iTrade Integrated Systems SRL

Procedura de securitate a informatiei

Document Control

Versiune	Data	Autor	Motivul schimbarii
1.0	16.05.2018	Andrei Dumitrel	Versiunea 1

1. SCOPUL SI DOMENIUL DE APLICARE

Aceste proceduri cuprinse in prezentul document sunt reglementate de politica de Securitate a Informatiei. Acest set de proceduri se aplica tuturor angajatilor companiei iTrade Integrated Systems cat si colaboratorilor, vizitatorilor si subcontractorilor companiei.

2. CONTROLUL ACCESULUI

Toti utilizatorii mediului informational al companiei iTrade Integrated Systems SRL trebuie sa fie autorizati si sa aiba access specific si monitorizat la sistemele si datele companiei. Accesul se da cu aprobarea managementului companiei iar activitatea poate fi monitorizata in functie de gradul de risc reprezentat de datele si sistemele accesate.

Elementele folosite pentru controlul si monitorizarea accesului sunt : Identificarea, autorizarea si autentificarea.

2.1 IDENTIFICAREA

a. Toti angajatii companiei au un identificator unic (user id) pentru accesul la sistemele informatice ale companiei
b. Identificatorul de acces (user id) nu poate fi instrainat sau utilizat de catre alta persoana decat cea caruia ii apartine
c. Utilizatorii sunt responsabili de securitatea identificatorului lor personal si sunt raspunzatori de toate actiunile intreprinse pe sisteme sub acest identificator
d. Managementul companiei poate aproba crearea temporara de identificatori sau identificatori generici pentru cazuri particulare cum ar fi testare sau instruirea personalului.

2.2 AUTORIZAREA

a. Managerii sistemelor sunt responsabili cu setarea unui nivel corespunzator de drepturi de access pentru utilizatorii acestor sisteme. Utilizatorii pot fi clienti, utilizatori din cadrul companiei, dezvoltatori, sub-contractori.
b. Managerii sistemelor au responsabilitatea de a face regulat o revizuire a tuturor drepturilor de utilizatori de pe sistemele lor pentru a vedea daca exista aprobarile necesare sau daca mai sunt de actualitate. Neregulile descoperite in urma acestor actiuni de revizuire trebuie remediate cu prioritate maxima si documentate.

2.3 AUTENTIFICAREA

Accesul la sistemele informatice ale companiei iTrade Integrated Systems vor necesita acel identificator unic si o parola. Parola este in responsabilitatea si sub protectia utilizatorului. Este interzisa partajarea identificatorului si al parolei cu alti utilizatori.

2.4 PAROLELE

Parolele sunt folosite pentru accesul in diferite sisteme.

2.4.1 REGULI IN ALEGEREA PAROLELOR

a. Parolele trebuie sa contina minim 8 caractere alfanumerice
b. Parolele trebuie sa contina cel putin un caracter majuscul si cel putin unul micuscul
c. Parolele trebuie sa contina cel putin un caracter special (ex. !@#$%^&*()_+-=:";'<>,.?/)

Parolele nu trebuie sa contina:

- Identificatorul de retea sub nicio forma
- Numele sau prenumele utilizatorului
- Numele unei persoane apropiate, animal de companie sau obiect preferat
- Caractere la rand de pe tastatura
- Mai mult de 2 cifre consecutive
- Numarul de inmatriculare al autovehiculului personal
- Data de nastere
- Numarul de telefon
- Adresa
- In general orice data a utilizatorului care poate fi dedusa sau aflata

2.4.2 MANAGEMENTUL PAROLELOR

a. Toate parolele initiale trebuie generate aleator iar utilizatorul trebuie fortat sa isi schimbe parola la prima utilizare
b. Toate parolele folosite pentru accesul sistemelor trebuie schimbate odata la 30 de zile. Acest lucru trebuie fortat acolo unde sistemele permit.
c. Parolele nu trebuie scrise si lasate la indemana persoanelor neautorizate
d. Parolele nu trebuie pastrate niciodata in fisiere text ci doar in volt-uri criptate
e. Parolele nu trebuie instrainate niciodata indiferent de catre cine sunt cerute
f. Atunci cand se creaza un utilizator si trebuie transmise informatiile de acces in alta locatie atunci acest lucru se face pe 2 canale de comunicare (ex. Utilizatorul pe mail, parola pe telefon)
g. Parolele trebuie trimise criptat pentru sistemele critice

Parolele care se considera in pericol de a fi compromise sunt schimbate imediat si se documenteaza acest incident.

