea sistemului de management al securitatii informatiei, se identifica, dupa caz, si sunt controlate.

Accesul la documentele controlate presupune o decizie cu privire la permisiunea numai de a vizualiza informatiile documentate sau permisiunea si autoritatea de a vizualiza si modifica informatiile documentate etc.

Documentele cerute de SMSI trebuie sunt protejate si controlate.

SC Synergy Softworks SRL a stabilit o procedura documentata pentru a defini actiunile conducerii pentru:

* a aproba documentele privind adecvarea inainte de a le emite;
* a revizui si actualiza documentele in functie de necesitate si a reaproba documentele;
* a asigura faptul ca schimbarile si revizia curenta a documentelor sunt identificate;
* a asigura faptul ca versiunile relevante ale documentelor aplicabile sunt disponibile la punctele de utilizare;
* a asigura faptul ca documentele raman inteligibile si pot fi identificate imediat;
* a asigura faptul ca documentele sunt disponibile celor care au nevoie de ele si sunt transferate,
* depozitate si distruse in conformitate cu procedurile aplicabile nivelului lor de clasificare;
* a asigura faptul ca documentele de origine externa sunt identificate;
* a asigura faptul ca distributia documentelor este controlata;
* a preveni utilizarea neintentionata a documentelor care nu mai sunt actuale; si
* a aplica mijloace de identificare adecvata a acestora daca acestea sunt pastrate pentru orice alt scop.

1. ***Functionarea sistemului de management al securitatii informatiei***

*8.1. Planificarea operationala si controlul sistemului de management al securitatii informatiei*

SC Synergy Softworks SRL planifica, implementeaza si controleaza procesele necesare pentru a satisface cerintele de securitatea informatiilor cerinte, precum si sa puna in aplicare actiunile stabilite pentru atingerea obiectivelor SMSI.

SC Synergy Softworks SRL pastreaza informatiile documentate in masura in care este necesar sa ofere incredere ca procesele SMSI au fost efectuate conform planului.

SC Synergy Softworks SRL controleaza modificarile planificate si revizuieste consecintele schimbarilor nedorite, si intreprinde masuri pentru a atenua orice efecte adverse, daca este necesar.

SC Synergy Softworks SRL se asigura ca procesele externalizate sunt determinate si controlate.

*8.2. Evaluarea riscurilor de securitatea informatiei*

SC Synergy Softworks SRL va efectua evaluari ale riscurilor de securitate a informatiei la intervale planificate sau atunci cand sunt propuse modificari semnificative sau apar, tinand cont de criteriile stabilite.

SC Synergy Softworks SRL pastreaza informatiile documentate cu privire la rezultatele evaluarilor riscurilor de securitate a informatiei.

SC Synergy Softworks SRL defineste si aplica un process de tratare a riscurilor de securitate a informatiilor la:

-selectarea optiunilor adecvate de tratare a informatiilor cu risc de securitate, tinand seama de riscul calculat in urma evaluarii;

-stabilirea tuturor controaleor care sunt necesare pentru punerea in aplicare a tratamentului riscului de securitate a informatiilor pentru varianta aleasa;

-compararea controalele stabilite cu cele din anexa A si verificarea daca controale necesare nu au fost omise;

Politica P-015 contine metodologia de evaluare a riscurilor in cadrul SC Synergy Softworks SRL.

Metoda aleasa pentru calculul nivelului de risc este:

Risc = Probabilitate x Impact x 10

Probabilitatea va avea valori intre 0 si 100% iar impactul intre 1 si 5 conform tabelului de mai jos:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Probabilitatea de aparitie** | | **Impact** | | | |
| **Confidentilitate** | **Integritate** | **Disponibilitate** | **Impact rezultat (C+I+D)** |
| Foarte ridicata | (80%-100%] -  Se intampla cel putin o data la 3 luni | 5 = impact major  Pierdere financiara  > 10 000 euro | 5 = impact major  Pierdere financiara  > 10 000 euro sau | 5 = impact major  Pierdere financiara  > 10 000 euro | 15 |
| Ridicata | (60%-80%] = prezenta foarte probabila  Se intampla anual | 4 =impact considerabil  Pierdere financiara cuprinsa in intervalul [6001, 10000] euro | 4 =impact considerabil  Pierdere financiara cuprinsa in intervalul [6001, 10000] euro | 4 =impact considerabil  Pierdere financiara cuprinsa in intervalul [6001, 10000] euro | 12 |
| Medie | (40%-60%] - prezenta probabila  S-a intamplat peste 5 ori in ultimii 3 ani | 3 = impact moderat  Pierdere financiara cuprinsa in intervalul [3001, 6000] euro | 3 = impact moderat  Pierdere financiara cuprinsa in intervalul [3001, 6000] euro | 3 = impact moderat  Pierdere financiara cuprinsa in intervalul [3001, 6000] euro | 9 |
| Redusa | (20%-40%] – prezenta putin probabila  S-a intamplat 2-3 in ultimii 3 ani | 2 = impact minor  Pierdere financiara cuprinsa in intervalul [1001, 3000] euro | 2 = impact minor  Pierdere financiara cuprinsa in intervalul [1001, 3000] euro | 2 = impact minor  Pierdere financiara cuprinsa in intervalul [1001, 3000] euro | 6 |
| Foarte redusa | (0%-20%] – prezenta neglijabila  S-a intamplat o singura data in ultimii 3 ani | 1 = impact  Foarte redus  Pierdere financiara  < 1000 euro | 1 = impact  Foarte redus  Pierdere financiara  < 1000 euro | 1 = impact  Foarte redus  Pierdere financiara  < 1000 euro | 3 |

Formula de calcul a riscului: Risc = Probabilitate x Impact x 10

Valoare maxima riscului = 150

Valoarea nivelului de risc acceptat de organizatie: 20

Intrucat produsul maxim poate avea valoarea 150 pentru nivelul de risc se defineste valoarea 4 ca fiind valoarea pragului de risc acceptat

Orice risc sub aceasta valoare este asumat de organizatie.

Riscurile identificate cu valori intre [20, 150] nu sunt acceptate si trebuie tratate pentru a fi reduse sub valoarea pragului de risc acceptat prin aplicarea sistematica a masurilor de securitate.

Responsabilul cu gestionare riscurilor numit prin decizie a managementului informeaza conducerea daca totusi nivelul de risc ramane peste valoarea de prag stabilita chiar si dupa aplicarea.

*8.3. Tratarea riscurilor de securitatea informatiilor*

SC Synergy Softworks SRL pune in aplicare planul de tratare a riscurilor de securitatea informatiilor.

SC Synergy Softworks SRL pastreaza informatiile documentate cu privire la rezultatele tratarii riscurilor de securitatea informatiilor.

A fost stabilita o metodologia de analiza si tratare a riscurilor, metodologia este inclusa in politica referitoare la analiza si tratarea riscurilor SMSI.

Riscurile sunt identificate si definite in raport cu obiectivele a caror realizare este afectata de materializarea lor. Din aceasta cauza existenta unui sistem de obiective clar definite constituie premisa esentiala pentru identificarea si definirea riscurilor.

Responsabilul cu gestionare riscurilor numit prin decizie a managementului informeaza conducerea daca totusi nivelul de risc ramane peste valoarea de prag stabilita chiar si dupa aplicarea.

Implementarea, mentinerea si imbunatatirea SMSI se va face in baza riscurilor specifice de securitate a informatiei identificate de partile interesate. Criteriul in functie de care riscul trebuie evaluat depinde de impactul asupra organizatiei al exploatarii vulnerabilitatilor identificate de amenintarile specifice si al probabilitatii ca acest lucru sa se intample.

SC Synergy Softworks SRL analizeaza si evalueaza riscul, evalueaza impactul asupra rezultatelor in urma unor incidente de securitate, tinandu-se cont de consecintele pierderii confidentialitatii, integritatii sau disponibilitatii resurselor.

SC Synergy Softworks SRL evalueaza probabilitatea de aparitie a problemelor de securitate luand in considerare amenintarile si vulnerabilitatile predominante, impactul asociat asupra obiectivelor si indirect asupra resurselor si masurile de securitate implementate in prezent.

SC Synergy Softworks SRL estimeaza nivelurile de risc, determina daca riscurile sunt acceptabile sau necesita tratarea lor, folosind pentru aceasta criteriile de acceptare a riscului stabilite, identifica si evalueaza optiunile pentru tratarea riscului.