2.4.3 FOLOSIREA SI CONTROLUL UTILIZATORILOR PRIVILEGIATI

Utilizatorii privilegiati sau super userii sunt acei utilizatori care au drepturi de administrare asupra sistemelor. Ei pot da acces altor utilizatori si pot reconfigura sistemele. Activitatea acestor utilizatori va fi monitorizata.

a. Managerii de sisteme vor revizui listele de acces odata la 6 luni de zile. Eventualele neconformitati vor fi remediate imediat si vor fi documentate
b. Accesul la sistemele de jurnalizare va fi dat managerilor de sisteme care vor putea revizui activitatea administratorilor
c. Managerii de sisteme sunt responsabili cu aprobarea accesului la sistemele pe care le administreaza
d. Managerii de sisteme sunt responsabili cu aprobarea accesului pentru utilizatorii externi. Acesti utilizatori trebuie sa actioneze in conformitate cu politica de securitate a companiei
e. Orice activitate suspecta sau incident de securitate trebuie raportat managementului companiei
f. Daca incidentele de securitate au vizat date cu caracter personal trebuie raportate si catre responsabilul cu protectia datelor sau catre autoritatea nationala de supraveghere privind datele cu caracter personal. Raportarea catre autoritate va fi facuta doar de catre managementul companiei sau responsabilul cu protectia datelor.

3. MESAGERIA DIGITALA

Acesta sectiune cuprinde folosirea mesageriei digitale in cadrul companiei iTrade Integrated Systems SRL

3.1 PERMISIUNI DE FOLOSIRE ALE MESAGERIEI DIGITALE

Pentru scopurile si activitatile companiei vor fi folosite doar conturile de comunicare puse la dispozitie de catre companie. Este interzisa trimiterea de mesaje sau date apartinand companiei prin alte canale in afara celor puse la dispozitie de companie. Este interzisa trimiterea de date cu caracter personal prin mijloacele de comunicare digitala fara aprobare. Este interzisa folosirea in scopuri personale a canalelor de comunicare puse la dispozitie de companie.

In cazul obtinerii aprobarii de transmitere a datelor cu caracter personal sau confidentiale prin mijloace electronice (email, webtransfer, FTP, HDD extern, USB stick etc.) se are in vedere criptarea obligatorie a acestor date si transmiterea parolei sau cheii de criptare printr-un mediu diferit fata de cel folosi pentru transmiterea datelor (ex: se arhiveaza fisierele intr-o arhiva criptata cu parola. Arhiva se transmite pe mail iar parola pe telefon sau se aleg alte 2 modalitati diferite de comunicare)

Canalele de comunicare digitale puse la dispozitie de catre companie si apartinand acesteia pot fi monitorizate de catre aceasta in scopul prevenirii scurgerilor de informatii voluntare sau accidentale.

3.2 SCOPURILE IN CARE POATE FI FOLOSITA MESAGERIA DIGITALA

Mesageria digitala pusa la dispozitie de catre compania iTrade Integrated Systems angajatilor poate fi folosita doar in scopurile activitatii companiei.

Urmatoarele aspecte sunt interzise in folosirea mesageriei digitale:

a. Folosirea in scopuri care incalca legislatia Romaniei sau legislatia internationala
b. Castiguri financiare ori scopuri comerciale nelegate de scopurile sau interesele companiei
c. Trimiterea de mesaje care afecteaza drepturile sau libertatile persoanelor
d. Trimiterea de mesaje repetate catre persoane fara a avea acordul acestora. Aspect care ar incalca Regulamentul European privind protectia datelor cu caracter personal
e. Trimiterea de date cu caracter personal sau confidentiale fara acordul companiei
f. Trimiterea fara criptare (sau trimiterea datelor criptate si a cheii de decriptare prin acelasi mediu) a datelor cu caracter personal sau confidentiale
g. Folosirea in scopuri personale

4. MANAGEMENTUL OPERATIONAL

4.1 PROCEDURI OPERATIONALE

Setul urmator de proceduri este creat pentru a oferi protectia si securitatea informatiilor.

4.1.1 DOCUMENTAREA PROCEDURILOR OPERATIONALE

Procedurile operationale au rolul de a stabili si documenta procesele operationale. Ele introduc de asemenea puncte de control pentru a asigura securitatea si buna functionare a proceselor. Procedurile operationale trebuie revizuite periodic sau in momentul in care se introduc schimbari la nivel de procese. Procedurile operationale trebuie sa fie disponibile la cerere

4.1.2 DIFERENTIEREA ATRIBUTIILOR

Pentru a controla procesele si pentru a evita accesul neautorizat sau modificarile eronate asupra datelor. Rolul de utilizator trebuie sa fie diferit de cel de aprobator. Rolul de aprobator este asociat in cadrul companiei managementului companiei.

4.1.3 SEPARAREA MEDIILOR OPERATIONALE

Mediile de dezvoltare, testare si productie trebuie sa fie complet separate pentru a reduce riscul de pierdere a datelor, access neautorizat sau compromitere. Pentru a evita aceste lucruri se recomanda de asemenea ca pentru mediul de test si cel de productie sa fie folosita pseudonimizarea sau anonimizarea.