Actiunile de tratare a riscurilor includ:

* aplicarea unor masuri de securitate corespunzatoare;
* acceptarea constienta si obiectiva a riscurilor, cu conditia ca acestea sa satisfaca in mod

clar politicile si criteriile de acceptare a riscurilor din cadrul SC Synergy Softworks SRL;

* Analizeaza evitarea riscurilor transferarea riscurilor asociate catre alte parti, de exemplu prin asigurari de bunuri (polita de asigurarea abunurilor);

SC Synergy Softworks SRL analizeaza selecteaza obiectivele de control si masurile pentru tratarea riscurilor confrom Registrului riscurilor si planului de tratare a riscurilor.

Prin implementarea cerintelor sistemului de management al securitatii informatiei se asigura protejarea bunurilor informationale ale organizatiei de toate amenintarile, fie ele interne sau externe, deliberate sau accidentale.

Implementarea, mentinerea si imbunatatirea SMSI se va face in baza riscurilor specifice de securitate a informatiei identificate de partile interesate. Criteriul in functie de care riscul trebuie evaluat depinde de impactul asupra societatii al exploatarii vulnerabilitatilor identificate de amenintarile specifice si al probabilitatii ca acest lucru sa se intample.

Angajatii indeplinesc sarcinile ce ii revin prin fisa postului precum si din prevederile regulamentului de ordine interioara. Orice abatere de la prevederile acestuia si de la politicile si regulile interne de protejare a informatiei din domeniul de aplicabilitate se monitorizeaza.

Metodologia de analiza a riscurilor aleasa se bazeaza pe identificarea amenintatilor care pot exploata vulnerabilitatile resurselor informationale.

Se au in vedere impactul asupra pierderii confidentialitatii, integritatii si disponibilitatii informatiei dar si probabilitatea ca o amenintare sa exploateze o vulnerabilitate existenta.

***9. Evaluarea performantelor SMSI***

*9.1. Monitorizarea, masurarea, analiza si evaluarea performantelor SMSI*

SC Synergy Softworks SRL evalueaza performanta si eficacitatea sistemului de management al securitatii informatiei.

SC Synergy Softworks SRL stabileste:

* Ceea ce trebuie sa fie monitorizat si evaluat, inclusiv procesele si controalele de securitate a informatiilor;
* Metodele de monitorizare, masurare, analiza si evaluare, dupa caz, pentru a asigura rezultate valide;
* Metodele selectate trebuie sa produca rezultate comparabile si reproductibile a fi considerate valide;
* Cand se efectueaza monitorizarea si masurarea;
* Ce aspecte SMSI vor trebui monitorizate si masurate;
* În ce caz rezultatele de la monitorizare si masurare trebuie sa fie analizate si evaluate;
* Cine analizeaza si evalueaza aceste rezultate;

SC Synergy Softworks SRL pastreaza informatiile documentate corespunzator ca dovada a rezultatelor de monitorizare si masurare.

### SC Synergy Softworks SRL a identificat parametrii cheie de performanta pentru SMSI

La evaluarea conformarii se folosesc informatii din urmatoarele activitati:

* Audituri interne si externe
* Analiza documentelor si inregistrarilor
* Interviuri
* Analiza activitatilor SMSI etc.

In cadrul SC Synergy Softworks SRL sunt determinate, colectate si analizate date corespunzatoare pentru a demonstra adecvarea si eficacitatea SMSI si pentru a evalua unde se poate aplica imbunatatirea continua a eficacitatii sale.

Analiza datelor furnizeaza informatii referitoare la:

* Satisfactia partilor interesate;
* Conformitatea cu cerintele serviciilor;
* Caracteristicile si tendintele proceselor SMSI si oportunitatile pentru actiuni corective.

Analiza datelor se face in scopul evaluarii performantei SMSI si ajuta la determinarea cauzelor problemelor existente sau potentiale, servind ca ghid pentru deciziile care privesc actiunile necesare pentru imbunatatire.

Persoanele responsabile conform documentelor SMSI prezinta la solicitarea Directorului General sau pentru analizele SMSI rapoarte de analiza a datelor provenite din activitatile desfasurate. In urma analizarii acestor rapoarte in sedintele de analiza efectuate de management sunt stabilite dupa caz, actiuni corective si/sau de imbunatatire a SMSI.

SC Synergy Softworks SRL colecteaza si analizeaza toate datele necesare pentru demonstrarea adecvarii si eficacitatii sistemului de management al securitatii informatiei.

Analiza datelor ajuta firma sa identifice cauzele problemelor ce apar, iar rezultatele analizate sunt utilizate pentru a identifica:

* acele activitati care au impactul cel mai nefavorabil asupra SMSI si a partilor interesate;
* erorile (abaterile) sistematice, a cauzei lor si modul de prevenire a acestora;
* satisfactia sau insatisfactia partilor interesate;
* eficacitatea si eficienta societatii;
* performantele economice si financiare;
* conformitatea serviciului prestat fata de cerintele specificate.

Datele sunt analizate si interpretate utilizandu-se tehnici si metodologii statistice. Rezultatele acestor interpretari constituie date de intrare a analizei efectuate de managementul.

***9.2. Auditul intern***

SC Synergy Softworks SRL efectueaza audituri interne ale SMSI la intervale planificate pentru a furniza informatii cu privire la:

a) Conformitatea sistemului de management al securității informației cu nevoile proprii ale SC SparkleTech Solutions SRL și cu cerințele ISO 27001.

b) Implementarea și menținerea eficientă a sistemului de management al securității informației.

In cadrul SC Synergy Softworks SRL:

* Se planifica, stabileste, implementeaza si mentine un program de audit, inclusiv frecventa, metodele, responsabilitati, cerinte de planificare si raportare. Programul de audit are in vedere importanta procesului in cauza si rezultatele auditurilor precedente;
* Se defineaste criteriile de audit si domeniul de aplicare pentru fiecare audit;
* Se selecteaza auditori si se stabileste conduita auditorului care sa asigure obiectivitatea si impartialitatea procesului de audit;
* Se asigura ca rezultatele auditurilor sunt raportate la gestionarea corespunzatoare; si
* Se retin informatiile documentate ca dovada a programului de audit, precum si rezultatele auditului SMSI.

Planul de audit ia in considerare pozitia si importanta proceselor si zonelor care urmeaza sa fie auditate precum si rezultatele auditurilor anterioare. Criteriile de audit, aplicabilitatea, frecventa si metodele trebuie definite. Selectarea auditorilor si efectuarea auditurilor asigura obiectivitatea si impartialitatea procesului de audit. Auditorii nu isi vor audita propria lor activitate.

Responsabilitatile si cerintele pentru planificarea si efectuarea de audituri si pentru raportarea

rezultatelor si pastrarea inregistrarilor sunt definte in procedura procedura PG-822.

Managementul SC Synergy Softworks SRL este responsabil si se asigura ca actiunile necesare sunt luate fara intarzieri neprevazute pentru a elimina neconformitatile detectate si cauzele acestora.

Activitatile de urmarire includ verificarea masurilor luate si raportarea rezultatelor acestei verificari.

Managementul riscurilor in cazul procesului de auditare interna a SMI urmareste identificarea si gestionarea riscurilor care pot afecta atingerea obiectivelor specifice auditului intern.

In continuare sunt prezentate cateva tipuri de riscuri in cazul procesului de auditare interna a SMI: calificarea necorespunzatoare a auditorilor, auditarea propriei activitati, conditiile de mediu necorespunzatoare desfasurarii auditului, nerespectarea procedurii de audit, atitudinea necorespunzatoare a auditorilor, nerespectarea programului de audit de catre partile interesate.

Procedura, PG-822, Audit intern descrie metodologia de realizare a auditului intern.

***9.3. Analiza efectuata de management***

Conducerea de top analizeaza informatiile referitoare la functionarea sistemului de management al securitatii informatiei la intervale planificate pentru a se asigura ca este in permanenta corespunzator, adecvat si eficient.

Analiza de management include:

a) stadiul actiunilor din analizele anterioare de management;

b) modificarile problemelor interne si externe care sunt relevante pentru organizatie

c) feedback-ul cu privire la performanta de securitate a informatiilor, inclusiv evolutia:

* neconformitati si actiuni corective;
* rezultatele monitorizarii si masurariii;
* rezultatele auditului SMSI; si
* realizarea obiectivelor de securitate a informatiilor;

d) feedback-ul de la partile interesate;

e) rezultatele evaluarii riscurilor si rezultatele plan de tratare a riscurilor; si

f) oportunitati de imbunatatire continua.