4.1.4 CONTROLUL IMPOTRIVA ATACURILOR DE TIP MALICIOUS CODE

a. Pentru a proteja datele de eventuale atacuri informatice se foloseste o protectie de tip endpoint-protection cu management centralizat. Solutia enpoint-protection previne atacurile informatice prin mecanisme de tip antivirus, IPS, webfiltering administrate cu ajutorul unei console centrale ce ofera de asemenea o vizibilitate crescuta la nivel de sistem. Cu ajutorul acestei solutii se poate interveni rapid in cazul unui atac.
b. Pentru a proteja intreaga retea si sistemele critice din data center-ul companiei se foloseste un echipament de tip UTM care previne atacurile cibernetice
c. Pentru a mari gradul de protectie a fost implementat un produs pentru managementul vulnerabilitatilor. Folosind consola integrata de pe solutia de endpoint se monitorizeaza starea statiilor din punct de vedere al vulnerabilitatilor cunoscute si aplicarea pachetelor de remediere.
d. Pentru a preveni atacurile informatice se desfasoara regulat (odata la 6 luni) programe de constientizare a utilizatorilor din companie - sesiuni de training.

4.1.5 BACKUP SI RESTORE

Pentru a mentine integritatea si disponibilitatea datelor procesate s-a creat o procedura de backup si restore care cuprinde urmatoarele:

a. Documentarea procesului de backup si metodele de testare aplicate
b. Procesul de restaurare a datelor si metodele de testare aplicate

4.1.6 MANAGEMENTUL SECURITATII RETELEI

Reteaua trebuie controlata pentru a preveni atacurile informatice. Separarea retelei interne de reteaua folosita pentru oaspeti sau pentru device-urile mobile (telefoane, tablete) este obligatorie.

Accesul in reteaua companiei este dat doar cu aprobarea managementului.

4.1.7 MANIPULAREA MEDIILOR DE STOCARE

Scoaterea datelor pe echipamente externe este documentata si descrisa intr-o procedura separata. Aceasta ofera o descriere a procesului de manipulare a mediilor de stocare externe, drepturi, autorizari, metode obligatorii de siguranta. Toate datele cu caracter personal ce vor fi autorizate pentru a fi stocate pe medii externe vor fi criptate.

4.1.8 MONITORIZAREA

Procedura de monitorizare a datelor cu caracter personal si a datelor confidentiale trebuie stabilita si revizuita periodic.

Nivelul de monitorizare trebuie stabilit in functie de riscul procesului de prelucrare a datelor cu caracter personal sau / si al datelor confidentiale.

4.1.9 PROTECTIA SI JURNALIZAREA INFORMATIILOR

Jurnalele prelucrarilor de date cu caracter personal si / sau al datelor confidentiale trebuie protejate impotriva stergerilor / modificarilor voluntare sau accidentale.

a. Se vor crea controale pentru a proteja impotriva schimbarilor neautorizare sau problemelor tehnice legate de mecanismul de jurnalizare (loguri)
b. Jurnalele trebuie pastrate si trebuie sa fie disponibile pentru a proba activitatile in cazul plangerilor catre autoritatea de supraveghere a datelor cu caracter personal sau pentru a putea identifica eventualele probleme de securitate (scurgeri sau deteriorari de date produse in mod voluntar sau accidental)
c. Activitatile de administrare si de operare trebuie sa fie jurnalizate cu cat mai multe detalii posibile. Gradul de detaliere va fi stabilit in functie de resursele disponibile dar trebuie mentinut un grad care sa ofere posibilitatea de identificare a problemelor si probarea activitatilor de prelucrare.
d. Jurnalele activitatilor administratorilor sunt revizuite periodic iar eventualele nereguli gasite documentate si raportate managementului
e. Erorile sunt jurnalizate, analizate si luate masuri adecvate pentru remedierea lor
f. Erorile raportate de catre utilizatori sunt procesate printr-un sistem de tickete care sa ofere urmatoarele detalii :

- Data si ora la care a fost reportat incidentul
- Cine a facut analiza si remedierea
- Cum a fost remediata problema
- Confirmarea din partea celui care a deschis ticketul ca problema a fost remediata

Pentru a avea o acuratete in detectarea problemelor toate sistemele trebuie sa fie sincronizate cu aceeasi sursa de timp.