Iesirile de date ale analizei de management includ deciziile legate de imbunatatirea continua oportunitati si eventualele nevoi de modificare a sistemului de management al securitatii informatiei. SC Synergy Softworks SRL pastreaza informatiile documentate ca dovada a rezultatelor analizelor de management.

Procedura, PO-56, Analiza efectuata de management descrie metodologia de desfasurarea analizei efectuate de management.

***10. Implementarea SMSI***

*10.1. Nonconformitate si actiuni corective*

Atunci cand apare o neconformitate, SC Synergy Softworks SRL intreprinde actiunile:

a) reactioneaza la neconformitatea, si dupa caz

* ia masuri pentru a controla si de a corecta neconformitatea;
* ia masuri sa faca fata consecintelor;

b) evalueaza necesitatea de a actiona pentru a elimina cauzele neconformitatilor, pentru ca neconformitatea sa nu se produca si in alta parte, prin:

* analizarea neconformitatilor;
* determinarea cauzelor neconformitatii; si
* determinare daca exista neconformitati similare sau alt tip de neconformitati potentiale;

c) punerea in aplicare a oricarei actiuni necesare;

d) evaluarea eficacitatii oricarei actiuni corective intreprinse; si

e) modificarea sistemului de management al securitatii informatiei, daca este necesar

Actiunile corective trebuie sa fie adecvate efectelor neconformitatilor intalnite.

SC Synergy Softworks SRL pastreaza informatiile documentate ca dovada pentru:

* natura neconformitatilor si orice actiuni ulterioare intreprinse, si
* rezultatele oricarei actiuni corective implementate.

***10.2 Imbunatatire continua***

SC Synergy Softworks SRL isi imbunatateste in mod continuu, gradul de adecvare si eficacitatea sistemului de management al securitatii informatiei.

SC Synergy Softworks SRL in mod regulat actioneaza pentru:

* implementarea imbunatatirilor identificate ale SMSI;
* aplicarea de masuri corective corespunzatoare;
* a aplica lectiile invatate din experientele de securitate ale altor organizatii si cele ale propriei organizatii,
* de a participa la consultarea diveselor surse de informatii:
* enisa.europa.eu/
* first.org/
* trusted-introducer.org/
* cert-ro.ro
* dataprotection.ro
* itgouvernace.co-uk
* securitatea-informatiilor.ro/forum/
* comunicarea masurilor si imbunatatirilor tuturor partilor interesate tinand cont de circumstante si, in functie de relevanta, in scopul implementarii de masuri specifice;
* asigurarea ca masurile de imbunatatire intrepinse ating obiectivele planificate;

In SC Synergy Softworks SRL eficacitatea SMSI este analizata periodic de catre Directorul General in cadrul activitatilor curente si a sedintelor de analiza, urmarindu-se modul de indeplinire a politicii in domeniul SMSI si a obiectivelor aprobate, rezultatele auditurilor, stadiul si eficacitatea implementarii actiunilor corective. In urma acestor analize se stabilesc decizii si actiuni care sa conduca la imbunatatirea continua a eficacitatii SMSI si a proceselor sale care se inregistreaza de Responsabilul SMSI in “Programul de imbunatatire” si aprobat de Directorul General. Monitorizarea deciziilor luate si a actiunilor de imbunatatire este asigurata de Responsabilul SMSI si raportata Directorului General.

Organizatia a stabilit, implementat si mentine reguli pentru a trata o neconformitate existenta sau potentiala si pentru a intreprinde actiuni corective. Procedura defineste cerinte pentru:

* identificarea si corectarea neconformitatii (neconformitatilor) si luarea actiunii (actiunilor) de reducere a impacturilor asupra partilor interesate,
* investigarea neconformitatii, determinarea cauzei lor si intreprinderea actiunilor pentru a impiedica revenirea lor,
* evaluarea necesitatilor de actiuni pentru a preveni neconformitatea si implementarea actiunilor corespunzatoare desemnate a impiedica aparitia lor,
* inregistrarea rezultatelor actiunilor corective intreprinse
* analizarea eficacitatii actiunilor corective intreprinse.

Actiunile intreprinse corespund dimensiunii problemelor si a impacturilor asupra partilor interesate intalnite. SC Synergy Softworks SRL se asigura ca orice schimbari necesare sunt aplicabile SMSI.

Exista o politica privind imbunatatirea continua a SMSI si a serviciilor. Politica include criteriile de evaluare pentru oportunitatile de imbunatatire.