5. ACHIZITIONAREA DE NOI ECHIPAMENTE, DEZVOLTARE SI INTRETINERE

5.1 CERINTE DE SECURITATE LA SETAREA DE NOI SISTEME

In momentul setarii unui nou sistem trebuie avut in vedere urmatoarele cerinte pentru a fi in conformitate cu politica de securitate a informatiei adoptata de compania iTrade Integrated Systems SRL

a. Este necesara documentarea sistemului din punct de vedere al instalarii si setarilor de securitate

b. Procesul de autentificare sa fie conform politicii de securitate a companiei
c. Jurnalele de tranzactii si monitorizare (loguri) trebuie sa fie setate
d. Accesul la codul sursa trebuie sa fie restrictionat
e. Sistemul trebuie sa asigure alinierea cu normele GDPR inca din faza de proiectare (compliance by design)
f. Toate patch-urile trebuie instalate
g. Trebuie instalata protectia impotriva atacurilor cibernetice (endpoint protection)
h. Trebuie introdus in inventarul procesarilor de date cu caracter personal (daca este cazul)
i. Sistemul trebuie introdus in procedura de backup si restaurare daca este cazul
j. Sistemul trebuie introdus in inventarul de sisteme si nominalizate persoanele responsabile (managerii de sistem si administratorii)

6. RELATIA CU CONTRACTORII

6.1 ACCESUL LA SISTEMELE INFORMATICE ALE COMPANIEI DE CATRE CONTRACTORI

Pentru a controla riscul asociat cu accesul la datele companiei de catre furnizorii externi se vor institui controale si proceduri care sa reglementeze acest acces. Aceste controale trebuie sa contina:

a. Identificarea si tipul de serviciu oferit de furnizor (ex. Infrastructura IT, Servicii Financiare, Servicii de dezvoltare soft)
b. Se va stabili o perioada de valabilitate a contractului
c. Se va defini minimum de drepturi si masuri de securitate necesare pentru fiecare tip de acces.
d. Se va stabili clar setul de masuri de securitate si obligatii pentru fiecare furnizor de servicii sau subcontractor
e. Se va stabili o procedura de change management detaliata pentru a evita schimbarile facute de provideri sau subcontractori neautorizate de companie
f. Se va stabili o procedura de incident management, rezolvarea defectelor
g. Problemele si conflictele vor fi urmarite si rezolvate folosind platforma de ticketing
h. La cererea companiei subcontractorii sau providerii de servicii vor accepta procese de audit prin care compania se asigura ca sunt indeplinite masurile de securitate agreate.

7. MANAGEMENTUL INCIDENTELOR

7.1 MANAGEMENTUL INCIDENTELOR DE SECURITATE SI AL IMBUNATATILRILOR

Responsabilitatea managementului, planificarile si procesele trebuie stabilite in asa fel incat sa asigure un raspuns si o remediere rapida a incidentelor de securitate. Procesul de raspuns la incidentele de securitate trebuie comunicat intregii companii.

Procesele trebuie sa cuprinda:

a. Proceduri de monitorizare, detectare, analiza si raportare a incidentelor de securitate
b. Proceduri de inregistrare a incidentelor de securitate. Raportari ale incidentelor.
c. Proceduri de investigare si documentare
d. Proceduri de rezolvare si monitorizare a vulnerabilitatilor
e. Proceduri de preventie

8. ASPECTE PRIVIND RECUPERAREA IN CAZ DE DEZASTRE

8.1 RECUPERAREA SISTEMELOR IN CAZ DE DEZASTRU

Acesta sectiune stabileste cerintele de recuperare a sistemelor in caz de dezastru sau crize.

a. Trebuie avute in vedere aspectele de securitate a informatiei in cazul recuperarii sistemelor in cazul dezastrelor
b. Documentatia trebuie sa fie clara si actualizata pentru a sustine procesele de recuperare a sistemelor.
c. O structura de management trebuie definita pentru a fi pregatita sa raspunda si sa rezolve evenimentele care pot duce la intreruperea bussines-ului
d. O echipa de raspuns la incidente va fi stabilita. Acesta echipa va avea competenta si autoritatea sa rezolve incidentele si sa asigure restaurarea sistemelor
e. Planul de recuperare in cazul dezastrelor va fi testat periodic

9. ASPECTE LEGALE

9.1 ALINIEREA CU NORMELE GDPR

Pentru a asigura alinierea cu normele GDPR toate contractele trebuie sa contina in mod clar specificatiile necesare pentru a asigura conformitatea subcontractorilor si al furnizorilor de servicii cu normele GDPR.

Acestea trebuie sa contina:

a. Cerinta clara de a asigura conformitatea cu normele GDPR
b. Instructiuni clare de prelucrare a datelor cu caracter personal si acordul subcontractorilor de a efectua doar acele prelucrari pentru care au primit instructiuni
c. Acordul subcontractorilor si al furnizorilor de servicii ca vor asigura toate masurile necesare pentru protectia, disponibilitatea si integritatea seturilor de date cu caracter personal puse la dispozitie de catre companie
d. Acordul subcontractorilor de a accepta un audit din partea companiei